

# **Software Vulnerability Research**

User Guide

# Legal Information

Book Name: Part Number: Software Vulnerability Research User Guide

Product Release Date:

SVR-MARCH2022-UG00 March 2022

# **Copyright Notice**

Copyright © 2022 Flexera

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

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

## **Intellectual Property**

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

## **Restricted Rights Legend**

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

# Contents

1	Software Vulnerability Research Help Library	9
	Product Support Resources	11
	Contact Us	12
2	Introduction	. 13
	About Software Vulnerability Research	13
	Software Vulnerability Editions	14
	Optional Modules	15
	The Scan Process – How Does it Work?	15
	Software Vulnerability Research Life Cycle	16
	System Architecture Overview	16
	Vulnerability Assessment of Microsoft Products	17
	Getting Started with Software Vulnerability Research	17
3	Software Vulnerability Research Quick Start Guide	. 19
	Account Activation	19
	Accept the Flexera Sales Token and Create Your Account	19
	Configure Two-Factor Authentication (2FA)	22
	Token-Based Two-Factor Authentication	22
	SMS-Based Two-Factor Authentication	23
	Two-Factor Authentication Recovery	24
	Configuring Single Sign-On (SSO)	25
	Opening a Support Case	31
	System Requirements for Software Vulnerability Research	31
	Scan Configuration	32
	Agent Deployment	32
	Deploy a Windows Agent	33
	Deploy a Mac Agent	33

	Deploy a Linux Agent	34
	Deploy the Windows Agent Application through Microsoft's System Center Configuration Manager (SCCM)	36
	Run Windows Agent through the Microsoft System Center as a Task Sequence	38
	Randomize the Agent Scan Schedule	44
	Deploy a Windows Agent through Microsoft's Windows Server Update Services (WSUS)	44
	Daemon Deployment	46
	Install the Daemon	46
	Add a Digital Certificate to Windows Server Update Services (WSUS)	48
	Create a Group Policy to Deploy Your Certificate	48
	Smart Group Configuration	51
	Conditions and Logic Operators	51
	Simple Smart Groups	52
	Advanced Smart Groups	52
	Additional Smart Group Information	53
	Workflow Management Rules	53
	Create a Workflow Rule - Overview	54
	Rule Triggers	54
	Patch Rule Actions	55
	Notification Actions	56
	Default Workflow Rules	56
	Custom Workflow Rules	57
	Patching	57
	System Requirements for Patching	58
	Packages	58
	Patch Template	58
	Build Package	60
	Package Deployment	60
	Additional Patching Information	61
_		
4	Dashboard	63
	Dashboard with Threat Intelligence Module	63
	Dashboard without Threat Intelligence Module	64
_		
5	NOTIFICATIONS	69
6	Vulnerability Manager	71
0		/1
	Overview	71
	Watch Lists & Advisories	72
	Watch Lists	72
	View Watch Lists	73
	Create Watch Lists	74
	Edit Watch Lists.	76
	Import a New Watch List	78
	Import an Updated Watch List	81
	Historic Advisories	82

	Product Advisories
	Shared Watch Lists
	FlexNet Manager Suite (FNMS) Import
	Ticketing in Vulnerability Manager
	Create Tickets in Vulnerability Manager
	Delete Tickets in Vulnerability Manager
	Default Ticket Statuses in Vulnerability Manager
	Approve Advisories
7	Research
	Advisory Database
	Advisories
	Advisories with Threat Score
	Advisories without Threat Score
	Rejected Advisories
	Products Database
	Vendors
	Product Versions
	Products
	Suggest Software
8	Assessment Scenarios
	Agent-Based Scan – Requirements for Windows 102
	Agent-Based Scan – Requirements for Mac OS X
	Prepare Your Mac
	Install the Vulnerable Software Discovery Tool for Mac
	Agent-Based Scan – Requirements for Red Hat Enterprise Linux (RHEL)
	Install the Vulnerable Software Discovery Tool for Red Hat Linux 6 RPM and 7 RPM
	Vulnerable Software Discovery Tool Command Line Ontions
	Help 108
	Version 108
	Install
	Uninstall
	Modify Settings
	Controlling the Service
	Scanning from the Command Line
	Agent Configuration Options
	Scanning Via Local Agents
	Scan Types
9	Assessment Reports
-	

	Create a Smart Crown
	Create a Smart Group
	Create a Smart Groups Report
	Device Datails
	Device Details
	Products
	Product Details
	Advisor/Details
	Advisory Details
10	Patching 131
	Patch Library
	Templates
	Packages
	Deployment
	Information
	Update Deployment
	Patching Tickets
	Delete Patching Tickets
	Manual Signatures
	Enable Manual Signatures
	Share Unsigned and Signed .cab Files137
	Deploy the Agent for a Manual Signature
	Deploy a Patch Package for a Manual Signature
	Manual Signature Notifications
11	Policy Manager
	Overview 143
	Policies 142
	Puncies
	Dreaches
12	Analytics
	Advisories
	Advisories by Threat Score
	Tickets
	Devices
	Products
	Reports
	LiveUpdate
13	Ticket Manager    161
	View and Change Tickets Status and Priority

	Default Ticket Statuses in Ticket Manager
14	Settings
	Account
	License Status
	Account Options
	Security Policy
	User Management
	Users
	User Groups
	Roles
	SSO Settings
	Vulnerability Management
	Watch List Groups
	Watch List Subscriptions
	Workflow Management
	Rules
	Default Workflow Rule Examples
	Ticket Queues
	Ticket Status
	Ticket Priorities
	Assessment
	Update Servers & Daemon
	Daemon Resources
	Daemon and WSUS Troubleshooting
	Certificate Configuration
	Certification Authorities
	Scan Configuration
	Scan Configuration
	Microsoft Update Options
	Add Custom Scan Paths
	Downloads
	API 195
	Logs
	Logins
	Tickets
	Watch Lists
	Email Logs
	SMS Logs
	Service Calls
15	Liser Profile
	USET FORCE
16	About Securia Advication
16	About Secunia Advisories

	CVSS (Common Vulnerability Scoring System) 202
	CVSSv3 Score
	CVE References
	Where (Attack Vector)
	Criticality (Severity Rating)
	Impact (Consequence)
A	Appendix A - Threat Intelligence
	Evidence of Exploitation
	Criteria for the Threat Score Calculation
	Threat Score Calculation - Examples

 Threat Intelligence Data for Operations and Security
 214

 Threat Intelligence for Research
 214

# Software Vulnerability Research Help Library

Flexera's Software Vulnerability Research is a one-stop solution for vulnerability management. The solution is available via a web-portal, giving you access to all the modules that you are entitled to use according to your subscription.

Торіс	Content
Introduction	Flexera's Software Vulnerability Research combines Vulnerability Intelligence, Assessment, and Patch Creation with Patch Deployment Tool Integration to enable targeted, reliable, and cost- efficient Patch Management.
Software Vulnerability Research Quick Start Guide	This quick start guide walks you through setting up the key features of Software Vulnerability Research.
Dashboard	The Dashboard is the default home page that provides you with an overview of vulnerability management processes and gives you access to your latest vulnerability intelligence and advisories. The information is presented with the help of various widgets.
Notifications	Notifications provide detailed information about alerts you have received and any required actions. The number in the yellow bubble signifies the number of unread notifications.
Vulnerability Manager	Vulnerability Manager pages are used to manage the Vulnerability Intelligence associated with your account.         Image: Constraint of the Vulnerability Manager module is not available for Software Vulnerability Research - Assessment Only.

Table 1-1 • Software Vulnerability Research Help Library

#### Table 1-1 • Software Vulnerability Research Help Library (cont.)

Торіс	Content
Research	Vulnerability Tracker (VulnTrack) represents our full Vulnerability Database, which has been updated and maintained since the inception of Secunia in 2002.
	<i>Edition</i> • The Research module is not available for Software Vulnerability Research - Assessment Only.
Assessment	The Assessment Scenarios page provides descriptions of the available assessment scenarios.
Scenarios	
	<i>Edition</i> • This module is not available for Software Vulnerability Research.
Assessment	The Assessment Reports page displays a tree view of the Device Groups within your
Reports	environment. The security status of each Device Group is assessed based on <b>Average System</b> Score, Device Details and Product Details.
	<b>Edition</b> • This module is not available for Software Vulnerability Research.
Patching	The Patch Library and Grouped Patch Library pages list the patches available for your environment. Users can create a patch template for deploying patches and can track the patches deployed.
	<b>Edition</b> • This module is not available for Software Vulnerability Research.
Policy Manager	The Policy Manager pages are used to configure internal Compliance Policy Rules to associate with your account and view the details of breaches to your policies.
	<b>Edition</b> • The Policy Manager module is not available for Software Vulnerability Research - Assessment Only.
Analytics	The Analytics pages are used to filter data contained in the widgets and to create and save dynamic reports on Advisories.
Ticket Manager	The Ticket Manager page lists all issued tickets. Use this page to:
	View and Change Tickets Status and Priority
	Create Tickets in Ticket Manager
	Delete Tickets in Ticket Manager
	Default Ticket Statuses in Ticket Manager

Table 1-1 • Software Vulnerability Research Help Library (cont.)

Торіс	Content
Settings	The Settings pages allow the main Administrator account holder to create and manage other accounts.
	This section also tracks details of all activities taken by users related to your account, such as Logins and changes to Tickets, Watch Lists, Email Logs, SMS Logs and Service Calls.
User Profile	The User Profile page is used to view and edit your account information, including your password, personal details, preferences, and security settings.
About Secunia Advisories	Describes CVSS (Common Vulnerability Scoring System), CVE References, Where (Attack Vector), Criticality (Severity Rating), and Impact (Consequence).
Appendix A - Threat Intelligence	Threat Intelligence Module augments Software Vulnerability Research's vulnerability intelligence with a Threat Score that provides the ultimate prioritization tool for your busy desktop operations teams. This module requires purchase by the user.

# **Product Support Resources**

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

- Flexera Product Documentation
- Flexera Community
- Flexera Learning Center
- Flexera Support

#### **Flexera Product Documentation**

You can find documentation for all Flexera products on the Flexera Product Documentation site:

https://docs.flexera.com

#### **Flexera Community**

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

https://community.flexera.com

#### **Flexera Learning Center**

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

https://learn.flexera.com

#### **Flexera Support**

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

https://community.flexera.com

#### **Product Feedback**

You can submit feedback about Software Vulnerability Manager in the Flexera Customer Community Forum. You can also submit feedback through the Software Vulnerability Manager user interface by clicking the feedback icon in the upperright-hand corner of each module.



# **Contact Us**

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

#### http://www.flexera.com

You can also follow us on social media:

- Twitter
- Facebook
- LinkedIn
- YouTube
- Instagram

# Introduction

Flexera's Software Vulnerability Research combines Vulnerability Intelligence, Assessment, and Patch Creation with Patch Deployment Tool Integration to enable targeted, reliable, and cost-efficient Patch Management.

- About Software Vulnerability Research
- Software Vulnerability Editions
- Optional Modules
- The Scan Process How Does it Work?
- Software Vulnerability Research Life Cycle
- System Architecture Overview
- Vulnerability Assessment of Microsoft Products
- Getting Started with Software Vulnerability Research

# **About Software Vulnerability Research**

Vulnerability Intelligence 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 Research, IT Operations and Security Teams are empowered to take control of the Vulnerability Threat from both Microsoft and non-Microsoft (third-party) product vulnerabilities.

The Software Vulnerability Research Assessment module scanning technology takes a different approach than other vulnerability scanning solutions by conducting non-intrusive scans to accurately identify all installed products and plugins on the system.

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

The solution is available via a web-portal, giving you access to all the modules that you are entitled to use according to your subscription.

The sequence of the module descriptions in this document corresponds with the order in which they are presented in the graphical user interface of the solution.

**Note** • The available modules, menus and options will vary depending on the permissions granted to you by your Administrator.

# **Software Vulnerability Editions**

Flexera offers the following editions for Software Vulnerability:

- Software Vulnerability Research (Includes all Modules)
- Software Vulnerability Research

The table below describes the differences between the Software Vulnerability editions.

Any module not available for a specific edition will be noted with an Edition Note. See the example below.

Edition • This module is not available for Software Vulnerability Research.

Table 2-1 • User Interface differences between Software Vulnerability Editions



Table 2-1 • User Interface differences between Software Vulnerability Editions

Software Vulnerability Research (includes all modules)	Software Vulnerability Research does not include Assessment or Patching)
Settings > Workflow Management > Rules Account + User Management + Vulnerability Management + Workflow Management + Assessment + API + Logs +	Settings > Workflow Management > Rules Account • User Management • Vulnerability Management • Workflow Management • API • Logs •
Settings Menu	Settings Menu

# **Optional Modules**

Flexera offers the following optional modules:

• Software Vulnerability Research - Threat Intelligence Module

#### **Threat Intelligence Module**

When added to our Software Vulnerability Research solution, the Threat Intelligence Module helps operations to focus on the patches most critical to the security of the software deployed in your environment. When added to our Software Vulnerability Research (SVR) solution, the Threat Intelligence Module provides security professionals even more insight by exposing threat scores not only for security advisories, but for the specific CVEs associated with those advisories as well as what evidence was triggered to arrive at the provided threat score.

 $\bigcirc$ 

Tip • For more details about the Threat Intelligence Modules, see the following data sheet:

https://www.flexera.com/media/pdfs/datasheet-svm-threat-intelligence-module.pdf

# The Scan Process – How Does it Work?

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

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

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

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

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

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

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

For further information about the different Software Vulnerability Research scanning approaches, see Assessment Scenarios.

# Software Vulnerability Research Life Cycle

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

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

Software Vulnerability Research automates all steps of the software vulnerability management life cycle, allowing you to strengthen the security of your networks.



Figure 2-1: Software Vulnerability Research Lifecycle

# **System Architecture Overview**

The following screenshot provides an overview of the Software Vulnerability Research system architecture.



Figure 2-2: System Architecture Overview

# **Vulnerability Assessment of Microsoft Products**

For Windows and other Microsoft products, Software Vulnerability Research obtains information about missing Microsoft security updates from the scanned device's local Windows Update Agent.

If the Windows Update Agent is managed by the company's IT department, the Microsoft security update has to be approved by the IT administrator before Software Vulnerability Research will report whether it is missing or not.



Figure 2-3: Check for Missing Microsoft Security Update Settings

# Getting Started with Software Vulnerability Research

See Software Vulnerability Research Quick Start Guide to help you set up the key features of Software Vulnerability Research.

Chapter 2 Introduction Getting Started with Software Vulnerability Research

# Software Vulnerability Research Quick Start Guide

This Quick Start guide walks you through setting up the key features of Software Vulnerability Research:

- Account Activation
- Opening a Support Case
- System Requirements for Software Vulnerability Research
- Scan Configuration
- Agent Deployment
- Daemon Deployment
- Smart Group Configuration
- Workflow Management Rules
- Patching

# **Account Activation**

This section takes you through the steps to securely create your Software Vulnerability Research account:

- Accept the Flexera Sales Token and Create Your Account
- Configure Two-Factor Authentication (2FA)
- Configuring Single Sign-On (SSO)

### Accept the Flexera Sales Token and Create Your Account

To create your account, perform the following steps.



#### To accept the Flexera Sales Token and Create your Software Vulnerability Research account:

1. After your sales order is complete, you will receive an activation email from Flexera Sales with a customized link to create your account. The link looks similar to the following token:

https://app.flexerasoftware.com/trial/?token=xxxxxx

Your activation email from Flexera includes the particular token number. Click the token link to begin the initial setup process for the main Administrator account. The following window will appear:

Want to test us out? Pl fill in the form below	ease
First Name	
Last Name	
Email Address	
Job Title	
Company	
Number of Employees	
Country	
Request Trial Account	
Cancel	

- 2. After completing the relevant details that are mandatory for the creation of your account, click **Request Trial Account**.
- **3.** Go to your email's inbox and find the verification link sent by Flexera. Click the verification link, and a new window will open for you to create your account's user name and password.

Set up your account information
Choose admin username
Choose a password
Confirm password
I hereby accept the Flexera <u>Terms &amp; Conditions</u> and <u>Privacy Policy</u>
Create Trial Account
Cancel

# 

Important • Before you enter any passwords, consider the default password rules required by Flexera:

- 8-200 characters
- At least one lowercase letter
- At least one uppercase letter
- At least one digit



Important • You should also consider the following recommendations for creating account passwords:

- No common passwords
- No personal details
- No old passwords
- Passwords created by a password generator
- 4. After entering your username and password, click Create Trial Account. You will then be taken to the Software Vulnerability Research Login page where you login with the previously configured credentials. When logging in to your account for the first time, you will be asked to Configure Two-Factor Authentication (2FA) to secure the account. You must configure 2FA before you are allowed to login, as two-factor authentication is mandatory.

#### Logging In to Software Vulnerability Research

If you already have a Software Vulnerability Research account and want to login, perform the following steps.



#### To login to Software Vulnerability Research:

- 1. Open the Software Vulnerability Research Login page and enter your username and password.
- 2. If you have forgotten you password, click **Forgot your password?** Enter your email address and click **Send mail** to receive instructions to reset your password.

## **Configure Two-Factor Authentication (2FA)**

To secure your account in the event that the account password has been compromised, two-factor authentication (2FA) is mandatory.

Software Vulnerability Research allows the following 2FA configuration options:

- Token-Based Two-Factor Authentication
- SMS-Based Two-Factor Authentication

Choos auther	e a two-factor itication method
Token SMS	
	Next

Figure 3-1: Choosing a Two-Factor Authentication Method

Token-based two-factor authentication is the default and recommended option.

In case your phone is lost or compromised, two-factor authentication can be reset. The reset method varies by account type. For details, see Two-Factor Authentication Recovery.

#### **Token-Based Two-Factor Authentication**

To use token-based two-factor authentication, you first need to install an application specific to your device. Flexera's Software Vulnerability Research uses the standard Time-Based On-Time Password Algorithm (TOTP) for token-based two-factor support, which is supported by applications like Google Authenticator or Duo by Cisco.

Android devices—Download the Google Authenticator application from the Google Play Store:

https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2

• iOS devices—Download the Google Authenticator, available under iTunes in the App Store:

https://itunes.apple.com/us/app/google-authenticator/id388497605?mt=8

#### Logging Into Your Account Using Two-Factor Authentication

To login to your account using two-factor authentication, perform the following steps.

#### To log in to your account the first time with token-based two-factor authentication:

- 1. After entering your username and password, you will be presented with a QR code and a field for the verification code.
- 2. Open the Google Authenticator application and select the Scan a Barcode option.
- 3. When the application loads the device camera, scan the QR barcode displayed on your computer screen.
- The mobile application will generate a unique code. Enter this code in the Verification Code field at the Software Vulnerability Research Login page.



÷

Task

5. Click Save to proceed with logging in to your new account.

#### **SMS-Based Two-Factor Authentication**

SMS-based two-factor authentication is a less secure and a less reliable method that is available and can be used as a fallback in case your phone does not have an authenticator application.

- Logging in the First Time
- Logging in Subsequent Times

# Logging in the First Time Image: Comparison of the first time with SMS-based two-factor authentication:

1. At the Software Vulnerability Research two-factor authentication window, select SMS and click Next.

Choose a two-factor authentication method					
🔵 Token					
O SMS					
	Next				

- 2. Enter your phone number in international format, starting with a +.
- 3. Click Send an SMS.
- Once the SMS arrives, enter the code it contains on the Software Vulnerability Research Login page and click Verify Token.

#### **Logging in Subsequent Times**

#### filler Task

To log in to your account with SMS-based two-factor authentication for all future logins:

- 1. After you are asked for the authentication Token, click Send SMS.
- 2. Once the SMS arrives, enter the code on the Software Vulnerability Research Login page and click Log in.

# **Two-Factor Authentication Recovery**

In case your phone is lost or compromised, two-factor authentication can be reset. The reset method varies by account type.

- Recovering Two-Factor Authentication for Main Administrator Accounts
- Recovering Two-Factor Authentication for User Accounts

#### **Recovering Two-Factor Authentication for Main Administrator Accounts**

Two-factor authentication for the main Administrator account can be reset by our Support department after verifying the identity of the account holder.

#### **Recovering Two-Factor Authentication for User Accounts**

For User accounts, two-factor authentication can be reset by the main Administrator directly from Software Vulnerability Research. In the Settings module, go to **User Management > Users**. Expand the appropriate user row and click **Reset two factor login**. It is recommended to verify first the identity of the user requesting the reset.

Settings > User N	/lanagement > เ	Jsers								?	→[
Account 🗸	User Manage	ement 🗸	Vulnerability Manag	ement 🗸	Workflow Management -	Asse	ssment ·	→ API →	Logs 🗸		
Browsing 1-20 of 2	8 users į							<b>Q</b> Search by us	ername or email address	+	Ŧ
Username 💠	First Name	Last Name	Job Title	Email Address	÷	Active ≑	Blocked	Groups			
						Yes	No	Administrators			
					Edit	Reset two	factor logii	n Disable	Delete		

# Configuring Single Sign-On (SSO)

Task

<b>Not</b> ven	<b>te</b> • The following information is unique to the single sign-on vendor Okta (SAML 2.0). Single sign-on procedures from other dors may vary.
To s	et up Okta (SAML 2.0) to use as a single sign-on (SSO) with Software Vulnerability Research:
1.	Sign in to Okta.
2.	Create an admin account.

3. Click Create New App to create a new Okta SSO app.

okta Dashboard		Applications				•
← Back to Applications						
Q Search for an application			ABCDE	FGHIJ	KLMNOPQ	RSTUVWXYZ
Can't find an app? Create New App		Teladoc Okta Ve	rified			Add
Apps you created (1) $\rightarrow$	&fra	ankly &frankly Okta Ve	nfied 🗸 SAMI	-		Add

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

Create a New Application Integration		×
Platform	Web 🔻	
Sign on method	<ul> <li>Secure Web Authentication (SWA)</li> <li>Uses credentials to sign in. This integration works with most apps.</li> </ul>	
	<ul> <li>SAML 2.0</li> <li>Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.</li> </ul>	
	OpenID Connect Uses the OpenID Connect protocol to log users into an app you've built.	
	Create	

5. Enter an App name (Example: SVM) and App logo (Example: see Software Vulnerability Research logo below). Then click Next.

okta	Dashboard	Directory	Applications	Security	Report	s Se	ettings		Ð
📭 Create SA	AML Integ	Iration							
<b>1</b>	General Settings		2	Configure SAM				3 Feedback	
1 General Settin	ngs								
App name		SVM S	taging						
App logo (option	al) 😰								
		Logo.p	ng			Browse	]		
		Uploa	d Logo						
App visibility		Do	not display applicati	on Icon to users					
		Do	not display applicati	on Icon In the Ok	ta Mobile	app			
Cancel					(	Next	lm		

- 6. Copy the following from the Software Vulnerability Research Settings > User Management > Single Sign On fields and paste in the Okta SAML Settings > fields:
  - Single Sign On URL (Same with Recipient URL and Destination URL) to Single sign on URL and Audience URL (SP Entity ID)

• Account Key to accountKey Value

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

- firstName
- lastName
- email
- username

GENERAL		E Settings > User Management > Single Sign On
Single sign on URL	https://stage.app.secunia.com/sso/sami/bf9a6faa-99a8-4cab-	
	Allow this app to request other SSO URLs	SSO Settings 🦸
Audience URI (SP Entity ID)	https://stage.app.secunia.com/sso/sami/bf9a6faa-99a8-4cab-	IDP Configuration Instructions
Default RelayState 🌚	If no value is set, a blank RelayState is sent	Single Sign On URL (Same with Recipient URL and Destination URL)
Name ID format 💿	Unspecified +	https://stage.app.secunia.com/sso/saml/bf9a6faa-99a84cab-94c1-e5153b0e3faf
Application username	Okta username v Show Advanced Settings	Account Key Set the below value in your identity Provider (idP) as a SAML attribute named "accountKey"
ATTRIBUTE STATEMENTS (OPTION	VAL) LEARN MORE	7KcLPYlubaaA Generate and Show Key
Name Name form (optional)	hat Value	Note: This key is not stored on the SVM server, please make sure that you keep it in a safe place. If lost, you may regenerate the key but doing so will invalidate the old key.
firstName Unspecifi	▼ 7KcLPYlubaA      ▼ × ied ▼ user.firstName      × ×	Please see <u>product help</u> for more information and examples.

7. Click (if not already selected) I'm an Okta customer adding an internal app for the Create SAML Integration - Step 3 Feedback screen. You can leave the rest of the fields blank.



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

General	Sign On	Import	Assignments	
Settings				Edit
SIGN ON The sign- on metho	N METHODS on method dete ods require addit	ermines how a tional configui	user signs into and manages their credentials for an application in the 3rd party application.	ation. Some sign-
SAN	/IL 2.0			
	Default Relay St	ate		
ŧ	SAML 2.0 Is View Setup Identity Prov	not configure o Instructions Ider metadata	d until you complete the setup instructions.	on.

9. Copy the Identity Provider metadata URL from Okta into the Software Vulnerability Research Settings > User Management > Single Sign On > IDP Metadata URL field. Check SSO Enabled, check Automatically create new users, and assign a Default group for new users.

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

← → C  Secure   https://flexera.okta.com/app/exk622qw73e7ezvhC355/sso/saml/metadata	* • <b>G</b> :	← → C • Secure   https://stage.app.secunia.com/#/settings/um/sso/	• @ \$ @ <b>\$</b>				
This XML file does not appear to have any style information associated with it. The document tree is s	hown below.	Settings > User Management > Single Sign On					
This XML file does not appear to have any style information associated with it. The document tere with information of the second secon	honn below: tta.com/esk2240/12/2016/15/55 i energi tt15040/12/01protocol "> 4160804/12/01protocol ">	Exitings > User Management > Single Sign On  Account Key Set the below value in your identity Provider (idP) as a SAML attribute named "accountKey"      Generate and Show Key Network This key is not stored on the SVM server, please make sure that you keep it in a safe place. If lost, you may regenerate the below to dring so will invalidate the old key. Please see product help for more information and examples.					
<ul> <li>umr.caskinames tet 2004.1.1.maskid-format unspecified vindimasiDformati vi</li></ul>	el*∕>	Service Provider Configuration  Service Provider Configuration  So Chabled  DP Metadata URL  Intro://fibrera.okta.com/ann/ex/c52/nu/7ac7en/hr/355/cso/saml/metadata					
		Control of the second					
		API Developers	•				
		© 2015-2018 Flexera. All rights reserved. <u>Terms. and. Conditions. Data. Privacy</u>	<mark>e×</mark> era				

- **10.** If you want to disable standard login options for all of your users (except root), select the **Disable standard login** option under **Settings > User Management > SSO Settings > Service Provider Configuration**.
- **11.** Click **Save** to on the **Settings > User Management** page.

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

**12.** Add Software Vulnerability Research users to the Okta SSO account.

okta			Applications			My Applications 🔿
🔜 Applic	cations					Help
💐 Add Appl	Ication 🐺 As	sign Applications	More 🔻			
QSearch						
STATUS		Ø	SVM Dev			•
ACTIVE	2					
INACTIVE	0	ß	SVM Staging	9		\$ v

13. Assign Software Vulnerability Research users to the Okta SSO app. A reset password link is sent to each user.

SVM Staging	Ø •
	Assign to Users
	Assign to Groups
	U Deactivate
	Copy embed link

**14.** Users open the reset password link, reset their password, and click open the Okta SSO application.

okta		٩	🔒 Home	<b>.</b> •	<b>1</b> -	+ Add Apps	Admin
Work	+						
SV/M Staging							
SVM Staging							

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



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

# **Opening a Support Case**

If you have any questions or concerns regarding your Software Vulnerability Research account, please open a support case via Flexera's Customer Community. For more information, see:

https://community.flexera.com/t5/Using-the-Case-Portal/tkb-p/case-portal-help

# System Requirements for Software Vulnerability Research

The Software Vulnerability Research User Interface will resize and adapt when being used on different devices. You can access the system from anywhere using any device, such as a smartphone or tablet.

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

#### Table 3-1 • System Requirements

Requirement	Description		
Monitor resolution	The minimum resolution required is 1280 x 1024.		
Browser	<ul> <li>The following browsers are supported:</li> <li>Internet Explorer 11 or higher</li> <li>Chrome</li> <li>Opera</li> <li>Firefox</li> </ul>		
	• Safari		
Internet connection	Internet connection capable of connecting to https://app.flexerasoftware.com/ is required.		
Allow Listed sites	The following addresses should be Allow-listed in the Firewall/Proxy configuration:		
	• https://*.secunia.com/		
	• crl.verisign.net		
	• crl.thawte.com		
	• http://crl3.digicert.com		
	• http://crl4.digicert.com		
	• http://*.ws.symantec.com		
First-party cookie settings	First-party cookie settings should be set to at least <b>Prompt</b> (in Internet Explorer).		
Session cookie settings	The option to allow session cookies should be selected.		

#### Table 3-1 • System Requirements

Requirement	Description
PDF reader	A PDF reader is required.

Ŏ

**Important** • The listed required URLs are absolutely mandatory as they relate to Certificate Validation of the non-repudiated SSL certificates, which guarantee that communication between your network and the Cloud is not intercepted, redirected, or modified in any way by a third-party.

#### Ì

*Important* • The Software Vulnerability Research IPs are subject to change without notice, and you should not lock access to Software Vulnerability Research based on the current IP, but should rely on the SSL and certificate validation instead.

# **Scan Configuration**

To control when and how Software Vulnerability Research agents, that are installed and running as a services, collect data, perform the following steps.

# Task To control when and how Software Vulnerability Research agents collect data:

- 1. Log in to https://app.flexerasoftware.com/login/?next=/
- 2. Go to https://app.flexerasoftware.com/#/settings/env/scan/
- **3.** The panel allows you to configure when and what you scan. By default, we scan daily at midnight (during the local agent host's time zone). See Scan Configuration for further details.

# **Agent Deployment**

This section details the following agent deployment methods:

- Deploy a Windows Agent
- Deploy a Mac Agent
- Deploy a Linux Agent
- Deploy the Windows Agent Application through Microsoft's System Center Configuration Manager (SCCM)
- Run Windows Agent through the Microsoft System Center as a Task Sequence
- Deploy a Windows Agent through Microsoft's Windows Server Update Services (WSUS)

## **Deploy a Windows Agent**

These deployment instructions explain how to install the Software Vulnerability Research Agent on a single Windows machine, where the agent will run as a service and report back to the Software Vulnerability Research server on a daily basis.

Before deploying the Windows Agent, see the prerequisites in Agent-Based Scan - Requirements for Windows.

Task	To deploy a Windows Agent:					
	1.	Log in to https://app.flexerasoftware.com/login/?next=/				
	2.	In the Settings module, go to <b>Assessment &gt; Downloads</b> . For details see, Downloads.				
	3.	Download the Vulnerable Software Discovery Tool Installer for Windows.				
		Vulnerable Software Discovery Tool Installer for Windows:         Version: 8.0.344         Download: SVMScanInstall.msi         Checksum (sha256): cdcmpc6561a3695ca13a001768700b416a95831d1fa98fd76fe01da3ce5b45b				

- 4. Run the SVMScanInstall.msi on a Windows machine you wish to scan. This step will set the Agent up to run as a service.
- 5. Follow the scan settings you have configured in the Scan Configuration (https://app.flexerasoftware.com/#/settings/ env/scan/). There are no configuration options to set during installation. In about 30 minutes, you should see the first set of scan results in the Software Vulnerability Research website.

## **Deploy a Mac Agent**

The Vulnerable Software Discovery Tool for Mac (svmscan\_macos) is a small, simple, customizable and extremely powerful scan engine that offers a fully featured command line interface (CLI) for scanning functionality.

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

#### 

*Important* • Ensure that the Vulnerable Software Discovery Tool for Mac is always available in a local folder on the target host.

Before deploying the Mac Agent, see the prerequisites in Agent-Based Scan – Requirements for Mac OS X.



#### To deploy a Mac Agent:

- 1. Log in to https://app.flexerasoftware.com/login/?next=/
- 2. In the Settings module, go to Assessment > Downloads. For details see, Downloads.
- 3. Download the Vulnerable Software Discovery Tool for Mac.
- 4. Click svmscan\_macos.dmg to download the Mac.

Vulnerable Software Discovery Tool for Mac: Version: 8.0.358 Download: svmscan\_macos.dmg Checksum (sha256): 3cac04f62beec6a4e341d6a67afc02a893e85216412fbbe4ebf02381e9132e04

- 5. Double-click on downloaded dmg to view the contents. To save, drag and drop it to the preferred location.
- 6. Open a Terminal windows and run the following commands:

cd Downloads/

To install:

sudo ./svmscan\_macos -i

7. Enter your administrator password. Then you should get information like this.



In about 30 minutes, you should see the first set of scan results in the Software Vulnerability Research website.



**Note** • To un-install run the following command.

./svmscan\_macos.dmg -r

## **Deploy a Linux Agent**

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

The scan Agent for RHEL uses the inventory which is already present (RPM) and displays this in Software Vulnerability Research after being processed by Flexera Detection/Version Rules.

Before deploying the Linux Agent, see the prerequisites in Agent-Based Scan – Requirements for Red Hat Enterprise Linux (RHEL).

#### Task To deploy a Linux Agent:

¢

- 1. Log in to https://app.flexerasoftware.com/login/?next=/
- 2. In the Settings module, go to Assessment > Downloads. For details see, Downloads.
- 3. Based on your version of Red Hat Linux, download the appropriate Vulnerable Software Discovery Tool for Red Hat Linux.



4. Open a terminal session and run the following commands.



**Note** • Your file name may be different depending on the agent version you downloaded.

```
cd Downloads/
sudo yum install svmscan_linux-8.0.345-1.el7.x86_64.rpm
```

5. Enter your administrator password.

```
      @localhost:~/Downloads
      _ I ×

      File Edit View Search Terminal Help
      [ @localhost ~]$ cd Downloads/

      [ @localhost Downloads]$ sudo yum install svmscan_linux-8.0.345-1.el7.x

      86_64.rpm

      [ sudo] password for :
```

6. If the following prompt appears, enter **y** if the installation is OK.





**Note** • To un-install run the following command.

./svmscan -r

parameters.

# Deploy the Windows Agent Application through Microsoft's System Center Configuration Manager (SCCM)

To deploy the Windows agent application (SVMScanInstall.msi) through System Center Configuration Manager, perform the following steps.

ask	To deploy the Windows Agent Application through SCCM:						
	1.	Download the Widows Agent Application (SVMScanInstall.msi) from Software Vulnerability Research under <b>Settings &gt; Assessment &gt; Downloads</b> .					
	2.	Move the installer into a source package directory on the SCCM server.					
	3.	Open the Configuration Manager Administration Console and browse to Software Library.					
	4.	Click Applications and right-click the central window to Create Application.					
	5.	If you get any errors to browse and attach the SVMScanInstall.msi to the new application wizard while you're browsing through shared directories on the local server, use instead the UNC path of the file.					
		Automatically detect information about this application from installation files:      Type: Windows Installer (*.msi file)      Location: \\cm12sq\\cs\shares\demos\SVMScan[Install\SVMScanInstall.msi     Example: \\Server\Share\File					
		O Manually specify the application information					

7. Set the installation command: msiexec /i "SVMScanInstall.msi" /q

If you wish, append extra logging with: /L c:\agent.log

General	Specify information about this application					
Import Information						
General Information						
Summary	Name:	Flexera SVM Next ScanInstall				
Progress Completion	Administrator comments:	This is a Vulnerability Scanning Program by Rexera that enables Administrators to determine the security state of their installed Applications				
	Publisher:	Flexera				
	Software version:	8.0.0.320				
	Optional reference: Administrative categories:	www.flexera.com				
		"Rexera" Select				
	Specify the installation program for this application and the required installation rights.					
	Installation program:	msiexec // "SVMScanInstall.msi" /q Browse				
	Run installation program	as 32-bit process on 64-bit clients.				
	Install behavior:	Install for system v				
- **8.** Finish the application wizard. Find your new application displayed under the **Applications** menu in the **Software Library** of the Configuration Manager Console.
- **9.** Right-click the application name and select **Distribute Content**. Select your distribution point and then complete that wizard too.

Filter			2	Add 🔻
Name	Description	Associations		Collections
CM12SQL.RD12.LAB	Distribution point			Distribution Po
				Distribution Po

- **10.** Right-click your new application once again and select **Deploy** to enable your clients to install the application package containing the SVMScanInstall.msi installer file.
- **11.** Target your Agent package to the necessary device collections you wish to deploy your package to.

General	Specify general information for this deployment					
Content						
Deployment Settings						
Scheduling						
User Experience	Software: Flexera	Flexera SVM Next ScanInstall	Browse			
Alerts	Collection:	Workstations	Browse			
Summary						
Progress	Use default distribu	Use default distribution point groups associated to this collection				
Completion	✓ Automatically distribute content for dependencies					
	Comments (optional):					

- **12.** Under **Deployment Settings**, select **Required** if you want your application to be deployed with maximum priority as soon as possible.
- **13.** Select **Available** to allow users to interact with the application and install it through the Software Center. Click **Next** to finish the wizard and deploy the application.

<u>م</u>		Deploy Software Wizard	x				
Deployment Set	ttings						
General Content	Specify set	tings to control how this software is deployed					
Scheduling User Experience Alerts Summary	Action: Purpose:	Install V Available V Available Required					
Progress Completion	Progress  Require administrator approval if users request this application  Automatically upgrade any superseded versions of this application						
		< Previous Next > Summary Cancel					

14. On the receiving end, open the Control Panel and then the Configuration Manager Client. Run the Machine Policy Retrieval & Evaluation Cycle and the Application Deployment Evaluation Cycle to sync and install the Agent application on the local machine.



Note • More detailed steps can be requested from Flexera's Software Vulnerability Research Technical Support Team.

# Run Windows Agent through the Microsoft System Center as a Task Sequence

To run the Software Vulnerability Research Agent from the Microsoft System Center as a scheduled task, see the steps below. No agents will be installed, and you will only need to maintain one agent binary. To stagger the scanning of multiple machines within a system, see Randomize the Agent Scan Schedule.

- Running the Vulnerable Software Discovery Tool Inside an SCCM Package
- Creating the Initial Scan and Weekly Reoccurring Scan

#### **Running the Vulnerable Software Discovery Tool Inside an SCCM Package**

To run the Vulnerable Software Discovery Tool inside an SCCM package, perform the following steps.



To run the Vulnerable Software Discovery Tool inside an SCCM package:

 Open the Software Vulnerability Research console. From Settings > Assessment > Downloads, download the latest SVRScan.exe file and place it into a deployment share.

Settings > Assessment > Downloads

```
Account 
Vulnerability Management 
Workflow Management 
Vulnerability Management 
Workflow Management 
Vulnerable Software Discovery Tool Installer for Windows:
Version: 8.0.308
Download: <u>SVMScanInstall.msi</u>
Checksum (sha256): 6e38b8bf626baec368714a502036479ad1539a6fc570ac52425b9b7874cae36a
Vulnerable Software Discovery Tool for Windows:
Version: 8.0.308
Download: <u>SVMScan.exe</u>
Checksum (sha256): 2cf1404ddd561a8000963fbdc3d40a7c80e5b55533c7a11b707fa07c7ba682dc
```

SVMScan.ex	e Properties	×
eneral Comp	atibility Digital Signatures Security Details Previous Vers	ions
P.	SVMScan.exe	
Type of file:	Application (.exe)	
Description:	Flexera Software Vulnerable Software Discovery Tool	
Location:	C:\Users\MKoppen\Downloads	
Size:	0.98 MB (1,028,536 bytes)	
Size on disk:	0.98 MB (1.032,192 bytes)	
Created:	Today, November 17, 2017, 10:16:46 AM	
Modified:	Today, November 17, 2017, 10:16:49 AM	
Accessed:	Today, November 17, 2017, 10:16:46 AM	
Attributes:	Read-only Hidden Advanced	
Security:	This file came from another computer and might be blocked to help protect	

- 2. Launch the ConfigMgr console. Select Software Library > Application Management > Packages.
- **3.** From the ribbon, click **Create Package**.

**-**

4. Complete the package information and click Next.

🚮 Create Package and Progr	ram Wizard	×
Package		
Package Program Type Standard Program	Specify inform	ation about this package
Requirements Summary Progress	Enter a name and o Application Catalog,	ther details for the new package. To take full advantage of new features that include the , use an application instead.
Completion	Name:	Flexera SVM Scan Package
compression	Description:	×
	Manufacturer:	Rexera
	Language:	ENG Version: 8.0.257
	This package c	ontains source files
	Source folder:	
	\\sccm16\Sour	rce\Packages\SVM_agent Browse
		< Previous Next > Summary Cancel

- 5. On the **Program Type** page, ensure **Standard Program** is selected and click **Next**.
- 6. On the **Standard Program** page, configure the following settings and click **Next**.

Setting	Description		
Name	Enter SVM Vulnerable Software Discovery Tool.		
Command Line         Enter the following:			
	SVMScan.exe -c - v -d c:\windows\temp\svmscan.log		
	This command line creates a scan log file up to 16 MB in size.		
Run	Set to Hidden.		
Program can run	Select Whether or not a user is logged on.		

🛐 Create Package and Prog	ram Wizard	×
Standard Progra	m	
Package Program Type Standard Program	Specify information	n about this standard program
Requirements	Name:	SVM Scan
Summary Progress Completion	Command line: Startup folder: Run: Program can run: Run mode: Allow users to view ar	SVMScan.exe -c -v c:\windows\temp\svmscan.log       Browse         Hidden          Whether or not a user is logged on          Run with administrative rights          ad interact with the program installation
	Drive mode:	Runs with UNC name  V
		< Previous Next > Summary Cancel

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

Create Package and Progra	am Wizard	×
Requirements		
Package Program Type Standard Program Requirements Summary Progress Completion	Specify the requirements for this standard program  Run another program first Package: Program: Number of this program first Platform requirements Number of this program can run on any platform This program can run on any platform All Windows RT 8.1 All Windows RT 8.1 All Windows 10 (32-bit) All Windows 10 (64-bit) All Windows 10 (64-bit) All Windows 8.1 (64-bit) All Windows 8.1 (64-bit) Windows 8.1 (64-bit) All Windows 8.1 (64-bit) Windows 8.1 (64-bit) How Senbedded 8.1 Industry (64-bit) Windows Embedded 8.1 Industry (64-bit)	
	Estimated disk space: Maximum allowed run time (minutes): 30 <pre></pre>	el

- **8.** Finish the wizard.
- 9. Distribute the package to all Distribution Points or groups using the **Distribute Content** feature.



#### **Creating the Initial Scan and Weekly Reoccurring Scan**

To create the initial scan and the weekly reoccurring scan, perform the following steps.

Task	То	create the initial scan and the weekly reoccurring scan:
	1.	Select the Package and click <b>Deploy</b> on the ribbon.
	2.	On the General page, select the target collection and click Next.

- 3. On the **Content** page, verify that the content is distributed and click **Next**.
- 4. On the **Deployment Settings** page, ensure the purpose is Required and click **Next**.
- 5. On the **Scheduling** page, in the Assignment schedule click **New**. Schedule a scan for as soon as possible and create a weekly scanning schedule. Also configure the Rerun behavior deployment to **Always rerun program**.

中 Deploy Software Wizard					×
Scheduling					
General Content Deployment Settings Scheduling User Experience	Specify the schedul This program will be availab later time below. For require	e for this deployment le as soon as it has been distribu d applications, specify the assign	ted to the content so ment schedule.	ervers unless it is sch	reduled for a
Summary Progress Completion	Schedule when this dep         11/17/2017         Schedule when this dep         11/17/2017         ✓         Assignment schedule:         As soon as possible         Occurs every 1 weeks on	loyment will become available: 10:01 AM	UTC New D2 AM	Edit	Delete
	Rerun behavior:	Always rerun program	Next >	Summary	Cancel

 $\mathbf{V}$ 

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

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

🔶 Deploy Software Wizard		×
Distribution Point	z	
General Content Deployment Settings	Specify how to run the content for this program according to the type of bounda the client is connected to	iry
Scheduling	Select the deployment option to use when a client uses a distribution point from a current boundary group.	
Distribution Points	Deployment options:	
Summary	Download content from distribution point and run locally	•
Progress Completion	Select the deployment option to use when a client uses a distribution point from a neighbor boundary group or the default site boundary group.	
	Deployment options:	_
	Download content from distribution point and run locally          This option allows clients that use Windows BranchCache to download content from on-premises distribution points. Content downloads from cloud-based distribution points can always be shared by clients that use Windows BranchCache.         Allow clients to share content with other clients on the same subnet         Allow clients to use distribution points from the default site boundary group          Next >         Summary       Cancel	•

8. Finish the wizard.

You can now monitor the scanning results from the Software Vulnerability Research console. To stagger the scanning of multiple machines within a system, see Randomize the Agent Scan Schedule.

#### **Randomize the Agent Scan Schedule**

To set up a random scan schedule to stagger the scanning of multiple machines within a system, the following command line applies to all platforms:

SVMScan.exe -c -si <scan interval upper limit>

"si" represents the scan interval, and the scan interval's upper limit can be set up by the number of minutes.

For example, SVMScan.exe -c -si 50 would mean that the scanning agent will start scanning after a delay of random minutes, which could be from 1 to 50 minutes.

### Deploy a Windows Agent through Microsoft's Windows Server Update Services (WSUS)

When you deploy the Software Vulnerability Research Windows Agent through Microsoft's WSUS, the Windows Agent is installed on machines that report into WSUS, is scheduled to run as a service, and reports results back daily.

#### To deploy a Windows Agent through WSUS:

Task

- 1. If not already done, install and configure the Software Distribution Daemon for Windows. See Daemon Deployment and Install the Daemon.
- To view the Daemon's status page, go to Settings > Assessment > Update Servers & Daemon. After you click a Daemon, select one of the following options: More Info, Schedule Refresh, View Servers & Groups, Deploy Daemon, Delete Daemon, and Disable Daemon.

W8		Available		2018-09-05		2018-11-02
	More Info	Schedule Refresh	View Servers & Groups	Deploy Agent	Delete Daemon	Disable Daemon
			He Page 1	of 1 🕨 🔛		

• Select the **More Info** option to see Daemon information like the screen capture below. The **Last Connected** time stamp confirms whether the Daemon has reported recently, which is usually an indicator for good health. To sign packages externally, click **Sign Packages manually**. By default, it is set to **Automatic**.



- Select **View Servers & Groups** to display the Software Vulnerability Research instance your Daemon has been integrated with.
- **3.** To publish an Agent Deployment package to WSUS and to select the server and corresponding computer groups it maintains, select **Deploy Agent**.



In theory and practice, you can have multiple Daemons set up in multiple networks connected to multiple deployment servers. You can also select your package to be published to multiple deployment servers simultaneously in a centralized fashion.

## **Daemon Deployment**

The Software Distribution Daemon has to be installed and configured to publish patches (see Patching) as software updates to WSUS. It runs as a background service with no user interaction. It doesn't have to be installed on the WSUS server, but the host must be the exact same operating system version and patch level. For details, see the Daemon Software Requirements.

The account that runs the Daemon must have:

- Run-as Service privileges
- Windows Server Update Services Administrator privileges

This section details the following daemon deployment activities:

- Install the Daemon
- Add a Digital Certificate to Windows Server Update Services (WSUS)
- Create a Group Policy to Deploy Your Certificate

For additional Windows Server Update Services (WSUS) and daemon information, see Update Servers & Daemon.

### **Install the Daemon**

To install the daemon, perform the following steps.

#### Task To install the daemon:

- 1. Log in to https://app.flexerasoftware.com/login/?next=/
- 2. In the Settings module, go to Assessment > Downloads. For details see, Downloads.
- 3. Download the Software Distribution Daemon for Windows.

```
Software Distribution Daemon for Windows:
Version: 8.0.344
Download: SVMDaemonInstall.msi
Checksum (sha256): fa<sup>lm</sup>a2966898a2f897ccfc318c4e49cd12a1bf0de9b9c4adee5ef7e722eb886
```

- 4. Identify the machine to host the SVM Daemon. This machine must have access to your company's Windows Server Update Services (WSUS) server and must have the Windows Remote Server Administration Tools installed. The daemon runs in the background of this machine and acts as the host to receive patch data from the Software Vulnerability Research web server and to deploy the patches to your company's WSUS server.
- 5. Run the Installer.
- 6. Enter the server name, scheme, port, and credentials to your WSUS server.

😹 Software Vulnerability Manager Daemon - InstallShield Wizard	$\times$
Ready to Install the Program The wizard is ready to begin installation.	P.
Click Install to begin the installation.	
Windows Server Updates Services connection	
Server:	
Scheme: https v Port: 8531	
User Name:	
Password:	
InstallShield	
< Back	incel

#### 7. Click Install.

**8.** After the daemon is installed (wait about 10 minutes), you should see the daemon appear in the Software Vulnerability Research web server.

Settings > Assess	ment > Update Servers & Dae	mon							
Account 🗸	User Management 👻	Vulnera	bility Management 👻	Workflow Management	•	Assessment -	API 👻	Logs 🗸	
Name			Hostname		Status	5	Created		Last connected
					Availa	ble	2017-05-11		2017-05-12
					Availa	ble	2017-11-04		2018-05-08
		More Info	Schedule Refresh	View Servers & Groups	Deplo	oy Agent Delete	Daemon	Disable Daemon	

**9.** The best way to test to ensure the daemon is communicating correctly is to click **View Servers & Groups.** You should see a list of computers your WSUS server can talk to.

	More Info	Schedule Refresh	View Servers & Groups	Deploy Agent
_	10/11	SO4OEWAD8ME		Available
Daemon	#7 Servers			×
v 🖵		details		
~ =	All Computers			
	🗎 Unassigne	d Computers		
	Windows	10		
	Windows	7		
	Windows	<sup>8.1</sup>		
		Wir	ndows 8.1	

At this point, the daemon is configured. Before you can deploy patches, you must Add a Digital Certificate to Windows Server Update Services (WSUS), and then ensure that certificate is trusted by all machines you wish to deploy patches to.

# Add a Digital Certificate to Windows Server Update Services (WSUS)

Before you can deploy third-party patches in WSUS, you must prepare the WSUS server.

Task	То	add a Digital Certificate to WSUS:			
	1.	Create the following Registry Key:			
		Windows Registry Editor Version 5.00			
		[HKEY LOCAL MACHINE\SOFTWARE\Microsoft\U	pdate Services\Server\Set	tupl	
		"EnableSelfSignedCertificates"=dword:000	00001		
		📑 Registry Editor			
		📑 Registry Editor File Edit View Favorites Help			
		Registry Editor File Edit View Favorites Help Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Update Services\Server\Setu	p		

2. Add a Code Signing Digital Certificate to WSUS.

You have two options:

- Add a Code Signing Digital Certificate you already have to WSUS
- Have the Daemon generate a new code signing certificate

#### Add a Code Signing Digital Certificate you already have to WSUS

Open a command prompt and enter (replace <pfxFile> with a path to your pfx file and replace [password] with the pfx file password):

cd "c:\Program Files\Flexera Software\SVM Daemon"
svmpd.exe UseCert <pfxFile> [password]

#### Have the Daemon generate a new code signing certificate

Open a command prompt and enter:

cd "c:\Program Files\Flexera Software\SVM Daemon"
svmpd.exe NewCert

Once you have added a certificate, you need to deploy the certificate to machines that will receive the patches (they need to trust the patched from WSUS). See the next topic for this.

### **Create a Group Policy to Deploy Your Certificate**

This section describes how to create a Group Policy Object (GPO) for WSUS by using the Group Policy Management console. Once the GPO is created and linked to the correct Organizational Unit (OU), the computers in that OU will download the WSUS publisher self-signed certificate and Windows settings so that third-party updates can be downloaded correctly.

#### To create a Group Policy Object (GPO):

Ê

Task

- 1. Connect to the WSUS server and click Next.
- 2. When the "Export Signing Certificate" pop-up appears, click OK to save certificates to your documents folder.
- 3. Launch the Group Policy Management Console on your Domain Controller.
- 4. Navigate to Group Policy Management > Forest > Domains > Organizational Unit.
- Right-click the Organizational Unit > Create a GPO in this domain, and Link it here > Name the GPO such as "SVM-WSUS" or as per your policy.
- 6. Right-click the GPO and click Edit.
- 7. Navigate to Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies.
- **8.** Import the previously exported "wsuskey.cer" Certificate in the "Trusted Root Certification Authorities" and "Trusted Publishers" Folders.



- 9. Navigate to Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Update.
- **10.** Double-click the Windows Update Folder.
- **11.** Double-click **Specify Intranet Microsoft update service location** and change the Settings to **Enabled**. Specify your WSUS server address on **Set the intranet update service for detecting updates** and click **Apply**.

Note • This setting should only be changed if you are using WSUS. Don't configure this setting if you are using SCCM).

If you have another GPO which points your machines to the correct WSUS server, then re-specifying WSUS is not required.

Speci	fy intranet Microsoft	update service locat	ion		x
Specify intranet Microsoft update s	ervice location	Previous Setting	Next Setting	]	
Not Configured Comment:     Enabled     Disabled     Supported on:	At least Windows XP Prr excluding Windows RT	ofessional Service Pack 1 o	r Windows 2000 Se	rvice Pack 3	< > < >
Options:	Help:				
Set the intranet update service for dete updates: Set the intranet statistics server: (example: http://intranetUpd01)	cting Specifi Udd#t a a ni search yourn To use server for use server insteau uddat organi and it	es an intranet server to ho . You can then use this up computes on your netwe titing lets you specify a ser- netrain update service. Ihn this service for updates the this service of updates the this setting, you must set from which the Automatif the Automatif action updates and the service actions updates, and the service actions updates, and the server. Tabus is set to Enabled, the ts to the specified intrane I windows Update, to a s. Enabling this setting me zation don't have to go this yees you the opportunity?	st updates from Mi date service to aut ork. wer on your network Automatic Updat at apply to the com two servername va Updates client de trot owhich update our can set both value Automatic Update the Microsoft update arch for and down cans that end users rough a firewall to test updates before to test updates before to t	icrosoft tomatically rk to function es client will mputers on alues: the tects and ed ues to be the es client : in your get updates in your	e e
	and it	gives you the opportunity	to test updates bef	fore deployin	ng . Iy

12. Double-click Allow signed updates from an intranet Microsoft update service location and change the Settings to Enabled.

Allow signed upd	lates from an intra	net Microsoft update service location Previous Setting Next Setting	
Not Configured     Fnahled	Comment:		~
Dirabled			v
O bisabled	Supported on:	At least Windows Server 2003 operating systems or Windows XP Professional with SP1, excluding Windows RT	
ptions:		Help:	
		This policy setting allows you to manage whether Automatic Updates accepts updates aigned by enblies other than Microsoft when the update is found on an intranet Microsoft update service location. If you enable this policy setting, Automatic Updates accepts updates received through an intranet Microsoft update service location, if they are signed by a certificate found in the "Trusted Publishers" certificate store of the local computer. If you disable or do not configure this policy setting, updates from an intranet Microsoft update service location must be signed by Microsoft. Note: Updates from a service other than an intranet Microsoft update service must always be signed by Microsoft and are not affected by this policy sitting. Note: This policy is not supported on Windows RT. Setting this policy will not have any effect on Windows RT PCs.	
		OK Cancel Apply	

**13.** Click **Apply > OK** and close the GPO editor.

Computers will download the Policy after the next policy refresh interval or reboot. You can force the policy to apply by running the command:

#### gpupate /force

Sometimes it may take several hours for the policy to actually propagate. You can verify that the GPO is being applied to the machine by checking to see if the certificates have been added to the appropriate certificate stores on any given machine.

If the GPO has not been applied yet, or it is not being applied to the machine in question, then you will receive an error (0x800b0109) when deploying third-party updates.

# **Smart Group Configuration**

Smart Groups are powerful reporting tools that can be customized to deliver a valuable overview of the software vulnerability exposure of your clients, networks, and products. You can create a Smart Group in the **Assessment** module of Software Vulnerability Research.

This section includes the following Smart Group topics:

- Conditions and Logic Operators
- Simple Smart Groups
- Advanced Smart Groups
- Additional Smart Group Information

### **Conditions and Logic Operators**

Smart Groups can be saved when there is one or more conditions configured with their corresponding logic operators and values. You can create as many Smart Groups as you need, as long as you don't repeat the same condition and logic combination twice within a single smart group.

Smart Group configuration consists of 21 conditions, which are sorted into three primary categories: Device, Product, and Advisory. Many of the conditions include one or more logic operators, which allow you to further customize your use cases.

Conditions:	Conditions:	Conditions:
Device Conditions	Device Conditions	Device Conditions
Select Device Condition	<ul> <li>Select Device Condition</li> </ul>	✓ Select Device Condition
Device Platform Device Name In	Product Version Conditions	Product Version Conditions
Device Secure Type	Select Product Condition	▲ Select Product Condition ▼
Device System Score Device Name	Product Secure Type Product Version Name	Advisory Conditions
Device Active Directory Operating System In Device Last Scan Date	Product Version In Product Version Not In Parent Product In Parent Product Not In Product Vendor In	Select Advisory Condition       Advisory SAID       Advisory Title contains       Advisory Criticality       Advisory Where       Advisory Solution Status
		Advisory Zero Day Advisory CVE(s) Advisory CVSS Score Advisory Initial Release Date Advisory Current Release Date

### Simple Smart Groups

Before creating a Simple Smart Group, you should consider the scenario you want to report on and know the particular conditions of your use case. For example, insecure status, product name, network location, and attack vector are all conditions that can be used on its own to report a great deal of valuable information.

Smart Groups that contain a single condition are simple by design, but they can deliver great insight on devices and network, products and vulnerabilities.

The following are Simple Smart Group examples that contain one condition:

#### Table 3-2 • Simple Smart Group Examples

Smart Group	Condition
Show all Insecure Products or EOL	Product Secure Status = Insecure / EOL
Show Windows devices managed by me	Device Platform = Windows
Monitor a specific program version	Product Version Name = Flash 31.x
See sum of devices and programs under a specific organizational unit (OU)	Device Active Directory = DC=Clients, DC=domain, DC=com
See all vulnerable software from a Remote attack vector	Advisory Where = From Remote

### **Advanced Smart Groups**

Advanced Smart Groups usually represent a use case scenario with multiple logic conditions being true.

If you take the five Simple Smart Groups illustrated above and configure all of them under one single Smart Group, you will achieve an Advanced Smart Group.

For example, the Advanced Smart Group shown in the screen shot below will report on Insecure Flash 31.x with attack vector From Remote on PCs in the Workstations OU of my domain.

Name						
Insecure Flash 31.x at Workstati	ons on Windows fro	m Remote				
Priority						
High						
Conditions:						
Device Conditions						
Device Active Directory	-			Desktops @Select Active Directory		×
Device Platform	•			Windows	-	×
Product Version Conditions						
Product Secure Type	-			Insecure	-	×
Product Version Name	-	contains	•	Rash 31.x		×
Advisory Conditions						
Advisory Where	-			From remote	<b>-</b> -	×

The more specific you are in the search you perform, the more specific the results will be that you get back from the vulnerability database of your account, which manages your Smart Group queries.

### **Additional Smart Group Information**

For additional Smart Group information, see:

- Smart Group Selection Order
- Create a Smart Group
- Create a Smart Groups Report

## **Workflow Management Rules**

In Software Vulnerability Research under **Settings > Workflow Management > Rules**, you can create rules that partially or fully automate workflow.

Rules can only be created by an Administrator and must contain at a minimum one trigger and one action. For a list of triggers and actions, see Rule Channels, Triggers, and Actions. If needed, you can configure many different options into one rule.

This section includes the following Workflow Management Rule topics:

- Create a Workflow Rule Overview
- Rule Triggers
- Patch Rule Actions
- Notification Actions

- Default Workflow Rules
- Custom Workflow Rules

### Create a Workflow Rule - Overview

To create a workflow rule, perform the following steps.

Task

#### To create a Workflow Rule:

- 1. Click 🌁 to create a new Workflow Rule.
- 2. Enter the Rule name and click Choose Rule Trigger. For details, see Rule Triggers.
- 3. Select the channel and trigger from the drop-down lists and click **Save**. An **Add Action** icon will appear. For an example, see Patch Rule Actions.
- 4. Select the action to be taken from the drop-down list when the rule is triggered and click Save. Add any additional actions required and save the rule.
- 5. Select the appropriate rule Notification. If you choose to send an email or SMS, you can select multiple users or broadcast groups for the email or SMS notification by clicking the appropriate user names or broadcast groups. A check mark will appear next to the selected users or broadcast groups. The selected user names will appear in the Users field; the selected broadcast groups will appear in the Broadcast to Groups field. For details, see Notification Actions.
- 6. Click Edit to change and to Enable or Disable a rule.

### **Rule Triggers**

Within a given rule, select one of the following **Rule Triggers**: Advisory, Analytics, Patch, Policy, Release, Ticketing, and User management.

Choose Rule Trigger	
Patch	*
Advisory	
Analytics	
Patch	~
Policy	
Release	
Ticketing	
User	
Cancel	

For example, if you select Patch as the subject of your desired workflow, you must choose one patch rule trigger:

Table	3-3•	Patch	Rule	Trigger	Option
Table 3	3-3•	Patch	Rule	Trigger	Option

Option 1: Patch ready for manual signing	Option 2: Patch available with template, affecting my environment = Yes, Not Critical or Above	Option 3: Patch available without template, affecting my environment = Yes, Not Critical or Above
Patch available,	Choose Rule Trigger	Choose Rule Trigger
Choose Rule Trigger	Patch available, with template	Patch available, without template
Patch -	Yes 🔹	Yes 👻
Package ready for manual signing	Not Critical and Above	Not Critical and Above 👻
Package ready for manual signing 🗸	Save	Save
Patch available, without template Patch available, with template	Cancel	Cancel

### **Patch Rule Actions**

After selecting the appropriate Patch Rule trigger option, you can create Patch Rule actions such as Patch - Create Packages and Patch - Publish to deployment servers.

Table 3-4 • Patch Rule Action Options



### **Notification Actions**

You can create several Notification Actions to communicate your rules using **Email**, **SMS**, **Notify**, **Create ticket**, and **Call service provider.** 

Table 3-5 • Notification Actions

Email the user with custom message and broadcast the email to members of a particular group	SMS the user with custom message and broadcast the text to members of a particular group	Notify the user with custom message and broadcast the email to members of a particular group	Create ticket with status Waiting for handling	Call Service Provider
Choose Action Email Final Fina	Choose Action SUS SUS Action Addition SUS Action Addition Action	Choose Action Nooly • Next Step Build Package relarvator • Yes • Patch Management Admins • Marning • Save Delete Cancel	Choose Action Greate ticket Handled Irrelevant Open Walting Delete Cancel	+       Add action         Choose Action       Image: Street action         Image: Street action       Image: Street action         Severa Method       Image: Street action         Image: Cancel       Image: Street action         Mote - This option       requires prior         integration       configuration with the         service provider.       Image: Street action

### **Default Workflow Rules**

Software Vulnerability Research includes default workflow rules, which relate to ticketing, advisories, patching, and more. When selecting workflow rules, you should use either default workflow rules or custom workflow rules. Custom rules cancel out default rules, and two custom rules with identical triggers and actions cancel each other out.

The screen shot below provides two default patch rules:

- The first rule detects Patches without a template, and it sends an internal notification and an Email.
- The second rule detects Patches with a configured template, creates the package, and sends an internal notification and an Email.

Patch avail	able no pro	ofile notifica	tion 🦸									
	<b>\\$</b> *	Patch available, without template	>	Â	Notify	+	$\bowtie$	Email				
Patch avail	' atch available with custom profile 💰											
	<b>‡</b> *	Patch available, with template	>	<i>₅</i> ∳3	Patch - Create packages	+	Â	Notify	+	$\bowtie$	Email	

The default workflow rules should be used as a template. It's good practice to disable the default workflow rules to make custom workflow rules with the same settings. Custom rules cancel out default rules, which might cause unforeseen issues. For additional information, see Default Workflow Rule Examples.

### **Custom Workflow Rules**

A Custom Workflow Rule is any workflow rule that was built from scratch by the user. It might be a simple workflow rule or a more complex one.

The custom workflow rule screen shot below includes:

- 1. A patch with a template
- 2. Creating an internal notification in Software Vulnerability Research
- 3. Creating a patch package
- 4. Single user email notification
- 5. Publishing the patch package
- 6. Creating a notification to the single user and to the Patch Management Admins user group
- 7. Creating a ticket and marking it **Handled** because this workflow rule automatically handled the package from its release phase to its publishing to the WSUS/System Center Configuration Manager.



Note • This custom workflow rule will cancel out all default workflows labeled Patch available with Template.

# Patching

Patching through the Software Vulnerability Research can be performed as a manual, semi-automated, or fully automated process.

This section describes the following patching topics:

- System Requirements for Patching
- Packages
- Patch Template
- Build Package
- Package Deployment

Chapter 3 Software Vulnerability Research Quick Start Guide Patching

### System Requirements for Patching

Before you start patching, allow your system to access http://crl3.digicert.com and http://crl4.digicert.com on the Software Vulnerability Research host machine to create patching packages.

Ì

**Important** • If your organization allows specific URL access to the Internet, and you are having problems downloading or verifying a patch, ensure the CRLs are allowed; examine the logs to identify the download's source, and examine the certificate at that address for its CRL distribution points.

### Packages

You can create packages without scanning your network because Flexera has provided several default package templates that are ready to be built into physical update packages on the fly.

It's a best practice to scan your hosts before creating any packages. After clicking the Patching module's blue filter icon, the left-most filter allows you to filter only patches **Affecting Your Environment**. There are other patching filters under the blue filter button.

Patch Library Templa	tes Packages Deployment Tickets					
Browsing 1-20 of 73 patches 🦸						<b>y</b> ±
Yes	* OE	Product name	Vendor name	Secureversion	SND	
Yes No	~				Apply	Reset
				Elter		Delete

# Task

#### To successfully create and deploy third-party packages:

- **1.** Install and configure the Software Distribution Daemon for Windows. See Deploy the Windows Agent Application through Microsoft's System Center Configuration Manager (SCCM).
- 2. Configure Workflow Rules for Patching and automate the patching process as much as you want or as much as the process requires.
  - For automatic patching workflow rule examples, see Rule Triggers, Patch Rule Actions, and Notification Actions.
  - For a manual patching workflow rule, create the following steps: Create Template > Build Package > Create Deployment > Confirm Daemon Publishing.

For further information regarding package deployment filters, package deployment details, and package updates see Patch Library, Packages, and Deployment.

### **Patch Template**

To create a patch template, perform the following steps.

#### To create a patch template:

Ŷ

Task

1. After applying the filter to view only the patches required in your environment as described in Packages, select the most important application to patch. Then select Create template.

A blank Patch Template window appears with fields to enter the features and configuration settings of an update package.

- 2. Enter the Template name and (optional) Description.
- 3. Select the **Package configuration** options from the drop-down lists and click **Save.** A sample patch template is shown below.



Note • The Package configuration options will vary depending on the Product you are creating a Patch template for.

Adobe Acrobat Reader DC	
Here you can give a description of the tem etc.	plate. For example, what it does, the contents, usage,
Description	
Package configuration	
Architecture	
32-bit/64-bit	•
Language settings	
English (US)	•
Default	
Default Protected View Settings	
Default Protected View Settings Default	•
Default Protected View Settings Default Clean Install Options	
Default Protected View Settings Default Clean Install Options Perform a clean installation	
Default Protected View Settings Default Clean Install Options Perform a clean installation Install/Update Options	•
Default Protected View Settings Default Clean Install Options Perform a clean installation Install/Update Options Disable Automatic Updates	•
Default Protected View Settings Default Clean Install Options Perform a clean installation Install/Update Options Disable Automatic Updates Remove Desktop Shortcut	、 、 、
Default Protected View Settings Default Clean Install Options Perform a clean installation Install/Update Options Disable Automatic Updates Disable Automatic Updates	•
Default Protected View Settings Default Clean Install Options Perform a clean installation Install/Update Options Disable Automatic Updates Prevent collection of anonymous usage set	statistics
Default Protected View Settings Default Clean Install Options Perform a clean installation Install/Update Options Disable Automatic Updates Remove Desktop Shortcut Disable Automatic Updates Prevent collection of anonymous usage s Enable Enhanced Standalone Security	statistics
Default Protected View Settings Pefault Clean Install Options Perform a clean installation Install/Update Options Disable Automatic Updates Remove Desktop Shortcut Disable Automatic Updates Prevent collection of anonymous usage se Enable Enhanced Standalone Security Enable Enhanced Browser Security	statistics
Default Protected View Settings Default Clean Install Options Perform a clean installation Install/Update Options Disable Automatic Updates Remove Desktop Shortcut Disable Automatic Updates Prevent collection of anonymous usage s Enable Enhanced Standalone Security Enable Enhanced Browser Security Remove Purchase Acrobat menu item	statistics
Default Protected View Settings Default Clean Install Options Perform a clean installation Install/Update Options Disable Automatic Updates Remove Desktop Shortcut Disable Automatic Updates Prevent collection of anonymous usage : Enable Enhanced Standalone Security Enable Enhanced Browser Security Remove Purchase Acrobat menu item Disable messages about upgrading to Ac	statistics
Default Protected View Settings Default Clean Install Options Perform a clean installation Install/Update Options Install/Update Options Disable Automatic Updates Remove Desktop Shortcut Disable Automatic Updates Enable Enhanced Standalone Security Enable Enhanced Browser Security Remove Purchase Acrobat menu item Disable messages about upgrading to Ac Enable Printer Toner Saver	statistics

4. The Path information option allows users to create custom patch templates, which may be specified to account for multiple or non-standard installation paths to aid in detection of such applications. To create a custom patch template, click Add Path. When the Add Path Applicability Rule for Package window appears, manually enter the

custom installation path and click **Add Path**. To delete this path, click the red minus button. After entering the applicable **Path information**, click **Save**.

Path information			
PATHS			
%SystemRoot%\Test			-
Add Dath			
Add Path			
	Cancel	Save	

5. After creating a Patch Template, deploy the patch using a Build Package.

### **Build Package**

#### 

**Important** • To build and deploy a package, you must first download and install the Software Vulnerability Research Daemon on your Windows Software Update Server. For further information, see Daemon Deployment and Install the Daemon.

<ol> <li>Click a package in the <b>Patch Library</b> grid and select Build packages.</li> <li>Google 70 x</li> </ol>	
Google 70 x SA85678	
	Yes
View templates Create template Build packages	

Build packages - Macromedia Flash Player 8.x	×
Set your package name Macromedia Flash Player 8.x	
Select all templates for which you want packages to be built.	
M27_Macromedia Flash Player_ActiveX [YojanaY, 2018-03-27 15:26:47]	÷
Cancel Build	I

3. Publish the package to your environment using Package Deployment.

### **Package Deployment**

Template was created.

To publish the package to your environment, navigate to **Patching > Packages** in Software Vulnerability Research. To view package options other than deployment, see Packages.

#### To create deployment:

Ê

Task

- 1. Select Create Deployment. The Choose where to publish the patch(es) dialog box will open.
- 2. Select the servers or groups to publish the patch(es).

Choose where to publish the patch(es)	×											
Select the server(s) where you want to publish the patch to:												
✓ □ □ □ cm12sql details												
✓												
🔲 🚔 Unassigned Computers												
✓ □												
Server Details												
Name: cm12sql												
Type: WSUS												
Created: 2018-09-05 13:00:15												
ID: a2753492-04fd-4cd7-bab0-												
e2f6e39eb1e8												
Daemon: W8	view deployments											
	, view deployments.											
Cancel	ок											

3. Click OK.

After you create your deployments, it is up to your Daemon to come and collect the deployed packages. The Daemon connects to the Flexera Cloud about once every 10 minutes. However, the Daemon connection time might be extended if the Daemon experiences network issues.

### **Additional Patching Information**

For additional Patching information, see:

- Patching Tickets
- Manual Signatures

Chapter 3 Software Vulnerability Research Quick Start Guide Patching



The Dashboard is the default home page that provides you with an overview of vulnerability management processes and gives you access to your latest vulnerability intelligence and Advisories. The information is presented with the help of various widgets.

- Dashboard with Threat Intelligence Module
- Dashboard without Threat Intelligence Module

### **Dashboard with Threat Intelligence Module**

The below figure shows the Dashboard with the Threat Intelligence Module, the additional widget **Highest threat scores affecting your watch lists** get included in the main page.



**Note** • Please note the following:

- This add-on requires purchase of the Software Vulnerability Research Threat intelligence Module
- To purchase this module, contact your sales representative or contact us online at: https://www.flexera.com/about-us/ contact-us.html

shboard	ł												<u>9</u>
													+
Devices	Overviev	¥ ő		×	Highes	t threat scores affecting your watch lists $\sharp$			×	Devices	status - System score 🦸		
Average	e score			70	SAID	Title	Criticality	Threat	Release		100	0 4	
		Insecure		<u>15</u>	L —	Manager Manager Course 2018 (Managers 10.10 State		ouore	2010		50 - 79	10	
Devices		Secure		Q	<u>SA878</u>	Vulnerabilities	-	89	03-13		<su Unknown</su 	0	
		Total		15	<u>5A878</u>	Microsoft Windows Server 2019 Multiple Vulnerabilities		99	2019- 03-13		Not Calculated	0	
		Insecure		<u>91</u>		WinRAR ACE File Processing Directory Traversal			2019-				
Product		End-of-Life		<u>19</u>	<u>SA8/4</u>	Vulnerability		99	02-13				
Products		Secure		250	<u>SA848</u>	Avaya Call Management System (CMS) Multiple Vulnerabilities		99	2018- 08-22				
		Total		380					2018-				
		Insecure		12	<u>SA839</u>	37 Oracle Linux update for samba		00	08-28				
la at ari	itiaal adui	action officition your accusity of			SA830	Microsoft Windows Server 2012 / Windows RT 8.1 / 8.1 Multiple Vulnerabilities		99	2018- 05-09	Mostore	ualant income coffunct installations d		
MOST CH	itical advi	sories affecting your security #		^	SA830	Microsoft Windows Server 2008 / Windows 7 Multiple			2018-	Most pre	valent insecure software installations #		
Rank	SAID	Title	Installations	Criticality	Dovice	e efatue				Rank	Name	Installations	Patch
1	<u>SA86719</u>	Microsoft Internet Explorer Memory Corruption	2		Device	s status - Time since last scan g			•	1	Microsoft .NET Framework 4.x	<u>6</u>	No
2	\$494005	Microsoft Internet Evolution Multiple Vulnershillitien	1			0 - 7 days 13 8 - 14 days 1				2	WinSCP 5.x	<u>5</u>	Yes
•	6070904	Managadi MET Experience Cade Even dan Managhility	-	_		15 - 30 days 0 +31 days 1				з	GNU C Library (glibo) 2.x	4	No
	37110304	Microsoft Stell Pranework Gode Execution volnerability	2							4	Network Security Services (NSS) 3.x	4	No
•	<u>SA12977</u>	Microsoft Products Multiple vulnerabilities	4	_						6	Microsoft Internet Explorer 11.x	3	No
•	<u>SA70398</u>	Microsoft Internet Explorer Multiple Vulnerabilities	1							6	Microsoft Windows 10	3	No
8	<u>SA61803</u>	Microsoft Windows OLE Object Handling Two Arbitrary Code Execution Vulnerabilities	2							7	FreeType 2.x	3	No

Click 💶 to add the **Highest threat scores affecting your watch lists** widget and Save to save the changes you made.

Advisories released last year
Highest threat scores affecting your watch lists
Latest advisories
Latest advisories per watch list
Opened tickets pattern
Tickets split by status
Your latest assigned tickets

**Note** • Click the *i* icon to see more information about the widget.

#### **Dashboard Widget**

In additional to the features explained in the **Dashboard > Dashboard without Threat Intelligence >** Dashboard Widgets, the following widget is added:

• **Highest threat scores affecting your watch lists** - displays those advisories with the highest threat scores affecting the watch lists.

### **Dashboard without Threat Intelligence Module**

The below figure shows the Dashboard without the Threat Intelligence module.

	rd													?
														+ Sa
Device	s Overview	v i			×	Device	es status - Ti	me since last scan 🦸		×	Device	s status - System score 🦸		
Avera	ge score			68				0 - 7 days 17				100 1		
			Insecure	29				15-30 days 8				50 - 79 17		
Devic	es		Secure	1				i si daja si						
			Total	30										
			Insecure	59										
			End-of-Life	36										
Produ	icts		Secure	472										
			Total	567										
Most o	ritical advi	sories affecting you	r security 🦸		×	Latest	advisories a	ffecting your security 💈		×	Most p	revalent insecure software installations 🦸		3
Rank	SAID	Title		Installations	Criticality	Date	SAID	Title	Installations	Criticality	Rank	Name	Installations	Patch
1	<u>SA81412</u>	Adobe Flash Player Free Vulnerabilities	Multiple Use-After-	29		2018-03-07	<u>SA81927</u>	Google Chrome Multiple Vulnerabilities	22		1	Microsoft.NET Framework 4.x	<u>55</u>	No
		Microsoft Windows (	DLE Object Handling			2018-		Adobe Flash Player Multiple Use-After-			2	Microsoft XML Core Services (MSXML) 3.x	<u>24</u>	No
2	<u>SA61803</u>	Two Arbitrary Code I Vulnerabilities	Execution	<u>12</u>		02-28	<u>SA81412</u>	Free Vulnerabilities	<u>29</u>		3	Microsoft XML Core Services (MSXML) 6.x	24	No
		Microsoft Windows				2018- 02-28	SA81606	Adobe Reader / Acrobat Multiple Vulnerabilities	z		4	VLC Media Player 2.x	22	Yes
3	<u>SA55611</u>	Microsoft Windows InformationCardSigr ActiveX Control Cod	inHelper Class e Execution	1		2018- 02-28 2018-	<u>SA81606</u>	Adobe Reader / Acrobat Multiple Vulnerabilities Microsoft Windows Server 2012 /	Z	_	4	VLC Media Player 2.x FileZilla Server 0.x	22 19	<u>Yes</u> No
3	<u>SA55611</u>	Microsoft Windows InformationCardSign ActiveX Control Cod Vulnerability	inHelper Class e Execution	1	_	2018- 02-28 2018- 02-27	<u>SA81606</u> <u>SA77077</u>	Adobe Reader / Acrobat Multiple Vulnerabilities Microsoft Windows Server 2012 / Windows RT 5.1 / 8 Multiple Vulnerabilities	Z 1		4 5 6	VLC Media Player 2.x FileZilla Server 0.x Microsoft_NET Framework 3.x	22 19 16	<u>Yes</u> No No
3	<u>SA55611</u> <u>SA81927</u>	Microsoft Windows InformationCardSign ActiveX Control Cod Vulnerability Google Chrome Mul	inHelper Class e Execution tiple Vulnerabilities	1 22		2018- 02-28 2018- 02-27 2018- 02-27	<u>SA81606</u> <u>SA77077</u> <u>SA81778</u>	Adobe Reader / Acrobat Multiple Vulnerabilities Microsoft Windows Server 2012 / Windows RT 8.1 / 8 Multiple Vulnerabilities Wireshark Multiple Denial of Service	Z 1 1	 	4 5 6 7	VLC Media Player 2.x FileZilla Server 0.x Microsoft .NET Framework 3.x Microsoft Internet Explorer 11.x	22 19 16 12	Yes No No No
3 4 5	<u>SA55611</u> <u>SA81927</u> <u>SA81605</u>	Microsoft Windows InformationCardSign ActiveX Control Cod Vulnerability Google Chrome Mul Adobe Reader / Acro Vulnerabilities	inHelper Class e Execution tiple Vulnerabilities obat Multiple	1 22 Z	 	2018- 02-28 2018- 02-27 2018- 02-26	<u>SA81606</u> <u>SA77077</u> <u>SA81778</u>	Adobe Reader / Acrobat Multiple Vulnerabilities Microsoft Windows Server 2012 / Windows RT 8.1 / 8 Multiple Vulnerabilities Wireshark Multiple Denial of Service Vulnerabilities	Z 1 1		4 5 6 7 8	VLC Media Player 2.x FileZilla Server 0.x Microsoft JNET Framework 3.x Microsoft Internet Explorer 11.x Wireshark 2.x	22 19 16 12 11	Yes No No No

Click 💶 to add widgets (when available) and Save to save the changes you made.

🖌 🔶 🛨
Advisories released last year
Latest advisories
Latest advisories per watch list
Opened tickets pattern
Open tickets split by advisory criticality
Tickets split by status
Your latest assigned tickets



**Note** • Click the *i* icon to see more information about the widget.

#### **Dashboard Widgets**

The Dashboard widgets on the main page includes the following:

#### Table 4-1 • Dashboard Widgets

Item	Description
Devices Overview	Displays an overview of the average security score (current verses last week) for the Devices, Products and Operating Systems within your environment.
Devices status - Time since last scan	Displays the number of devices that have been scanned within a given time frame.
Devices status - System Score	Displays how your devices rank based on the computed system score.

#### Table 4-1 • Dashboard Widgets

Item	Description					
Most critical advisories affecting your security	Displays the most critical Advisories based on all software detected within your environment.					
Latest advisories affecting your security	Displays a complete list of the latest Advisories released by Secunia. Click a Secunia Advisory ID (SAID) to view the complete advisory details, including (where applicable) the Creation Date, Criticality (Severity Rating), Impact (Consequence), Where (Attack Vector), Solution Status, Secunia CVSS (Common Vulnerability Scoring System), CVE References, Affected software and Advisory Description, Solution, References and Changelog.					
Latest advisories affecting your security	Displays the most recent Advisories affecting software from your Devices.					
Latest advisories per watch list	Displays the most recent Advisories released by Secunia based on your configured Watch Lists. Click a Secunia Advisory ID (SAID) to view the complete advisory details, including (where applicable) the Creation Date, Criticality, Impact, Where, Solution Status, Secunia CVSS Scores, CVE references, Affected software and Advisory Description, Solution, References and Changelog.					
Advisories released last year	Displays a month-by-month graph of the total number of advisories released by Secunia over the previous 12 months.					
Your latest assigned tickets	Displays the latest tickets that have been assigned to you. Click a Secunia Advisory ID (SAID) to view the complete advisory details, including (where applicable) the Creation Date, Criticality, Impact, Where, Solution Status, Secunia CVSS Scores, CVE references, Affected software and Advisory Description, Solution, References and Changelog.					
Open tickets split by advisory criticality	Displays a color coded pie chart of the criticality of all open tickets assigned to you. Hover over the criticality legend (Low, Medium, High and Urgent) to display a tooltip with the total percentage of tickets applicable to the ticket criticality.					
Tickets split by status	Displays a color coded pie chart of the statistics of all tickets assigned to you. Hover over the ticket type legend (Open, Waiting, Handled and Irrelevant) to display a tooltip with the total percentage of tickets applicable to the ticket type.					
Open tickets pattern	Displays a trend line of the number of tickets that have been created based on your configured Watch Lists. The trend line applies to the status of all ticket types (Open, Waiting, Handled and Irrelevant).					
Most prevalent EOL software installations	Displays the list of End-of-Life (EOL) software installations that no longer provide security fixes, which can lead to insufficient firewall and anti-virus protection. Please note that Flexera's definition of EOL software may differ from a software vendor's.					
Most prevalent insecure software installations	Displays the most insecure software based on the number of Devices within your environment.					

#### Table 4-1 • Dashboard Widgets

Item	Description			
Latest available patches	Displays the latest available patches based on your scan results.			

Chapter 4 Dashboard



Notifications provide detailed information about alerts you have received and any required actions. The number in the yellow bubble signifies the number of unread notifications.



*Important* • You shall not, unless expressly authorized in writing by Flexera, reproduce, distribute, display, sell, publish, broadcast, or circulate any information or other material provided by Flexera and/or any information or other material provided as a result of the Product(s) (such as advisories and security updates) to any third-party, including Customer's affiliates, or any unauthorized Recipient, nor make such information or material available for any such use. The Product(s) may only be used by the legal entity that has purchased a license, and no shared use with any other legal entity (including Customer's affiliates) is allowed.

Notifications									<b>8</b> - 1
Browsing 1-20 of 1478 notifications 🦸									Y Ł Actions -
Search by keyword	Critica	lity 💌	Status	▼ From	=	То	=	Туре	-
								Apply	Reset
						Filter	-	Save	Delete
Created	Туре	Notification							
🖌 🔤 🃋 4/23/2018 9:10 AM	🌢 Alert	Advisory <u>SA81270</u> for watch list <u>t</u>	estMarch15 was updated. Message gene	erated by `Notify on advisory up	dates`.				

E Task

#### To view notifications:

- 1. Open the Notifications page.
- 2. Click 🔽 to filter the notifications by Search by keyword, Criticality, Status, From and To dates, and Type.
- 3. Click the Apply or Reset buttons to apply or reset the filters.

- 4. Click the **Save** or **Delete** buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.
- 5. Click a Secunia Advisory ID (SAID), ticket number and so on to view detailed information related to the item.
- 6. Click the Notification check boxes to select from the available options in the Actions drop-down list.
- 7. Click do export the results to a CSV file.

#### **Setting Rules for Notifications**

Your Administrator should set Rules to enable you to receive notifications, as shown in the following graphic. Please refer to Workflow Management > Rules for further information.





# **Vulnerability Manager**

Edition • The Vulnerability Manager module is not available for Software Vulnerability Research - Assessment Only.

You can use the Vulnerability Manager pages to manage watch lists, advisories, and ticketing and approve advisories.

Overview

凤

- Watch Lists & Advisories
- Ticketing in Vulnerability Manager
- Approve Advisories

### **Overview**

Use the Vulnerability Manager pages to manage the Vulnerability Intelligence associated with your account. You can:

- Create, import and view Watch Lists.
- Create and view Shared Watch Lists
- View and create tickets for Historic Advisories for all Watch Lists
- View and create tickets for Product Advisories for all products
- View, edit and Create Tickets in Vulnerability Manager
- View and approve Advisories associated with each Watch List
- Send Notifications to alert users via Email/SMS
- Edit, share or delete Watch Lists

Click an item in the grid to select from the available options.

# Watch Lists & Advisories

Select Watch Lists from the Watch Lists & Advisories drop-down menu to view, create and configure multiple Watch Lists, each with their own unique set of Vendors (all products from the vendor), Products (all versions) and specific Product Versions that you want to receive vulnerability alerts and track Advisories for.

Select Historic Advisories from the Watch Lists & Advisories drop-down menu to view a comprehensive and thorough collection of reports and statistics about all Advisories affecting a specific Watch List.

After adding a Watch List, it is recommended that you view the **Historic Advisories** page to confirm that the vendor has addressed all the relevant issues in the software.

### Watch Lists

You can define which vendors, products, and product versions you want to receive vulnerability alerts and track Advisories for.

The monitored Vendors (all products from the vendor), Products (all versions) and specific Product Versions are organized into Watch Lists. Each Watch List can have different notification levels, can be grouped into Watch List Groups and can be shared with all Users and User Groups associated with your account. There is no limit to the number of Watch List Groups that can be created.

For details, see:

- View Watch Lists
- Create Watch Lists
- Edit Watch Lists
- Import a New Watch List
- Import an Updated Watch List

The Watch List **Enforced by admin** column with a Yes or No response relates to the sharing of Watch Lists. For details see Shared Watch Lists. By default, the notifications (such as an email or SMS) generated by a Watch List are sent only to the Watch List creator when a new advisory is released that matches a Watch List. If Watch List creators wish to share their asset list with other users from their organization, the Watch List is then shared based on the following options:

- If an administrator shares a Watch List, he or she has the option to enforce the targeted users to receive the notification, with the selected subscription levels. All targeted users will then receive the notification, as it is mandatory. The targeted users can't unsubscribe from that Watch List. This will result in a **Yes** response in the **Enforced by admin** column.
- If a non-administrator shares a Watch List or an administrator does not select the Watch List's "enforce" subscription option, the targeted users can decide whether or not to subscribe to the shared Watch List. The targeted users can manually subscribe to the Watch List, and notifications will not be sent to them before they manually subscribe to the Watch List page with their preferred subscription levels. This will result in a No response in the Enforced by admin column.
| Vulnerability Manager > Watch Li  | sts & Advisori | es > Watch | Lists      |                     |           |         |                         |          |                     |           |       |            |                        |                                 |                               | 0-1                  |
|-----------------------------------|----------------|------------|------------|---------------------|-----------|---------|-------------------------|----------|---------------------|-----------|-------|------------|------------------------|---------------------------------|-------------------------------|----------------------|
| Watch Lists & Advisories +        | Ticketing      | Appr       | ove Adviso | ories               |           |         |                         |          |                     |           |       |            |                        |                                 |                               |                      |
| Browsing 1-20 of 40 watch lists 🦸 |                |            |            |                     |           |         |                         |          |                     |           |       |            |                        |                                 | 7                             | 3 <mark>+</mark> ± - |
| Name                              | G              | roup       |            | •                   | Enabled   |         |                         | -        | Approval nee        | eded      |       | -          | Created by             | •                               | Apply                         | Reset                |
|                                   |                |            |            |                     |           |         |                         |          |                     |           |       |            | Filter                 | •                               | Save                          | Delete               |
| Watch List Name                   | Group          | Enabled    | Receive    | Product<br>versions | Products  | Vendors | End of life<br>warnings | Adv      | sories need<br>oval | ls<br>sha | ared  | Created by | Ticket threshold       | Notification level for<br>email | Notification level for<br>SMS | Enforced by admin    |
| ×                                 | -              | Yes        | No         | <u>0</u>            | Q         | 2       | 0                       | No       |                     | Yes       |       | -          | Not Critical and Above | None                            | None                          | No                   |
|                                   |                |            |            | Historic a          | dvisories | View    | Edit                    | Change n | otification         | Unsubso   | cribe | Un-Share   | Delete                 |                                 |                               |                      |

### **View Watch Lists**

Vie	w Watch Lists						
1.	Open the Vulnerability Manager > Watch Lists & Advisories > Watch Lists page.						
2.	Click 💶 to create a new Watch List or 🖻 to import a Watch List from a text or CSV file that you have previously created and saved.						
3.	Click the Watch List check boxes in the grid to select from the available options from the CSV export button down menu.						
4.	Click 🔽 to filter the watch lists and advisories by <b>Name, Group, Enabled</b> (yes or no), <b>Approval Needed</b> (yes or no), and <b>Created by</b> .						
5.	Click the <b>Apply</b> or <b>Reset</b> buttons to apply or reset the filters.						
6.	Click the <b>Save</b> or <b>Delete</b> buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.						
7.	Click a Watch List in the grid to select <b>Historic Advisories</b> , <b>View</b> , <b>Edit</b> , <b>Change notification</b> , Unsubscribe, <b>Un-Share</b> / <b>Share</b> , or <b>Delete</b> .						
8.	To enable all of your users to collaborate, you can click a Watch List, select <b>Share</b> , and select the <b>With all users,</b> <b>Group (or Groups)</b> from the drop-down list and Enforce subscriptions options as required and click Save.						
9.	Click Shared Watch Lists to View, Subscribe, or Clone the Watch List. Select Clone to copy it to your Watch Lists, where you can then use the Historic Advisories, View, Edit, Change notification, Share, Un-Share or Delete options for the cloned Watch List.						
<b>No</b> sho	te • Any changes you make to a shared Watch List are shared by all users. If you want to change only your Watch List, you uld first clone it.						

**Important** • When creating, editing or sharing Watch Lists, the Deny auto-approval role will determine if the normal user can create Watch Lists with auto approval. The role must be manually added to a user group and that user group assigned to the restricted users by the administrators. For users with Deny auto-approval:

- **Create new Watch List**—The field Advisories need approval will be checked and cannot be disabled.
- Edit existing Watch List—The field Advisories need approval cannot be edited (either enabled or disabled).

• Shared Watch Lists for the user will have the normal behavior. It is the responsibility of the creator to ensure the Watch List has Advisories need approval selected if it is shared with restricted users

### **Create Watch Lists**

To create a watch list, perform the following steps.

Task	То	create a Watch List
	1.	Open the Vulnerability Manager > Watch Lists & Advisories > Watch Lists page.
	2.	To create a new Watch List, click 💶. The Create Watch List (Step 1 of 2) page opens. On this page, you can select <b>Product Versions, Products, Vendors,</b> or Assessment.

Create Watch List ( Step 1 of 2 )		×	5
Receive all advisories     Filter by FNMS data      Product Versions     Products     Vendors	Assessment		
Q Search			
Product Versions Database	+ +	Selected Product Versions X -	
001 File Joiner And Splitter Pro $4.\mathbf{x}$	ADD +		
009Soft File Splitter 1.x	ADD +		
010 Editor 2.x	ADD +		
010 Editor 3.x	ADD +		
₩ ♥ Page 1 of 5862 ▶ 1	×		
	Cancel	Next	
Note • You can select the Receive all a Products, and Vendors. Create Watch List (Step 1 of 2) Receive all advisories Filter by FINMS data	dvisories chec	k box to receive Secunia Advisories for all Product N	/ersions,
Cancel	Next		

- **3.** Use the search field to find the products, vendors, product versions, and device groups to select and add to your Watch List.
- 4. Click + in the Database suggestions column heading to add the current page or click + next to the individual items to add them to the **Selected** items list.

5. Click X in the Selected items column heading to remove the current page or DELETE X next to an individual item to remove it from the list.

Name	Watch List Group +	
Name	Watch List Group	*
Enabled	Advisories need approval	
Ticket threshold level	Confidentiality Requirement (CR)	
Not Critical and Above	<ul> <li>ConfidentialityRequirement</li> </ul>	*
Email notification level	Integrity Requirement (IR)	
Not Critical and Above	<ul> <li>IntegrityRequirement</li> </ul>	-
SMS notification level	Availability Requirement (AR)	
Extremely Critical	- AvailabilityRequirement	-

6. Click Next. The Create Watch List (Step 2 of 2) page opens.

- 7. Enter the Name of the Watch List.
- Select the Watch List Groups, if available, from the drop-down list to associate with this Watch List. You can also click
   to create a new Watch List group.
- **9.** Notifications and/or tickets are not sent for disabled Watch Lists. If you wish to preserve a Watch List for historical reasons, you can disable it by clearing the selection of the **Enabled** check box.
- **10.** If you select the **Advisories need approval** option, you will receive a notification and an email for advisories that match your Watch List. You can approve that advisory, in which case a ticket is created or you can dismiss the advisories.
  - **Note** If the users have the rejected advisories option enabled, the threshold filters may not apply since the advisory may not have the criticality set.
- 11. Select the Ticket threshold, Email and SMS notification levels from the drop-down lists.

The **Ticket threshold level** is used to determine whether or not tickets will be created for advisories matching your Watch List.

 You can optionally select the impact that a vulnerability in any item in the Watch List will have to your environment (Low, Medium or High) by Confidentiality Requirement (CR), Integrity Requirement (IR), and Availability Requirement (AR) from the drop-down lists (optional). The table below defines the Low, Medium, and High impact for CR, IR and AR. For the tickets created on the Watch List with values in the CR, IR, and AR fields, the system will use those values to calculate the custom Common Vulnerability Scoring System (CVSS) for the ticket.

Metric	Low Definition	Medium Definition	High Definition
CR	There is a low impact on the confidentiality of the system.	There is considerable disclosure of information, but the scope of the loss is constrained such that not all of the data is available.	There is total information disclosure, providing access to any or all data on the system.
IR	There is a low impact on the integrity of the system.	Modification of some data or system files is possible, but the scope of the modification is limited.	There is total loss of integrity; the attacker can modify any files or information on the target system.
AR	There is a low impact on the availability of the system.	There is reduced performance or loss of some functionality.	There is total loss of availability of the attacked resource.

**Note** • For further definition details, see:

https://en.wikipedia.org/wiki/Common\_Vulnerability\_Scoring\_System#Impact\_metrics

**Note** • After creating an Assessment Watch List from the Create a Watch List steps above:

- When a new scan is done, the new data is available in the Create Watch List pop-up window.
- When any scan result is deleted from the Assessment module, a refresh needs to be done to see the changes in the Assessment module and also in the **Create Watch List** pop-up window.
- When a Smart Group is deleted from the Assessment module, it may take at least 15 minutes to see the deleted Smart Group removed from the Assessment tab of the **Create Watch List** pop-up window.
- **13.** Click **Save** to save the Watch List. Once saved, you will begin to receive alerts and advisories based on your configuration.

### **Edit Watch Lists**

To edit a watch list, perform the following steps.

Task

#### To edit a Watch List:

1. Click an item in the grid and select Edit.

eceive all advisories				
liter by FNMS data				
roduct Versions	Products Vendors			
Q. Search	tabase	+ -	Selected Product Versions	×
		ADD +		
		ADD +		

2. Select Receive all advisories and Filter by FNMS data as appropriate. When you have finished making your selections, click Next. The Edit Watch List (Step 2 of 2) page opens.

Name	Watch List Group +	
FNMS_All_Windows_Servers	Watch List Group	,
Enabled	Advisories need approval	
Ticket threshold level	Confidentiality Requirement (CR)	
Not Critical and Above	- ConfidentialityRequirement	,
Email notification level	Integrity Requirement (IR)	
Email notification level	✓ IntegrityRequirement	
SMS notification level	Availability Requirement (AR)	
SMS notification level	<ul> <li>AvailabilityRequirement</li> </ul>	-

- 3. Enter the Name of the edited Watch List.
- Select the Watch List Groups, if available, from the drop-down list to associate with this Watch List. You can also click
   to create a new Watch List group.
- 5. Notifications and/or tickets are not sent for disabled Watch Lists. If you wish to preserve a Watch List for historical reasons, you can disable it by clearing the selection of the **Enabled** check box.
- 6. If you select the **Advisories need approval** option, you will receive a notification and an email for advisories that match your Watch List. You can approve that advisory, in which case a ticket is created or you can dismiss the advisories.

**Note** • If the users have the rejected advisories option enabled, the threshold filters may not apply since the advisory may not have the criticality set.

7. Select the Ticket threshold, Email and SMS notification levels from the drop-down lists.

The **Ticket threshold level** is used to determine whether or not tickets will be created for advisories matching your Watch List.

- 8. You can optionally select the impact that a vulnerability in any item in the Watch List will have to your environment (Low, Medium or High) by **Confidentiality Requirement (CR)**, **Integrity Requirement (IR)** and **Availability Requirement (AR)** from the drop-down lists (optional).
- 9. Click **Save** to save the edited Watch List. Once saved, you will begin to receive alerts and advisories based on your configuration.

### **Import a New Watch List**

To import a new Watch List, perform the following steps.

Task	То і	To import a new Watch List:								
	1.	Open the Vulnerability Manager > Watch Lists & Advisories > Watch Lists page.								
	2.	Click 🖪.								
	3.	Choose Create Watch List and Submit.								
		Select Option ×								
		Create Watch List     Edit Watch List								
		Close Submit								
		The Create Watch List (Step 1 of 4) dialog box opens.								
		Create Watch List ( Step 1 of 4 ) - Choose file ×								
		Choose File No file chosen								
		Note: please choose a text / csv file								
		Columns separator								
		First row has column names								
		Column with product names								
		Column with product names -								
		Cancel Upload file								

- 4. Define the Columns separator ("," is the default) for the file you are importing.
- 5. Select First row has column names, if applicable.
- 6. Click Upload file. The Create Watch List (Step 2 of 4) dialog box opens.

×

#### Create Watch List ( Step 2 of 4 ) - Match your products

Perfect match (420 items)	)			
🥝 Known alias (2 items)				
Previously selected (3 iter	ms)	+	Selected Products	×
B Bayesian suggestion (0 ite	ems)	+ ×		
Close suggestion based of Q Suggestion based on name	n name compare (0 items)	+ ×		
× No suggestions (0 items)		+ ×		
X Ignored (0 items)		+ ×		
7-Zip 3.x	⊘ 7-zip 3.x	+ ×		
7-Zip 4.x	✓ 7-zip 4.x	+ ×		
7-zip 9.x	⊘ 7-zip 9.x	+ ×		
Active Network Monitor 1.x	Active Network Monitor 1.x	+ ×		
Adobe Acrobat 2017 17.x	Adobe Acrobat 2017 17.x	+ ×		
Adobe Acrobat DC 15.x	Adobe Acrobat DC 15.x	+ ×		
	₩ ₩ Page 1 of 43 ₩ ₩			

- 7. Select the **Filter by quality** field to match your Watch List against the criteria you select from the drop-down list or use the **Search in your products** field to find a specific product.
- 8. Click + in the Database suggestions column heading to add the current page or click + next to the individual items to add them to the **Selected** items list.
- 9. Click 🗙 in the Selected items column heading to remove the current page or DELETE X next to an individual item to remove it from the list.
- **10.** When you have finished making your selections, click **Continue**. The **Create Watch List (Step 3 of 4)** dialog box opens.

roduct Versions	Products Vendor	Assessment		
<b>Q</b> , Search				
Product Versions Dat	abase	+ +	Selected Product Versions	×
001 File Joiner And Sp	litter Pro 4.x	ADD +		
009Soft File Splitter 1.3	¢	ADD +		
010 Editor 2.x		ADD +		
010 Editor 3.x		ADD +		
R	A A Page 1 of 5862	нн		

11. Choose other watch lists to add or delete and click Next. The Create Watch List (Step 4 of 4) dialog box opens.

×

Name	Watch List Group +
watchlist1.csv	Watch List Group
Enabled	Advisories need approval
Ticket threshold level	Confidentiality Requirement (CR)
Not Critical and Above	ConfidentialityRequirement
Email notification level	Integrity Requirement (IR)
Not Critical and Above	<ul> <li>IntegrityRequirement</li> </ul>
SMS notification level	Availability Requirement (AR)
Extremely Critical	AvailabilityRequirement
	Sack Save

Create Watch List ( Step 4 of 4 ) - Enter name and other properties

- 12. Enter the Name of the Watch List.
- 13. Select the Watch List Groups, if available, from the drop-down list to associate with this Watch List. You can also click
  to create a new Watch List group.
- 14. Select the Enabled and Advisories need approval check boxes as required.
- 15. Select the Ticket threshold, Email and SMS criticality notification levels from the drop-down lists.
- 16. You can optionally select the impact that a vulnerability in any item in the Watch List will have to your environment (Low, Medium or High) by Confidentiality Requirement (CR), Integrity Requirement (IR) and Availability Requirement (AR) from the drop-down lists (optional).

×

**17.** Click **Save** to save the Watch List. Once saved, you will begin to receive alerts and advisories based on your configuration.

### **Import an Updated Watch List**

To import an updated Watch List, perform the following steps.

Task	То	import an updated Watch List:
	1.	Open the Vulnerability Manager > Watch Lists & Advisories > Watch Lists page.
	2.	Click a.
	3.	Choose Edit Watch List, enter the Watch List to update in the search field, and click Submit.
		Select Option ×

<ul> <li>Create Watch List</li> <li>Edit Watch List</li> </ul>	
Q Search watch list	
Close	Submit

The Edit Watch List (Step 1 of 4) dialog box opens.

late: please choos	e a text / couñte	ь							
olumns separato	,	~							
E First row has col	umn names								
olumn with prod	wit names								
Product Name									
Account	Watch list	Product Id	Product Name	is operating system	Version	Full product name	is end of the	Vendur M	Vendor Name
Plexera Main Test Account	Friht5_impot	60234	Corel Photo Album		6.x	Corel Photo Album 8.x		378	Covel
Fiereria Main Tent Account	Frat5_impot	49034	Morosoft Vieb Publishing Wittend		tx.	Microsoft Vieb Publishing Witard 1.x		3	MouseR
Fiexana Main Tant Account	PNMS_import	833952	Toshika Buelooth Stack		4.x	Toshiba Buelooth Stack 4.x		3678	Toshiba
Flevera Main Test Account	FhildS_import	54729	Auditon		1.x	Auditor 1.x		12	Adulte Systems
Flexera Main Test Account	FNM5_Impot	70590	Canon PhotoRecord		2.×	Caron PhotoRecord 2 x		725	Canon
Flexera Main Tent Account	FRMS_Import	04406	Reatine Soft UltraMon		2×	Reative Soft UltraMon 2 x		3975	Faatine Soft
Plexera Main Test Account	PNMS_import	70590	PhotoSitch		3.4	PhotoSitch 3.x		795	Caron
Flexera Main Test Account	Phild5_import	130103	Oracledi Database Standard Edition			Cracletil Extabase Standard Edition		309	Oracle Corporation
Flexera Main Test Account	FNM5_Impot	70514	Zoonbrouser EX		5.x	Zoonbrovaer EX 5.x		725	Canon
Flexera Main Tent Account	FIRITS_Import	60097	Sophos SafeGuard PrivateCrypto		2.x	Sophon SafeGuard PrivateCrypto 2 x		162	Sophos

4. Choose File to import and click Upload file. The Edit Watch List (Step 2 of 4) dialog box opens.

		G Search myour pr	oducts	
emaining products: 623 slorized products already exist in r	one or more of your current watch lists			
Your Product	Suggested Product	+	Selected Products	:
ABBYY FineReader Sprint	O ABBITY FineReader Spirit 9 x	+ ×		
ABBYY FineReader Sprint	ADDITY FineReader Spirit 5.x	+ ×		
ABBYY FineReader Spirit	Abbyy FireReader Spirit 6 x	+ ×		
ACOSee	ACDSee 7.x	+ ×		
ACDSee	ACDSee 6 x	• *		
ACOSee	O ACOSee 5 x	+ ×		
ACO5ee	O ACDSee 4.x	+ *		
ACOSee	O ACOSee B x	+ ×		
Acronis True Image	O Aponis True Image 2013	+ *		
Acronis True Image	Acronis True Image 8 x	+ ×		

5. Make the necessary edits and click Continue. The Edit Watch List (Step 3 of 4) dialog box opens.

liter by FNMS data			
roduct Versions Products Vendors	Assessment		
Q, Search			
Product Versions Database	+ +	Selected Product Versions	×
001 File Joiner And Splitter Pro-4.x	A00 +	1-Citick Answers 2.x	DELETE
009Soft File Spitter 1.x	A00 +	1-click cleaner 2 x	DELETE
010 Editor 2.x	A00 +	5-Click YouTube Video Downloader 1 x (extension for Firefox)	DELETE
010 Editor 3.x	A00 +	A 1-Search 1.x	DELETE
03prepinstall ActiveX Control 1.x	A00 +	10 Finger BreakOut 2003	DELETE
A 04//ebServer 1.x	A00 +	10-Fingersystem in 5 Stunden 2.x	DELETE
A Overkill 0.x	A00 +	15-Sekunden-Haushaltsbuch 5 x	DELETE
10000000 1.x	Added	10-Strike LANState 2 x	DELETE
100 Doors of Revenge 1.x	Added	10-Strike Network Diagram 2 x	DELETE
100 Floors Escape 1.x	Added	100 Doors of Revenge 1.x	DELETE
TC CC Page 1 of 5001 bb bb	3	Ht dt Page 1 of3 be bit	

- 6. Make the necessary edits and click Next. The Edit Watch List (Step 4 of 4) dialog box opens.
- 7. Make any necessary edits and click Save.

## **Historic Advisories**

The **Historic Advisories** page provides access to a comprehensive and thorough collection of reports and statistics about all Secunia Advisories.

ulnerability Manager > Watch Lists	s & Advisori	es > Historic Advisories								8 -
Watch Lists & Advisories 👻	Ticketing	Approve Advisories								
owsing 1-20 of 75439 advisories for al	ll watch lists	n ž								7
All Watch Lists	• In	pact	▼ CVE(s)	SAID	From	=	То	=	Criticality	-
Solution status	• W	here	▼ CVSS Score Min	CVSS Score Max	Hasticket	-	Advisory type	-	Apply	Reset
							Filter	-	Save	Delete
Summary Month by Month	Soluti	on Status Criticality Wh	ere Impact							
		,								
Advisories 75439 Most Severe No Fix	None (Reje	cted)								
Advisories Based on OS / Softw	are		Advisories Based	on Vendor Solution			Advisories Based on 0	riticality		
Software 43990 (58.31) %			No Fix 12859 (	17.05) %			Extremely Critical	275 (0.36) %		
Operating System 33328 (44	.18) %		Vendor Patch	57001 (75.56) %			Highly Critical 1450	)5 (19.23) %		
			Vendor Worka	round 1615 (2.14) %			Moderately Critical	25247 (33.47) %		
			Partial Fix 177	1 (2.35) %			Less Critical 26893	(35.65) %		
							Not Critical 6325 (8	3.38) %		
										_
										+
CAUD Delever Dete	The second state of the se					<ul> <li>On booking an extension</li> </ul>	14/1	0100 0111	<ul> <li>The last Operated</li> </ul>	T
SAID Release Date ¢	Modified Dat	te	e Java Multiple Vulperabilities		Criticality	Solution status	Where From local petwork	CVSS Score	Ticket Created Ves	Type Securia Advisory



## **Product Advisories**

The **Product Advisories** page provides access to a comprehensive and thorough collection of reports and statistics about all Secunia Advisories affecting all products.

Vu	Inerability Mar	nager > Watch Lists & Ar	dvisories > Product /	Advisories								0 ·D
	Watch Lists &	Advisories - Tick	eting Approv	e Advisories								
Bro	owsing 1-20 of 75	6441 advisories for <b>all pro</b>	ducts.				Q, Search pro	duct version				Ŧ
	Zero Day	Ŧ	Impact	-	CVE(s)	SAID	From	<b></b>	То	<b></b>	Criticality	•
	Solution status	-	Where	-	CVSS Score Min	CVSS Score Max	Advisory type	-			Apply	Reset
									Filter	•	Save	Delete
	Summary	Month by Month	Solution Status	Criticality Whe	re Impact							
"						None Reject	ed) 2,194 tital 275 i 14,505 irital 25,248 26,693 6,326					
L	SAID	Release Date 🗢 🖨	Iodified Date	Title				Criticality 🗢 Solut	tion status	Where	CVSS Score	\$ Туре
6	<u>SA82793</u>	2018-04-25 2	018-04-25	Xen Raw CDROM Image H	landling Information Disclosu	re Vulnerability		<ul> <li>Vend</li> </ul>	or Patched	Local system	1.7	Secunia Advisory



## **Shared Watch Lists**

To enable all of your users to collaborate, you can click any of your Watch Lists, select **Share**, and select the **With all users**, **Group (or Groups)** from the drop-down list and **Enforce subscriptions options as required** and click **Save**.

If an account administrator wants to share a Watch List with all Users or User Groups on a mandatory basis, they can select Enforce subscriptions. All users that match from the selected groups (or from the entire account) will automatically receive notifications for the released advisories that match the Watch List. If Enforce subscriptions is not selected, the users have the option to voluntarily subscribe to advisories from that Watch List and can choose their own notifications levels.

**Note** • Subscribers to the Watch List can edit the Watch List, resulting in changes for all users.

Click a Shared List in the grid to View or Clone the Watch List. Select Clone to copy it to your Watch Lists, where you can then use the Historic Advisories, View, Edit, Change notification, Share, Un-Share or Delete options for the cloned Watch List.



**Note** • Any changes you make to a Shared List are shared by all users. If you want to change only your Watch List, you should first clone it.

**Note** • A watch list can only be shared once. If you need to share the watch list with multiple groups or with multiple levels, you will need different watch lists.

## FlexNet Manager Suite (FNMS) Import

Go to **Vulnerability Manager > Inventory > FNMS Import** to display a list of products imported from FlexNet Manager Suite.

You can Search by keyword for a specific product or click **I** to filter the list by **Name**, **Version**, **Publisher**, **Matched by Flexera** (select Unknown by Flexera or Matched by Flexera from the drop-down list), **Matched by Intelligence** (select Unmatched by Intelligence or Matched by Intelligence from the drop-down list) or **Import status** (select New, Same or Removed from the drop-down list).

For further information, please refer to the FlexNet Manager Suite Inventory Exporter documentation.

You can also select Filter by FNMS data when creating or editing Watch Lists.



**Note** • It may take up to 5 minutes for the submitted products to be processed and displayed.



*Important* • The minimum version of FlexNet Manager Suite supported by the Software Vulnerability Research import tool is 2015 R2 SP2.

## **Ticketing in Vulnerability Manager**

A ticket enables you to track and manage vulnerabilities based on the current state of all your Products, Vendors, and Watch Lists.

You can manually create a ticket from all Advisories, in case you would like to further process an Advisory for a vulnerability not affecting any of your Watch Lists, giving you the possibility to track any vulnerability which might affect the organization, not only vulnerabilities in software included in any of your Watch Lists.

Use the Ticketing page to view and change the Ticket Status and Ticket Priority of each Ticket.

Natch Li	sts & Advisories	<ul> <li>Ticketin</li> </ul>	g Appr	rove Advisories							
en tickets	13384 Waiting	tickets 38 Clo	sed tickets	285 Irrelevant tick	kets 10 F	Pending deployment tickets 3 At QA tickets 2					
wring 1-2	0 of 12722 tickets	1									
wang r-zi	0 01 13722 tickets [									<b>y</b> + 4	Action
ld 🗘	Ticket created Q	lueue 💠 Status	Priority \$	Watch List	SAID 🖨	Title	Criticality 🗧	Secunia Advisory published	Solution status	CVSS/Custom Score	Actio Assigned
Id ¢ 13746	Ticket created Q 2018-03-12 D	tueue 💠 Status lefault Open	Priority Medium	Watch List	SAID \$	Title HP-UX update for Tomcat-based Serviet Engine	Criticality	Secunia Advisory published 2018-03-12	Solution status	CVSS/Custom Score	Actic Assigned

📋 Task

#### To view and change ticket status and ticket priority

- 1. Open the Vulnerability Manager > Ticketing page.
- To filter the results by ticket status, select one of the bold ticket statuses in the upper-left-hand corner followed by a ticket count. The default ticket statuses are Open, Waiting, Handled, and Irrelevant. See Default Ticket Statuses in Vulnerability Manager for more information.

- 3. Click T to filter the results by ID, From and To dates, Queue, Priority, Watch List, SAID, Criticality, Solution status and CVSS Score Minimum and Maximum values, and Assigned User.
- 4. Click the Apply or Reset buttons to apply or reset the filters.
- Click the Save or Delete buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.
- 6. Click a Secunia Advisory ID (SAID) to view detailed information related to the Advisory.
- 7. To view one ticket, click the appropriate ticket check box in the grid to **View**, **Edit**, or **Delete** the ticket. To view multiple tickets, click the appropriate ticket check boxes in the grid and select an option from the Actions drop-down menu such as **Delete multiple tickets** (see Delete Tickets in Vulnerability Manager) or **Edit multiple tickets**.
- 8. Click 🚨 to export tickets to a CSV file.
- 9. Click 💶 to Create Tickets in Vulnerability Manager.

## **Create Tickets in Vulnerability Manager**

To create tickets in Vulnerability Manager, perform the following steps.

## Task To create a ticket in Vulnerability Manager:

- 1. Open the Vulnerability Manager > Ticketing page.
- 2. Click an Advisory or 🚹 to create a ticket for the Advisory.

Create ticket ×
Advisory
Q, Search by SAID or title
Status
Open -
Priority
Low •
Queue
Default 🔹
Assigned to
Assigned to 👻
Add comment
Add comment
Cancel Save

3. From the **Status** drop-down list, select the appropriate status. The default ticket statuses are **Open**, **Handled**, **Closed**, or **Irrelevant**. See Default Ticket Statuses in Vulnerability Manager for more information.

- 4. From the **Priority** drop-down list, select the appropriate priority. The default ticket priorities are **Low**, **Medium**, **High** or **Urgent**.
- 5. From the **Queue** drop-down list, select a queue to assign the ticket to.
- 6. From the Assigned to drop-down list, select an individual to assign the ticket to.
- 7. In the Add comment field, add an appropriate comment to the ticket (mandatory).
- 8. Click Save.

## Delete Tickets in Vulnerability Manager

To delete tickets in Vulnerability Manager, perform the following steps.

Тос	delete tickets in Vulnerability Manager:
1.	Open the Vulnerability Manager > Ticketing page.
2.	Insert a check mark in front of the ticket or tickets to delete.
3.	To delete one ticket, select <b>Delete</b> under the listed ticket in the grid.
	Vulnerability Manager > Ticketing
	Watch Lists & Advisories - Ticketing Approve Advisories
	Open tickets 1122 Walding tickets 🔝 Cored tickets 🔝 Irrelevant tickets 🗊 Pending deployment tickets 🚺 At QA tickets 🚦
	Browsing 1-20 of 1-206 tickes j
	the Table College Strain & State Block & State Block & State Stat
	14230 2018-03-15 Default Open Low predi-PO SAR2041 Magela phy Rejection Notice
4.	v       H230       2016-02-15       Defeut       Open       Low       prest-R0       Mages of the Regeledee Holdes
4.	v       14230       2016-02-15       Nore       -         View       Edit       Colored       -       -       -         View       Edit       Colored       -       -       -       -         View       Edit       Colored       -       -       -       -       -         View       Edit       Colored       -
4.	v       View       Core       prestic PD       View       View       Core       2016-03-15       Nore       -         View       Edit       Colored       View       Edit       Colored       -        -       -       - <td< td=""></td<>
4.	v       View       Core       Core <t< td=""></t<>
4.	v       View       Low       prest PD       View       Low       2016-03-15       Nore         View       Edit       Colored         View       Edit       Colored         Watch Lists & Advisories -       Ticketing       Image approve Advisories         Watch Lists & Advisories -       Ticketing       Image approve Advisories         Open tickets       Cored tickets       Image approve Advisories         Denoting 1-20 of 14/102 tickets       Image approve Advisories       At QA tickets
4.	v v

5. When the "Are you sure you want to delete these tickets" pop-up window appears, click Yes.



## **Default Ticket Statuses in Vulnerability Manager**

The default ticket statuses are used by the Advisories and Policy Manager to run and display reports. While you are free to configure the ticket statuses, priorities and queues as you see fit, Flexera needs to know your equivalent "open" statuses to be able to correctly report the statistics.

The following are the default ticket statuses:

#### Table 6-1 • Default Ticket Statuses

Status	Description
Open Tickets	An Open Ticket is one for which no action has yet been triggered.
Waiting Tickets	A ticket is marked as Waiting when it has been decided that an action needs to be taken at a later stage.
Handled Tickets	A ticket is considered Handled when the appropriate action has been taken.
Irrelevant Tickets	A ticket is considered Irrelevant when it has been handled and is no longer considered of importance to you.

Click a Secunia Advisory ID (SAID) to view detailed information related to the Advisory or click a ticket to View or Edit the details.

## **Approve Advisories**

The Approve Advisories page displays a list of all Advisories pending your approval.

<u> </u>
-

Note • To approve Advisories, you should select the Advisories need approval check box when you Create Watch Lists.

Task

#### Approve advisories

1. Open the Vulnerability Manager > Approve Advisories page.

ulnerat	bility Manager	<ul> <li>Approve</li> </ul>	Advisorie	s									0
Watch	h Lists & Advi	sories +	Ticketi	ng	Approve Advisories								
owsing	; 1-20 of 45 advis	sories i											Y Actions
In que	sue		*	Watch L	lst	-	SAID	From	iii	То	=	Title	
Critical	ality		-	Solution	status	-						Apply	Reset
										Filter	•	Save	Delete
Wa	atch List S	AID	Release da	te i	Modified date	Title				Criticality 0	Solution status	Where	CVSS Score
✓ bro	owsers S	A81977	2018-03-13		2018-03-13	Microsoft 8	dge Multiple Vulnerabilities				Vendor Patched	From remote	10

- 2. Click T to filter the Advisories by In queue, Watch List, SAID, From and To dates, Title, Criticality, and Solution status.
- 3. Click the Apply or Reset buttons to apply or reset the filters.

- 4. Click the Save or Delete buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.
- 5. To approve one advisory, click the appropriate advisory check box in the grid to **Approve** the advisory. The **Approve advisory** pop-up window appears. Continue to step 7.

Approve advisory	×
Advisory	
SA67053	
Status	
Status	•
Priority	
Priority	-
Queue	
Queue	•
Assigned to	
Assigned to	•
Add comment	
Add comment	
Cancel S	ave

**6.** To approve multiple advisories, click the appropriate advisory check boxes in the grid and select Approve multiple advisories from the Actions drop-down menu. The **Approve multiple advisories** pop-up window appears.

Approve multiple advisories	×
Advisory	
3 selected	
Status	
Status	•
Priority	
Priority	•
Queue	
Queue	•
Assigned to	
Assigned to	•
Add comment	
Add comment	
Cancel Save	

- 7. Select the Status (Open, Waiting, Handled or Irrelevant) from the drop-down list.
- 8. Select the Priority (Low, Medium, High or Urgent) from the drop-down list.
- 9. Select the Queue (Default or Approval) from the drop-down list.
- 10. Select who the ticket should be Assigned to from the drop-down list.
- **11.** Enter a comment.
- 12. Click Save to approve the Advisory or Advisories.



**Note** • Once an Advisory has been approved, the corresponding ticket will be marked as **Open**.

# 7 Research

Vulnerability Intelligence represents our full Vulnerability Database, which has been updated and maintained since the inception of Secunia in 2002.

Use the Research pages to:

- View Advisories
- Create Tickets in Vulnerability Manager
- View Vendors, Product Versions, Products and Suggest Software

## **Advisory Database**

When a potential software vulnerability is publicly disclosed, our Research Team verifies that it is in fact a vulnerability. Once confirmed, we analyze the severity and what software might be affected.

Then, a standardized and 100% vendor independent Secunia Advisory is written for the vulnerability, detailing attack vector, criticality rating, impact and solution.

The Secunia Advisory is uploaded to Software Vulnerability Research, and adapted intelligence feeds are delivered to you, based on customized pre-configured filters, to ensure the right groups of people are alerted whenever a new vulnerability that could affect your IT infrastructure is discovered.

You can customize filters according to, for example, software responsibility, compliance criteria or geography for each of the recipients in your organization.

Personalized security alerts - via email or SMS - are then issued in real-time to the correct individual in your organization.

Select Advisories or Rejected Advisories from the drop-down list to display details that are applicable to your Watch Lists.

## **Advisories**

The Advisories page displays details of all the advisories released.

The Advisories page can be,

- Advisories with Threat Score
- Advisories without Threat Score

#### To open the Advisories page, Research >> Advisory Database >> Advisories

🚱 Software Vulnerability Research	Research > Advisory Database > Advis	pries	
Dashboard	Advisory Database  Produc Browsing 1-20 of 82108 advisories	s Database 👻	
Notifications 2	SAID Release date 💠	Modified date 🗢 Title	
Vulnerability Manager	SA89210         2019-05-25           SA89205         2019-05-25           SA89196         2019-05-25	2019-05-25 SUSE blu 2019-05-25 SUSE up 2019-05-25 Debian up	rez Rejection Notice date for libvirt pdate for wpa
Research	SA89252         2019-05-25           SA89261         2019-05-24	2019-05-25 Nagios XI 2019-05-24 SUSE up	I "Reset Password" SQL Injection Vulnerability date for xen
Assessment	SA89391         2019-05-24           SA89382         2019-05-24           SA889382         2019-05-24	2019-05-24 IBM 1100 2019-05-24 SUSE up 2019-05-24 IBM Spec	i Network Manager IP Edition OpenSSL Rejection Notice date for curl strum Control Multiple Vulnerabilities
Patching	SA87643         2019-05-24           SA89190         2019-05-24           SA89263         2019-05-24	2019-05-24 IBM Cogr 2019-05-24 IBM Secu 2019-05-24 wolfSSL F	nos Analytics Multiple Vulnerabilities nity Guardium OpenSSL Rejection Notice PSK Identity Buffer Overflow Vulnerability
Policy Manager 1895	SA89237         2019-05-24           SA89245         2019-05-24	2019-05-24 F5 BIG-IF 2019-05-24 F5 BIG-IF	P Local Traffic Manager (LTM) Binutils Rejection Notice P Local Traffic Manager (LTM) Binutils Rejection Notice
Analytics	SA89238         2019-05-24           SA89236         2019-05-24           SA89232         2019-05-24	2019-05-24         SUSE sys           2019-05-24         Oracle Lin           2019-05-24         Oracle Lin	sstat Kejection Notice nux update for libvirt nux update for firefox
Ticket Manager	SA89239         2019-05-24           SA889233         2019-05-24           SA889235         2019-05-24	2019-05-24 Oracle Lir 2019-05-24 Ubuntu uj 2019-05-24 Red Hat u	nux update for firefox pdate for mariadb-5.5 update for libvirt
	SA89184 2019-05-23	2019-05-23 Red Hat u	update for firefox

### **Advisories with Threat Score**

The **Advisories** page with the Threat Score module is shown below.

Adv	isory D	atabase 👻	Products	s Database 👻										
Browsir	ng 1-20 c	of 80902 advisori	es į					<b>Q</b> Search by	y keyword					<b>Y</b> +
Zero	o Day		•	Impact	•	CVE(s)	SAID	From		То		<b></b>	Criticality	•
Solu	ition statu	IS 🕶 Where	•	CVSS Score Min	CVSS Score Max	Threat Score Min	Threat Score May	Advisory type		•			Apply	Reset
										Filte	r	•	Save	Delete
. S/	AID	Release date	Modified	date 💠 Title				Criticality	🗧 Zero Day 👙	Solution status	Where	CVSS Score	Threat Score	• Туре
<u>s</u>	A83063	2018-05-09	2018-05-0	9 Microsoft V	/indows Server 2012 / V	Vindows RT 8.1 / 8.1 Mu	Itiple Vulnerabilities		Yes	Vendor Patched	From remote	10.0	99	Secunia Advisory
<u>s</u>	<u> 476976</u>	2017-05-19	2017-05-2	4 Huawei Mu	Itiple OceanStor Produc	ts Multiple SMB Vulnera	bilities		No	Vendor Patched	From local network	8.3	99	Secunia Advisory
<u>s</u>	A68501	2016-01-27	2016-01-2	7 Gentoo upd	late for adobe-flash				No	Vendor Patched	From remote	10.0	99	Secunia Advisory
<u>s</u>	A75768	2017-03-15	2017-03-1	5 Microsoft W	/indows SMB Server Vu	Inerabilities			No	Vendor Patched	From local network	8.3	99	Secunia Advisory

**Note** • Please note the following:

- This add on requires purchase of the Software Vulnerability Research Threat intelligence Module.
- To purchase this module, contact your sales representative or contact us online at: https://www.flexera.com/about-us/contact-us.html

In additional to the features explained in the **Advisories Page >** Advisories without Threat Score, the following features are added:

- To filter the Advisories by Threat Score minimum and maximum values, click **V**.
- To see the threat score and threat reason, click a Secunia Advisory ID (SAID) > CVE References. Additional information of the selected Secunia Advisory ID is shown below:

**Microsoft Windows PDF Library Two Code Execution Vulnerabilities** 

Secunia Advisory ID	SA69399
Creation Date	2018-03-09
Criticality	- Highly critical
Zero Day	No
Impact	System access
Where	From remote
Solution Status	Vendor Patched
Secunia CVSS Scores	Base: 10, Overall: 8.3 (AV:N/AC:L/Au:N/C:C/I:C/A:C/E:F/RL:OF/RC:C)
CVE references	CVE-2016-0118 •   CVE-2016-0117 •
Threat Score	54 (Last Updated 2019-02-21)
Affected operating system and software	
Operating systems	
Microsoft Windows 10	CPE Exists. Click for details.
Microsoft Windows 8.1	CPE Exists. Click for details.

• To see the threat Score, threat Reason and their associated exploits, click on the CVE references, as shown below:

#### Microsoft Windows PDF Library Two Code Execution Vulnerabilities - CVE

CVE	cvss*	Threat Score	Threat Reason
CVE-2016-0118	CVSS v2: 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)	2	Linked to Historical Cyber Exploit
<u>CVE-2016-0117</u>	CVSS v2: 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)	53	Linked to Historical Cyber Exploit Historically Linked to Malware Historically Linked to Ransomware Historically Linked to Penetration Testing Tools

#### Description\*

The PDF library in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allows remote attackers to execute arbitrar crafted PDF document, aka "Windows Remote Code Execution Vulnerability."

#### Treat Intel Module

The CVE threat score of 53 was based on the following triggers:

- Linked to Historical Cyber Exploit
- Historically Linked to Malware
- Historically Linked to Ransomware
- Historically Linked to Penetration Testing Tools
- The threat score was last updated on 2019-05-07. These threats have been associated with the following exploits:

#### Qbot (Botnet)

- Cryptolocker (Ransomware)
- GozNym (Banking Trojan)
- Gootkit (Banking Trojan)
- Locky (Ransomware)

#### . .

 References\*

 ST
 http://www.securitytracker.com/id?1035202

 BID
 http://www.securityfocus.com/bid/84109

 Microsoft Security Bulletin
 http://technet.microsoft.com/security/bulletin/MS16-028

#### NOTE:

\* The information is written and maintained by <u>CVE MITRE</u>.

The data on this page reflects neither the opinions of Secunia or the results of our research.

Back

### **Advisories without Threat Score**

The **Advisories** page without the Threat Score is shown below:

search > Advisory Dat	abase > Advisories										?
Advisory Database 🚽	Products D	atabase 🗸									
owsing 1-20 of 75441 ad	sories i					Q, Search by keyword					<b>T</b>
Zero Day	-	Impact		CVE(s)	SAID	From	=	То	=	Criticality	-
Solution status	•	Where	-	CVSS Score Min	CVSS Score Max	Advisory type	•			Apply	Reset
								Filter	÷	Save	Delete
SAID Release	date 🗢 Modif	ed date	Title			Criticality 🍵 Ze	ero Day 🔶	Solution status	Where	CVSS Score	• Туре
SA82869 2018-04	25 2018-	4-25	Hitachi Multiple Products Oracle Ja	ava Multiple Vulnerabilities		- No	D	No Fix	From local network	6.8	Securia Advisory



#### To view advisories

- 1. Open the Research > Advisory Database > Advisories page.
- 2. Use Search by keyword to filter the Advisories by the text you enter.

3. Click T to filter the Advisories by Zero Day, Impact, CVE(s), SAID, From and To dates, Criticality, Solution status, Where, Score Minimum and Maximum values, and Advisory Type.

	<b>Note</b> • To search for multiple advisories at the same time to determine which advisories apply to more than a single CVE for which you have interest, enter the CVEs in the <b>CVE(s)</b> filter and leave one space between entries (Example: CVE-2014-0224 CVE-2014-0160 CVE-2013-0169 CVE-2009-3555 CVE-2015-7575).
4.	Click the <b>Apply</b> or <b>Reset</b> buttons to apply or reset the filters.
5.	Click the <b>Save</b> or <b>Delete</b> buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.
	If you select Hide rejected advisories under Settings > Account > Account Options:
	• The Advisory Type filter will not appear under Research > Advisory Database > Advisories.
	• The search result "No advisories found" appears under <b>Research &gt; Advisory Database &gt; Rejected Advisories</b> .
	<b>Note</b> • The CVSS Score column in the grid contains either a CVSS 2.0 score or a CVSS 3.1 score. A CVSS 3.1 score will be noted with "v3" listed after the score.

6. Click a Secunia Advisory ID (SAID) to view detailed information related to the Advisory.

Secunia Advisory ID	SA67058
Creation Date	2015-10-23
Criticality	- Highly critical
Impact	System access
Where	From remote
Solution Status	Vendor Patched
Securia CVSS Scores	Base: 10, Overall: 7.4 (AV:N/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C)
CVE references:	CVE-2015-7647   CVE-2015-7648   CVE-2015-7645
Affected operating system and software	
Software	
Google Chrome 46 x	
Google Chrome 46.x	UPE . IVA
Advisory Details:	
Description:	
Multiple vulnerabilities have been reported in 0	Google Chrome, which can be exploited by malicious people to compromise a user's system.
The vulnerabilities are caused due to the applie	cation bundling a vulnerable version of Adobe Flash Player.
For more information: SA66915	
The vulnerabilities are reported in versions priv	or to 46.0.2490.80.
Solution:	
Update to version 46.0.2490.80.	
Original advisory:	
http://googlechromereleases.blogspot.com/2	015/10/stable-channel-update 22.html
References:	
SA66915:	
https://secunia.com/advisories/66915/	
https://secunia.com/advisories/66915/ Changelog:	
https://secunia.com/advisories/66915/ Changelog: 2015-10-23: Initial release	

Google Chrome Adobe Flash Player Multiple Vulnerabilities

7. Click an Advisory check box in a row or rows in the grid or click the Advisory and select **View Advisory** or **Create ticket**.

_		
	-	
	-	

**Note** • If you select multiple advisories, one ticket is created for each of the Advisories selected.

**Note** • Once you have selected an Advisory check box, you can click • to create a ticket.

×

## **Rejected Advisories**

For compliance reasons, for example NERC (North American Electric Reliability Corporation), you may be required to report not only the vulnerabilities covered by the normal Advisories but also vulnerabilities, which our Research Team has rejected as not being a valid threat to security.

The **Rejected Advisories** page displays the advisories affecting your Watch Lists that did not pass our validation and filtering process rules and provides you with information about rejected vulnerabilities to make it possible for you to fulfill your compliance requirements. The Rejected Advisories page can be shown or hidden, depending on the Account Options set by your Administrator.

An advisory can be rejected for one of many reasons. The most common are:

- No reachability—The vulnerability cannot be exploited because the affected systems cannot be reached by an attacker.
- **No gain**—The vulnerability may be reached, but without any gain for the attacker.
- **No exploitability**—The vulnerability cannot be exploited because, for example, policy forbids installation of the affected software.
- **Dependent on other**—The vulnerability cannot be exploited by itself but is depending on another vulnerability being present.

	-	-	-
	-	-	-
	-	-	-
	-	_	_
14		_	

Note • The rules outlined below are rules of thumb and not strictly pass/fail rules.

### Task

#### To view rejected advisories

1. Open the Research > Advisory Database > Rejected Advisories page.

dvisory Datab	ase - Products	Datab	oase 👻													
Advisories Rejected Advisor	es į							Q, Searc	n by keyword							Ţ
Zero Day	·	•	mpact		*	CVE(s)	SAID	From		î	T	)	â	Criticality		
Solution status		·	Vhere		٠	CVSS Score Min	CVSS Score Max							Apply		Reset
											FI	ter		Save		Delete
SAID	Release date	Modi	fied date 🔶	Title					Criticality	Zero Da	у	Solution status	Where	CVSS Score	🗘 Туре	
SA82695	2018-04-25	2018-	-04-25	Symantec Reporter P	Reject	ion Notice				No		None	None	-	Rejected A	dvisory

2. Click **T** to filter the Advisories by Zero Day, Impact, CVE(s), SAID, From and To dates, Criticality, Solution status, Where, and Score Minimum and Maximum values.

**Note** • Rejected advisories may not have all the details of the normal advisories: CVSS Vector and score, criticality, and so on.

- 3. Click the Apply or Reset buttons to apply or reset the filters.
- 4. Click the **Save** or **Delete** buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.

- 5. Click a Secunia Advisory ID (SAID) to view detailed information related to the Advisory.
- 6. Click an Advisory check box in a row or rows in the grid or click the Advisory and select **View Advisory** or **Create ticket**.

Note • If you select multiple advisories, one ticket will be created for each of the advisories selected.

Once you have selected an Advisory check box, you can click 🚺 to create a ticket.

## **Products Database**

The Products Database represents the full list of products tracked by our database, which has been updated and maintained since the inception of Securia in 2002. You can browse Vendors, Products, and search for specific Product Versions applicable to your Watch Lists. You can also Suggest Software that you would like us to add to our database.

- Vendors
- Product Versions
- Products
- Suggest Software

## Vendors

The **Vendors** page displays a list of all available vendors. Click **View Products** to display the products associated with the vendor or click a vendor in the grid to view past advisories related to the vendor.

Research > Products Database > Vendors				0 -1
Advisory Database - Products Database -				
Browsing 1-20 of 10464 vendors 🦸		Q, Search by keyword		£
Vendor	Home Page		View Products	
The same of the sa			View Products	
		Past advisories		

ĭ Task

#### To view vendors

- 1. Open the **Research > Products Database > Vendors** page.
- 2. To search for a specific vendor, pick a name from the **Vendor** column, enter it in the **Search by keyword** field and press **Enter**.
- 3. Click 🗳 to download a CSV file containing details of all vendors.

### **Product Versions**

The **Product Versions** page displays a list of all available products, specified by product version number.

## Task

#### To view product versions:

#### 1. Open the Product Versions page.

Research > Products Databas	e > Product Versions								<b>0</b> -
Advisory Database +	Products Database +								
Prowsing 1-20 of 58321 product v	versions 💈		Q. Search by keyword						<b>Y</b> 4
Name	Vendor	Versi	Software type	Is end of life		*	Appl	y 👘	Reset
				Filter		-	Seve		Delete
Name		Vendor	Product		• Version	• Тур	,	End of Life	
001 File Joiner And Splitter Pro 4.x		Welltek Software	001 File Joiner And Splitter Pro		4.×	Sof	ware	No	

- 2. Click a product version in the grid to view past advisories related to the product version.
- **3.** To search for a specific product version, pick a number from the **Version** column, enter it in the **Search by keyword** field and press **Enter**.
- 4. Click T to filter the results by Name, Vendor, Version, Software type, (Software/Operating system), and Is end of life (No/Yes).
- 5. Click the Apply or Reset buttons to apply or reset the filters.
- 6. Click the **Save** or **Delete** buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.
- 7. Click 🗳 to download a CSV file containing details of all product versions.

## **Products**

The **Products** page displays a list of all available products.

## Task

#### To view products

1. Open the **Products** page.

Advisory Database * Products Database *	
Brewing 1-20 of 46603 products g	±.
Reme Vender Software ppe -	
Flor Sove Delete	
Name © Vendor © Type © View Releases	
001 Pile Joiner And Spätter Pro Veetkets Software Software Software	

- 2. Click a product in the grid to view past advisories related to the product.
- 3. To search for a specific product, pick a name from the Name column, enter it in the **Search by keyword** field and press **Enter**.
- 4. Click <sup>I</sup> to filter the results by Name, Vendor, and Software type (Software/Operating system).
- 5. Click the **Apply** or **Reset** buttons to apply or reset the filters.
- Click the Save or Delete buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.

- 7. Click View versions under the View Releases column to display the Vendor, Product, Version, Type and End-of-Life details.
- 8. Click 🔤 to download a CSV file containing details of all products.

## **Suggest Software**

Use the **Suggest Software** page to suggest new software to our Research Team. After clicking the **Suggest Software** button, the **Suggest a software** window appears. You must provide a Software name, Software version, a valid URL to the software Internet page, a valid email address, and an optional comment.

You can also upload a CSV file or a TXT file with multiple product suggestions. Each row from the file must contain all details needed for a single product suggestion (Name, Version, and a valid URL).

Α	В	C
Product Name	Product Version	URL
ApacheCommons-Id	1	http://commons.apache.org/sandbox/commons-id/downloads.html
ApacheECS	1	https://jakarta.apache.org/ecs/
Argparse4j	0.4.3	https://github.com/argparse4j/argparse4j/releases
Args4j	2.32	https://mvnrepository.com/artifact/args4j/args4j
Args4j	2.x	https://mvnrepository.com/artifact/args4j/args4j
Ascii-table	1	https://mvnrepository.com/artifact/de.vandermeer/asciitable
AtInject	1	https://mvnrepository.com/artifact/org.atinject
Boost	4.x	https://mvnrepository.com/artifact/com.googlecode.boost-maven-project
Bower-angular	1.3.x	https://github.com/angular/bower-angular

Figure 7-1: Suggest Software CSV Example

```
Product Name, Product Version, URL
ApacheCommons-Id, 1, http://commons.apache.org/sandbox/commons-id/downloads.html
ApacheECS, 1, https://jakarta.apache.org/ecs/
Argparse4j, 0.4.3, https://github.com/argparse4j/argparse4j/releases
Args4j, 2.32, https://mvnrepository.com/artifact/args4j/args4j
Args4j, 2.x, https://mvnrepository.com/artifact/args4j/args4j
Ascii-table, 1, https://mvnrepository.com/artifact/de.vandermeer/asciitable
AtInject, 1, https://mvnrepository.com/artifact/org.atinject
Boost, 4.x, https://mvnrepository.com/artifact/com.googlecode.boost-maven-project
Bower-angular, 1.3.x, https://github.com/angular/bower-angular
```

Figure 7-2: Suggest Software TXT Example



## **Assessment Scenarios**



Edition • This Assessment module is not available for Software Vulnerability Research.

With Flexera's Software Vulnerability Research, you can scan target hosts using a variety of approaches:

- Agent-Based Scan Requirements for Windows
- Agent-Based Scan Requirements for Mac OS X
- Agent-Based Scan Requirements for Red Hat Enterprise Linux (RHEL)
- Vulnerable Software Discovery Tool Command Line Options
- Scanning Via Local Agents



**Important** • Administrators must ensure that Software Vulnerability Research and its Vulnerable Software Discovery Tool have access to all necessary system and online resources which allow the application to run as intended. The following addresses should be white-listed in the Firewall/Proxy configuration to ensure that the client system is allowed access to these online resources:

- crl.verisign.net
- crl.thawte.com
- http://crl3.digicert.com
- http://crl4.digicert.com
- http://\*.ws.symantec.com
- https://app.flexerasoftware.com/

**Note** • If a machine has not checked in with Software Vulnerability Research in 90 days, the machine will be removed from your view. If the machine checks in again, it will reappear.

## **Agent-Based Scan – Requirements for Windows**

The flexibility offered by Software Vulnerability Research ensures that it can be easily adapted to your environment. To deploy the Windows agent, see Deploy a Windows Agent.

If you choose to scan using the installable Agent (Agent-based scans), the following requirements should be present in the target hosts:

Table 8-1 • Agent-Based Scan / Windows System Requirements

Requirement	Description
Permissions	Administrative privileges to download and install Software Vulnerability Research's Vulnerable Software Discovery Tool files SVMScanInstall.msi and SVMScan.exe from: https://app.flexerasoftware.com/
Access	Access to: https://agent.app.flexerasoftware.com
Operating systems	<ul> <li>Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016</li> <li>Microsoft Windows Operating System 7 Service Pack 1, 8.1, 10</li> </ul>
Internet Connection	SSL 443/TCP to https://app.flexerasoftware.com/
Update agent	Windows Update Agent 2.0 or later
Port	Port 443 (standard HTTPS) to access the cloud

## Agent-Based Scan – Requirements for Mac OS X

The following requirements should be met before installing the Software Vulnerability Research's Vulnerable Software Discovery Tool for Mac (see Deploy a Mac Agent) on an Intel-based Mac OS X machine:

#### Table 8-2 •

Requirement	Description
Operating System	Supported operating systems:
	• 10.8 Mountain Lion
	• 10.9 Mavericks
	• 10.10 Yosemite
	• 10.11 El Capitan
	• 10.12 Sierra
	• 10.13 High Sierra
	• 10.14 Mojave
Permissions	• Administrator at minimum ("root" privileges required for the installation)
	• The user installing the Agent must have 'execute' permissions on the file (chmod +x)
Internet Connection	SSL 443/TCP to https://app.flexerasoftware.com/.

To scan Apple Mac OS X machines, you need to deploy the Vulnerable Software Discovery Tool for Mac locally on the target system. This Vulnerable Software Discovery Tool for Mac pulls information from text and binary coded plist files.

The installation can only be done under the Mac Terminal, as the Vulnerable Software Discovery Tool for Mac will be installed as a daemon (service) under the LocalSystem account.

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

To view and edit the assessment configurations for Mac OS X, see:

- Prepare Your Mac
- Install the Vulnerable Software Discovery Tool for Mac

## **Prepare Your Mac**

Installation of daemons (services) on Mac OS X systems requires root account privileges. This means that the root account should always be used when installing the Vulnerable Software Discovery Tool for Mac.

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

#### bash-3.2\$ su root Password:

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

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

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

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

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

#### http://support.apple.com/kb/ht1528



**Important** • If you cannot enable the "root" account on the Mac, or you prefer to not use it directly, you can alternatively use the "sudo" switch before each command associated with Vulnerable Software Discovery Tool for Mac activities. For example: sudo ./svmscan\_macos -c -v -v -v can be used to install the Vulnerable Software Discovery Tool for Mac on the system.

Once you are ready with setting/logging the root account, you are one step away from installing the Vulnerable Software Discovery Tool for Mac.

When you download the Vulnerable Software Discovery Tool for Mac on your system, normally the file is being set with limited file permissions on the system. You must check whether the file is allowed execution on the system by using the ls -1 command, which will list the file and will show its file permissions.

```
sh-3.2# ls -l
total 3048
-rw-r--r--@ 1 administrator staff 1558928 Oct 25 12:25 svmscan_macos
```

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

```
chmod +x svmscan_macos
```

```
sh-3.2# chmod +x svmscan_macos
sh-3.2# ls -l
total 3048
-rwxr-xr-x@ 1 administrator staff 1558928 Oct 25 12:25 svmscan_macos
```

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

## Install the Vulnerable Software Discovery Tool for Mac

The traditional way of installing the Vulnerable Software Discovery Tool for Mac is as a daemon (similar to local service in Windows) as it will operate under the Mac OS X LocalSystem account. Install the binary by using the Mac Terminal services as follows:

) E		
Task	To install the Vulnerable Software Discovery Tool for Mac:	
	1. Prepare Your Mac (if not already done).	
	2. Browse to the directory where you have placed the svmscan_macos binary file.	
	3. Type the following command to install the Vulnerable Software Discovery Tool for Mac: ./svmscan_macos -i	
	sh-3.2# ./svmscan_macos -i [10/25 12:37:27.421] Initializing Flexera Software Vulnerable Software Discovery Tool 8.0.0.344 [10/25 12:37:27.453] GUID : 41713AB6-9437-4B8D-A1E6-5CA8D9883AC1 [10/25 12:37:27.493] 'Flexera SVM Scanner' service started [10/25 12:37:27.493] 'Vulnerable Software Discovery Tool' successfully installed [10/25 12:37:27.493] Vulnerable Software Discovery Tool 8.0.0.344 shutting down	

The Vulnerable Software Discovery Tool for Mac shows in the Software Vulnerability Research console approximately 15 minutes after the installation.

- 4. To launch a new scan manually under the Mac Terminal, issue the command "./svmscan\_macos -c"
- 5. Use the "-h" switch to see a full list of parameters supported by the Vulnerable Software Discovery Tool for Mac.

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

To deploy the Vulnerable Software Discovery Tool for Red Hat Linux 6 RPM and Vulnerable Software Discovery Tool for Red Hat Linux 7 RPM, see Deploy a Linux Agent.

Ē

<del>ک</del>

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

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

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

To install the RHEL agent, see Install the Vulnerable Software Discovery Tool for Red Hat Linux 6 RPM and 7 RPM.

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

## Install the Vulnerable Software Discovery Tool for Red Hat Linux 6 RPM and 7 RPM

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

For information on installing the Vulnerable Software Discovery Tool for Red Hat Linux 6 RPM and 7 RPM, see:

- Installing the Vulnerable Software Discovery Tool
- Specifying Proxy Settings for the Scanner (Recommended Method)
- Specifying the LAN Group of the Machine
- Immediately Update the RHEL Agent Configuration
- Uninstalling the Scanner RPM Package

#### **Installing the Vulnerable Software Discovery Tool**

To install the Vulnerable Software Discovery Tool for Red Hat Linux 6 RPM and 7 RPM, perform the following steps.

) E									
Task	То	To Install the Vulnerable Software Discovery Tool for Red Hat Linux 6 RPM and 7 RPM:							
	1.	The 6 RPM tool requires: bash, gzip, sed, gawk, procps, coreutils, glibc(x86-64), libcurl(x86-64), libconfig(x86-64), libuuid(x86-64), yum, yum-security							
		The 7 RPM tool requires: bash, sed, gawk, procps, coreutils, glibc(x86-64), libcurl(x86-64), libconfig(x86-64), libuuid(x86-64), yum							
	2.	Login as root at the RHEL machine and install/update the package (the same command line option works for both cases):							
		su root yum localinstallnogpgcheck: Red Hat 7 RPM: yum install <path>/svmscan linux-8.x.xxx-x.el7.x86 64.rpm</path>							

#### Red Hat 6 RPM: yum install <path>/svmscan linux-8.x.xxx-x.el6.x86 64.rpm

#### Specifying Proxy Settings for the Scanner (Recommended Method)

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

 $\sim$ 

#### Task To specify proxy settings for the scanner:

- 1. Update the proxy setting in the configuration file /etc/csia/svmscan\_conf
- 2. Login as root and restart the scanner service:

```
su root
service com.flexera.svmscan restart (RHEL 6)
```

OR

systemctl restart com.flexera.svmscan (RHEL 7)

#### Specifying the LAN Group of the Machine

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



Ŷ

#### To specify the LAN group of the machine:

- 1. Update the LanGroup setting in the configuration file /etc/csia/svmscan\_conf
- 2. Login as root and restart the scanner service:

```
su root
service com.flexera.svmscan restart (RHEL 6)
```

OR

systemctl restart com.flexera.svmscan (RHEL 7)

#### Immediately Update the RHEL Agent Configuration

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



#### To immediately update the RHEL agent configuration:

1. Login as root and restart the scanner service:

```
su root
service com.flexera.svmscan restart (RHEL 6)
OR
```

systemctl restart com.flexera.svmscan (RHEL 7)

#### **Uninstalling the Scanner RPM Package**

To uninstall the scanner RPM package, perform the following steps.



#### To uninstall the scanner RPM package;

1. Login as root and uninstall the scanner RPM package:

su root
yum erase svmscan\_linux.x86\_64

## Vulnerable Software Discovery Tool Command Line Options

You can use the following command line options for the Vulnerable Software Discovery Tool.

- Help
- Version
- Install
- Uninstall
- Modify Settings
- Controlling the Service
- Scanning from the Command Line
- Agent Configuration Options

## Help

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

SVMScan.exe -h

## Version

Print the version number of the Vulnerable Software Discovery Tool on the command line (exclusive):

SVMScan.exe -V

## Install

The following explain how to install the Vulnerable Software Discovery Tool from the command line:

- Install as Current User
- Install to Run as LocalSystem
- Install to Run as <user>
- Install to Run as <user> with <password>
- Install But Without Writing Anything to the Registry

#### **Install as Current User**

Install the Vulnerable Software Discovery Tool from the command line, with configuration options. Installs as current user, prompts for password, settings saved to HKCU:

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

#### Install to Run as LocalSystem

Install the Vulnerable Software Discovery Tool from the command line to run as LocalSystem, with configuration options. Saves settings to HKLM:

SVMScan.exe -i -L <config options>

#### Install to Run as <user>

Install the Vulnerable Software Discovery Tool from the command line to run as <user>, with configuration options. Prompts for password and saves settings to HKEY\_<user>:

SVMScan.exe -i -R <user> <config options>

#### Install to Run as <user> with <password>

Install the Vulnerable Software Discovery Tool from the command line to run as <user>, with <password> with configuration options. Saves settings to HKEY\_<user>:

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

## Install But Without Writing Anything to the Registry

Install the Vulnerable Software Discovery Tool from the command line but not write anything to the registry (also works with -R and -L):

SVMScan.exe -i -N

## Uninstall

Uninstall the Vulnerable Software Discovery Tool service, remove all settings and delete the key from the registry where the service reads them from:

SVMScan.exe -r



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

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

If the service is not installed, does nothing.

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

To uninstall the Vulnerable Software Discovery Tool service, while leaving the registry settings intact:

SVMScan.exe -r -N

To remove the service, if installed, and delete the Vulnerable Software Discovery Tool registry key from everywhere in the registry (exclusive):

SVMScan.exe --delete-all-settings

## **Modify Settings**

Save the command line setting to the registry, so the service will use it. The settings are saved to the location based on where installed the Vulnerable Software Discovery Tool reads the settings from. If the Vulnerable Software Discovery Tool is not installed, or the settings cannot be saved to the correct location, nothing is saved, an error is printed and the command aborts:

SVMScan.exe -S <config option>

## **Controlling the Service**

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

SVMScan.exe --start SVMScan.exe --restart

Stops the service if it is running (exclusive):

SVMScan.exe --stop

## Scanning from the Command Line

Run the Vulnerable Software Discovery Tool with immediate command line scan, with options. Ignores registry settings and server settings:

SVMScan.exe -c <config options>

Run the Vulnerable Software Discovery Tool with immediate command line scan for Proof of Concept environments that will process scans fast, typically less than 1 minute:

SVMScan.exe -c --urgent-scan

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

SVMScan.exe -fg <config options>

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

SVMScan.exe -fg -L <config options>
SVMScan.exe -fg -R <user> <config options>

Order of precedence:

Settings given on command line take precedence but, when running as a service, there is no command line.

• Settings from server take precedence over settings read from registry.

# **Agent Configuration Options**

The following table lists the Agent configuration options.

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

Category	Configuration Option	Description
Customer Area Option	-g/group <group></group>	Create host as a member of <group> in your Software Vulnerability Research Account (defaults to domain or langroup if unspecified).</group>
Mac Agent Option	delete-all-settings	Deletes all information, including Globally Unique Identifiers (GUID), from the system to ensure it is clean to accommodate a new installation.

Category	Configuration Option	Description
Network Settings	-Ddirect-connection	Bypass proxy, use direct connection.
	forcehttps	Force HTTPS, regardless of port.
		When this option is not specified, we default HTTPS on port 443 and HTTP on other ports. This option is for debugging purposes.
	ignore-ca	Ignore unknown certificate authority.
	ignore-cn	Ignore invalid Common Name in cert.
	ignore-crl	Ignore Certificate Revocation list.
	pac-url <url></url>	Proxy Autoconfig url
	request-timeout <minutes></minutes>	Sets a timeout on network connections. Set for 1-10 minutes or use 0 for no timeout.
		Use this option to increase the timeout period of HTTP requests to prevent the timeout error when the server does not respond in 2 minutes.
	-U <user:pass>proxy-user <user:pass></user:pass></user:pass>	Set proxy credentials (saved in encrypted form).
	use-network-winhttp	Enable WinHttp network stack.
		Use WinHTTP when you want the agent to control the behaviors of the HTTP Internet protocol. We default WinHTTP to force using TLS 1.2. Also, the command line options for proxy such as -x, -U, and -D are designed to work in conjunction with WinHTTP. This option is for debugging purposes.
	use-network-wininet	Enable WinInet network stack (default).
		Use WinINet when you want to control the behaviors of HTTP Internet protocol using the Internet Options. Since WinINet does not have services support, the agent running as a service ignores this option. This option is for debugging purposes.
	-x <proxy:port>proxy <proxy:port></proxy:port></proxy:port>	Set proxy.

Category	Configuration Option Description			
Proxy Options	-D/direct-connection	Force direct connection, overriding default internet proxy settings.		
	pac-url <url></url>	Specify the URL of the Proxy Auto Configuration file (.pac/.dat).		
	-U/proxy-user <user[:pass]></user[:pass]>	Specify Proxy authentication.		
	-x/proxy <host[:port]></host[:port]>	Use HTTP proxy on given port.		
Scan Options	check-wmi	Use WMI to get Windows updates.		
		Use this option to query Windows updates on SCCM using WMI in addition to a query using Windows Update Agent.		
		This option could be used to see if the SCCM client on the device/host can be used for reporting missing KBs.		
	-t/type	Software scan type:		
		• <b>Minimal Scan</b> —Scan Type 1: Inspect applications in default locations only.		
		• <b>Optimal Scan</b> —Scan Type 2: Inspect applications in non-default locations.		
		• <b>Full Scan</b> —Scan Type 3: Inspect all .dll, .exe, and .ocx files.		
		For details, see Scan Types.		
	-w/no-os-update/no-win- update	Do not connect to Windows Update.		
	wua-proxy <0,1 or	Configure proxy settings for Windows Update.		
	host[:port]>	• 0: Use the default setting.		
		• 1: Use the proxy configured with -x/proxy.		
		• <host[:port]> Manually set the proxy host and port.</host[:port]>		

Category	Configuration Option	Description	
Scan Settings that	-g <group>group <group></group></group>	Group name for association	
Server can overnue	-n <minutes>Mcheckin- interval <minutes>M</minutes></minutes>	Set Check-in interval.	
	-n <hours>Hcheckin- interval <hours>H</hours></hours>		
	-wno-win-updateno-os- update	Disable windows update check.	
Security Options	ignore-ca	Ignore Unknown SSL Certificate Authority (CA).	
	ignore-crl	Ignore SSL Certificate Revocation Check.	
	ignore-cn	Ignore Invalid SSL Certificate Common Name (CN).	
Server Options	userid <userid></userid>	Set the Software Vulnerability Research access user ID.	
	token <token></token>	Set the Software Vulnerability Research access token.	
	host <hostname></hostname>	Set the Server hostname.	
	port <port></port>	Set the Server port.	

Category	Configuration Option	Description
Service Options	delete-all-settings	Delete all settings related to this program from the registry.
		Deletes these settings from all registry keys.
	dry-run/dryrun	Run up to the point of scanning without writing any changes and then exit (useful to log the configuration).
		Use this option to examine if the agent is able to run and communicate with the server. It will exit before scanning and won't make any changes to the system. You can use this option along with -c.
	-i/install	Install service.
	-L/localsystem	Run the service as the LocalSystem user.
	manual	When installing, set service to only be started manually, rather than automatically
	-N/no-registry-write	When installing, do not write any settings to registry.
		When removing, do not delete settings from registry.
	-p/copy <dest></dest>	Before installing, copy executable file to <dest> and install the service to run from <dest>.</dest></dest>
	-r/remove	Remove service.
	-R/runas <user[:pass]></user[:pass]>	Specify the user the service should run as.
		For a domain user type "user@domain" or "domain\user"
	-S/only-save-settings	Only save settings from the command line to registry, as the relevant user.
		Does not run, install or remove.
		Use this option when you want to modify the agent registry settings after the agent is installed. You need to restart the agent service to make the changes effective.
		This option could be used to edit the server options like userid/token/host/port stored in the registry.
		This setting is the opposite of "-N" options. If -N is used, no registry setting will be edited.

Category	Configuration Option	Description
Service Recovery Settings:	service-failure-actions <actions></actions>	Failure actions and their delay time (in milliseconds), separated by / (forward slash) – e.g., run/5000/reboot/ 800. Valid actions are <run restart reboot>. (Must be used in conjunction with theservice-failure- reset option)</run restart reboot>
	service-failure-command <command line=""/>	Command line to be run on failure.
	service-failure-flag	Changes the failure actions flag setting of a service. If this setting is not specified, the Service Control Manager (SCM) enables configured failure actions on the service only if the service process terminates with the service in a state other than SERVICE_STOPPED. If this setting is specified, the SCM enables configured failure actions on the service if the service enters the SERVICE_STOPPED state with a Win32 exit code other than 0 in addition to the service process termination as above. This setting is ignored if the service does not have any failure actions configured.
	service-failure-reboot <message></message>	Message broadcast before rebooting on failure.
	service-failure-reset <period></period>	Length of period of no failures (in seconds) after which to reset the failure count to 0 (may be INFINITE). (Must be used in conjunction withservice-failure- actions)

# **Scanning Via Local Agents**

Software Vulnerability Research provides different Scan Types, 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 Vulnerable Software Discovery Tool will run silently in the background.

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

# Scan Types

Under Scan Configuration settings, you will be asked to select a scan type, which are compared below.

Table 8-4 • Scan Types

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



# **Assessment Reports**

Edition • This Assessment module is not available for Software Vulnerability Research.

The Assessment pages display where software vulnerabilities are installed across your organization by device and product. A list of advisories is also provided to address software vulnerabilities.

Overview

♬

- Devices
- Products
- Advisories

# **Overview**

The **Overview** page displays a tree view of the Device Groups within your environment. Click an item under the My Environment listing to view the **Average System Score**, **Device Details**, **Last Scan Details**, and **Product Details** of the security status of the Device Group.

You can customize your Device Groups using Smart Groups.

Click the Devices, Products and Advisories tabs to view detailed information regarding the selected Device Group.



*Important* • You must first download and deploy Software Vulnerability Research's Scan Agent to scan your devices. Refer to Downloads for further information.

Assessment > Overview					0 -
Overview Devices Product	ts Advisories				
✓ <sup>I</sup>		My Environment			
> 🖬 com					
> 🗰 local		Average System Score		Devices - System Score	
		Flexera Average System Score:	80.05	100 3	
		Advisories:	224	80-99 11	
✓	e	Devices Details		<50 0	
►=18		Insecure Devices:	17	Unknown 0 Not Calculated 0	
🖬 <18th		Secure Devices:	3		
		Total:	20		
		Last Scan Details			
		Status Unknown:	0		
		Successful:	18		
		Windows Update Failed (Partial Scan):	2	Products - Status	
		Total:	20	Secure 349	
		Product Details		End-of-Life 25	
		Insecure:	62	Insecure 62	
		End-Of-Life:	25		
		Secure:	349		
		Total:	436		
		<b>CN L L</b>			
		U Refresh			

## **Smart Groups**

Smart Groups organize your environment by defining specific groups of devices, products, or advisories to identify and meet regulatory needs that are situation specific. These Smart Groups filter assessment results and reports to prioritize remediation efforts.

This section includes the following Smart Group topics:

- Smart Group Selection Order
- Create a Smart Group
- Create a Smart Groups Report

## **Smart Group Selection Order**

To create a Smart Group, you can use any combination of device, products and advisories conditions. However, the order in which conditions are evaluated is this: device conditions filter out the devices on which the following conditions are applied; products conditions filter out devices without those products installed; advisory conditions filter out products and devices without those conditions. Following are some sample Smart Group selections.

- Only device conditions—Select those devices and show all products and advisories detected on those devices
- Only product conditions—Select the devices that have the products installed and show devices and advisories for those products
- Only advisory conditions—Select the devices and the products that have those advisories associated
- All types of conditions—Select the devices; then select devices with the product conditions and eliminate devices or products that do not have the advisory conditions. This selection order ensures that a group with the conditions "Windows platform, Python product installed, Highly and extremely critical advisories" show devices that have a Python product with highly critical advisories. This selection order also ensures you do not include devices with critical advisories on products that are not Python.

• **Product secure type**—Is context dependent on the list of devices; a product can be insecure on one device and secure on other devices (Example: Windows may be insecure depending on the KBs installed on the device). For example, if you create a Smart Group "Devices from AD group "NorthAmerica" and insecure products", you might not get "Windows 8" as insecure in your Smart Group list, although you see it as insecure in the full product list, since Windows 8 is secure on all devices in your Active Directory (AD).

## **Create a Smart Group**

To create a Smart Group, perform the following steps.

То с	create a Smart Group:	
1.	Click the green + sign next to My Smart Grou	ps.
	Assessment > Overview	
	Overview Devices Products Advis	ories
	✓	
	> 🚔 com	
	> 🛱 local	
	🗸 🗗 My Smart Groups	•

Create Smart Group					×
Name					
Smart Group Name					
Priority					
Normal					Ŧ
Conditions:					
Device Conditions					
Select Device Condition	•				× +
Product Version Conditions					
Select Product Condition	•				× +
Advisory Conditions					
Select Advisory Condition	-				× +
		Consul	Cours		
		Cancel	Save		

**3.** Select the Priority.

## 

**Note** • The priority determines how often a smart group recalculates to show the latest results. The more critical the priority, the more often the results are calculated to reflect the latest data, with the following mention: if all groups are critical, none are critical. The exact frequency with which results are being recalculated can't be determined or

guaranteed as it depends on the number of groups in your environment (both Active Directory groups and Smart Groups) and the priorities set on all Smart Groups.

4. Select the desired combination of Device, Product Version, and Advisory Conditions. Click the green + sign to add multiple conditions under the corresponding category.

_

**Note** • Device Platform is limited to Windows, macOS, and RedHat Enterprise Linux. If you want to select a particular operating system (Example: Windows 8), Select Windows as the Device Platform, add Device Condition "Operating System In", click "Select Operating System(s)", enter Windows 8 in the search tab, and click Save.

**Note** • To make sure date filters like Last Scan Date or Advisory Released conditions reflect the User Interface selection, ensure that your User Profile includes your time zone preference (Default time zone is set to Europe/Copenhagen). To change your time zone, go to User Profile and click Edit. Under Preferences, select the appropriate Timezone, and click Save.

**Note** • For the Advisory CVSS Score condition, Flexera applies the condition to the CVSS3 value if the advisory has CVSS3 data. Otherwise, the condition is applied to the CVSS2 score.

- 5. Click Save. The newly created Smart Group folder will now appear under My Smart Groups.
- **6.** You can now click Refresh to view the associated Overview, Devices, Products, and Advisories information. The data is calculated asynchronously, so you will need to change the group selection (or potentially refresh the page) to see the latest data.

Overview	Devices	Products
🗸 🕫 My Envir	onment	
> 🖀 com		
> 🛍 No-4	Active-Directory	
🗸 🖓 My Smar	rt Groups	Ð
🖬 Mac		
💼 Red	Hat	

**Note** • In the Smart Groups Overview tab is a field titled "Latest data available" with the options "Yes" or "No". For Active Directory (AD) groups, a "Yes" response means that no device in the folder tree underneath the AD sent new data. For Smart Groups, a "Yes" response means no device in a customer's environment has sent new data. When a new device for either an AD group or Smart Group sends data, the "No" option appears until the group is reprocessed by the system. Once the group's results are recalculated, the "Yes" option will reappear.

**Note** • The products counts on the device tab represent the total number of products installed on the device, regardless of the product conditions. The products and advisories counts on the products and advisories tabs are cross conditions. For example, for conditions "Adobe Flash products, Highly critical advisories", the counts will represent: **Device product counts**: total number of products installed, not just Adobe Flash products; **Product advisory counts**: number of Highly

critical advisories affecting the product; **Advisory product counts**: number of Adobe Flash products affected by the advisory.

### **Ensuring an Accurate Advisory Count**

To ensure an accurate advisory count between the Assessment module's User Interface (which considers the user's timezone and the Assessment module's filters for the whole day) and the user-generated Assessment Report, use the following date filters to create a list of advisories released on a specific date (Example: March 31, 2018):

- For the Advisory Initial Release Date and Advisory Current Release Date conditions, enter 2018-03-01.
- In the Assessment > Advisories > Advisory List From (date) To (date) filters, enter 2018-03-01 in the From (date) filter and 2018-03-02 in the To (date) filter.

## **Create a Smart Groups Report**

To create a Smart Groups Report, perform the following steps.

Task	То	create a Smart Groups report under Analytics > Reports:
	1.	Click the green + button and select Add Assessment Report.
	2.	When the <b>Configure New Assessment Report</b> pop-up window appears, under <b>Device Groups</b> select the appropriate Smart Group under the <b>My Smart Groups</b> listing.
	3.	Select any other appropriate report conditions and click <b>Save</b> . The new report will be listed under <b>Analytics</b> > <b>Reports</b> .
	4.	To save the report as a CSV file or PDF file:
		<b>a.</b> Select the appropriate Smart Group listing in the grid.
		b. Click View Files.
		c. Click Generate PDF.
		d. Click <b>Download</b> once the file is generated.
	No	te • For recurring reports based on a Smart Group, the Smart Group contents are recalculated, based on the conditions

# **Devices**

-

The Devices page displays the details of the scan configuration status of all Devices or machines within your environment.

The Last Scanned column refers to the last time the Vulnerable Software Discovery Tool (Daemon) submitted scan data to the user interface. The time stamp in the **Last Scanned** column refers to the local time zone of the scanned server.

The **Last Processed** column refers to the last time LiveUpdate identified any new advisories that have come in since you last scanned your system.

Overview Devic	es Products	Advisories								
wsing 20 devices 🦸										<b>•</b>
Device Name		Platform	-	System Score	~	Is Secure	-	Last Scan Status	<ul> <li>Days Since Last Sci</li> </ul>	in
									Apply	Reset
								Filter	- Save	Delete
vice Name - O	perating System		System Score	Secure Products	Insecure Products	EOL Versions	Last Scanned	Last Processed	Last Scan Status	Inventory Source
	licrosoft Windows 8.1		80	21	1	4	May 22, 2018 7:33 AM	Jun 4, 2018 10:08 AM	Successful	8.0.0.309

Task

#### To view devices:

- 1. Open the Assessment > Devices > Device List page.
- 2. Click I and select from the drop-down lists to filter the Devices by **Device Name**, **Platform** (Windows, macOS, or RedHat Enterprise Linux), **System score** (100, 80-89, 50-79, <50, Unknown, or Not Calculated), **Is secure** (Yes or No), and **Days since last Scan**.
- 3. Click the Apply or Reset buttons to apply or reset the filters.
- 4. Click the **Save** or **Delete** buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.
- 5. Click an item in the grid to select Device details, Installed products, Advisories, Queue scan or Delete.
- 6. Click determined to export the results to a CSV file.

## **Device Details**

The Device Details page displays Overview, Installations and Advisories details for the selected Device.

×

# **Task**

#### To view device details:

1. In the **Overview** tab, click an Installed or Missing **KB Details** link to view detailed KB information. The selected KB Details will be highlighted.



#### Device KB Details

Installed					
КВ	Title	Description		Published On	
<u>KB4287903</u>	Security update for Adobe Flash Player: June 7, 2018	Fixes vulnerabilities in Adob	e Flash Player on certain versions of Windows.	Jun 12, 2018 12 PM	2:17
KB4338825	July 10, 2018—KB4338825 (OS Build 16299.547)	Learn more about update KE to get the update.	34338825, including improvements and fixes, any known issues, and how	Jul 16, 2018 4:2 PM	27
KB4338832	Security update for Adobe Flash Player: July 10, 2018	Fixes vulnerabilities in Adobe	e Flash Player on certain versions of Windows.	Jul 10, 2018 12: PM	:08
Missing					
КВ	Title		Description	Published	l On
KB2538243	MS11-025: Description of the security update for Redistributable Package: June 14, 2011	or Visual C++ 2008 SP1	Resolves a vulnerability in certain applications that are built by using the Microsoft Foundation Class (MFC) Library.	Apr 11, 20 2:48 AM	17
			Close		

2. Click <sup>III</sup> in the Installations and Advisories tabs to export the results to a CSV file.

**3.** In the **Installations** tab, click a Device in the grid to can find further information regarding the device's **Missing KB(s)** for insecure Microsoft products, **Product details**, and **Available Patches**.

	CC3 7 DEVICE DECENS						
erview [	Devices Products Advisories						
Device	Overview Installations Ad	visories					
Installations	260 Insecure Installations 9 Secure Installations	241 EOL Installations	10				
Installations wsing 9 install	200 Insecure Installations Secure Installations lations	241 EOL Installations	10				
Installations wsing 9 install <b>vice :</b>	Insecure Installations         Secure Installations           lations         Product	241 EOL Installations	10 Architecture	Secure type 💠 Last	scan	¢ Path	
Installations wsing 9 install vice :	Insecure Installations     Secure Installations     Insecure Installations     Product     Microsoft Visual C++ 2008 Redistributable Package	201 EOL Installations Version 9.0 21022.8	10 Architecture Windows Intel 64-bit	Secure type 💠 Last Insecure Aug 2	scan 27, 2018 8:00 AM	Path C/Program Files/Common Files/Microsoft Shared/V/Cimsda90 dll	_

4. In the Advisories tab, click an SAID in the grid to view detailed information regarding the Advisory.

rview Devic	es Products	Advisories							
Device "	" Overvi	ew Installations Advisories							
									_
wsing 7 advisories (	I.								<b>4</b>
vsing 7 advisories ( SAID	i.	Tide	CVE	Criticality	*	From	1	То	Ŧ

# **Products**

The Products page displays the details of all Products within your environment.

Assessment > Products > Pro	duct List						€ -0
Overview Devices	Products	Advisories					
Browsing 1-20 of 397 products	I						<b>T</b>
Product status	*	Product name	Vendor name				Apply Reset
					Filter	-	Save Delete
Product name		- Vendor name	Patch version	n Insecure installations	End of life installations	Secure installations	Installations
7-zip 15.x			16.x	0	1	0	1
7-zip 16.x				0	0	4	4
				Product details Installations	Advisories		

Task

#### To view products:

- 1. Open the Assessment > Products > Product List page.
- 2. Click I and select from the drop-down lists to filter the Products by **Product Status** (Secure, Insecure, or EOL), Product name, and Vendor Name.
- 3. Click the Apply or Reset buttons to apply or reset the filters.
- 4. Click the **Save** or **Delete** buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.
- 5. Click an item in the grid to select Product details, Installations or Advisories.
- 6. Click 📥 to export the results to a CSV file.

# **Product Details**

¢

The **Product Details** page displays **Overview**, **Installations** and **Advisories** details for the selected Product.

## Task To view product details:

- 1. In the Advisories tab, click an SAID in the grid to view detailed information regarding the Advisory.
- 2. Click 🛃 in the Installations and Advisories tabs to export the results to a CSV file.

sessment > Products > Product D	etails		8 ->
Overview Devices Pr	oducts Advisories		
<ul> <li>"7-zip 16.x" Overview</li> </ul>	Installations Advisories		
Product details		Installations	
Name: Vendor:	7-zip 16.x	Secure 0 End-of-Life 2	
Is end of life: Research Created:	Yes May 10, 2016	insecure o	
Devices Details			
Insecure Devices:	2		
Secure Devices:	0		
Total: Product Installations	2		
Insecure:	0		
End-Of-Life:	2		
Secure:	0		
Total:	2		

ssessment > Products	>	Product Details	
----------------------	---	-----------------	--

**∂** -**1** 

Overview Devices Pro	ducts Advisories						
<ul> <li>"7-zip 16.x" Overview</li> </ul>	Installations Ad	visories					
All Installations  Insecure Inst Browsing 9 installations	allations 0 Secure Ins	tallations 9 EOL Ins	tallations 0				Ŧ
Device	<ul> <li>Product</li> </ul>	Version	Architecture	Secure type	Last scan	Path	
	7-zip 16.x	16.0.0.0	Windows Intel 32-bit	Secure	Mar 12, 2018 10:38 AM	Construction and the second second	
				Device details			

Assessment > Products > Product Details								0 -
Overview Devices Products	Advisories							
<ul> <li>"7-zip 15.x" Overview Installa</li> </ul>	ations Advisories							
Browsing 1 advisories 🦸							*	₹
SAID	Title	CVE	Criticality	From	-	То		
CVSS Score Min	CVSS Score Max	Solution status 💌	Where -	Impact	-	Apply	Reset	
SAID Release Date - Mor	dified Date 💠 Title		Criticality	Where	CVSS Score	Devices	Products	¢
SA70636 2016-05-18 201	6-05-18 7-zip HFS and UDF File H	andling Two Vulnerabilities	No Fix	From remote	10	3	2	

# **Advisories**

The Advisories page displays the details of all Advisories applicable to your environment.

On this page you can:

- View Advisory Details
- Create Advisory Tickets

Asse:	sment > A	Advisories > Ad	visory List																		0 J
0\	erview	Devices	Products	Adv	isories																
Brow	ing 1-20 of	289 advisories 1	i																		7 ±
Ze	ro Day		•	Impact		•	CVE(s)	SAID		From				То			Criticality				-
Se	lution status		•	Where		•	CVSS Score Min	CVSS Score M	800								A	oply		Rese	rt
														Filter		٠	S	ave		Delet	te
SAID	Re	elease Date	Modified Date	• •	Title						Criticality	Zero Day	Soli	ition Status	Where	cv	SS Score	\$	Devices	• Prode	ucts 🗢
<u>SA82</u>	609 201	18-04-20	2018-04-20		Red Hat update for java-1.8.0-openjde	k						No	Ven	dor Patched	From remote	7.6			1	1	
							Advisory details	Devices	Prod	lucts	Installations	Create tick	et								

📋 Task

#### To view advisories:

- 1. Open the Assessment > Advisories > Advisory List page.
- Click I to filter the Advisories by Zero Day (yes/no), Impact (select from the drop-down list), CVE(s), SAID, From and To dates, Criticality (select from the drop-down list), Solution status (select from the drop-down list), Where (select from the drop-down list), CVSS Minimum Score, and CVSS Maximum Score.



**Note** • To search for multiple advisories at the same time to determine which advisories apply to more than a single CVE for which you have interest, enter the CVEs in the **CVE(s)** filter and leave one space between entries (Example: CVE-2014-0224 CVE-2014-0160 CVE-2013-0169 CVE-2009-3555 CVE-2015-7575).

- 3. Click the Apply or Reset buttons to apply or reset the filters.
- Click the Save or Delete buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.
- Click a SAID in the grid to view the Advisory or click an item in the list and select Advisory details, Devices, Products
  or Installations that the Advisory relates to.
- 6. Click 🗳 to export the results to a CSV file.

## **Advisory Details**

The Advisory Details page displays Overview, Devices, Products and Installations details for the selected Advisory.

Click 🗳 in the **Devices**, **Products** and **Installations** tabs to export the results to a CSV file.

Under **Advisory Details > Overview** is a Zero Day field. Zero Day refers to a vulnerability that is actively exploited prior to its disclosure. A zero day is one criteria to increase criticality. For example, a typical "Highly Critical" vulnerability becomes an "Extremely Critical" vulnerability.

vsing 1 products 2 Product name rduct name rosoft Windows 8.1 ment > Advisories > Ac view Devices "SA81927" Overvir installations 22 Insee installations 22 Insee installations 22 Insee wsing 1-20 of 22 Installations ice c	dvisory Details Products Ac ew Devices cure Installations  Product Google Chrome 64 x	Products Secure Installat Version 64.0.3282	Installations Installations EOL Installation Contents Con	IS 22 Secure type	scan ¢ Path 17, 2018 9:52 AM C:IPron	ram Files (x86)/goode/chrom	elapplication/chrome.exe		
vsing 1 products # Product name vduct name rosoft Windows 8 1  rrent > Advisories > Ac view Devices  "SA81927" Overvi  nstallations 22 Insect vsing 1-20 of 22 Installati	dvisory Details Products Ac ew Devices cure Installations C	Visories Products Secure Installat	Installations	is 22					
vsing 1 products 2 Product name vduct name rosoft Windows 8 1 ment > Advisories > Ac vview Devices "SA81927" Overvia nstallations 22 Insector	dvisory Details           Products         Ac           ew         Devices           cure Installations         Image: Constant Science Sc	Products Secure Installat	Installations	ns <b>22</b>					
vising 1 products # Product name roudt Yindows 8 1 ment > Advisories > Adv view Devices "SA81927" Overvie	dvisory Details Products Ac ew Devices	Products	Installations	-					
vsing 1 products # Product name duct name osoott Windows 8.1 nent > Adivisories > Ac view Devices "SA81927" Overvir	dvisory Details Products Ac ew Devices	<b>lvisories</b> Products	Installations						
vising 1 products 2 Product name duct name occont Windows 8 1 nent > Advisories > Ac view Devices	dvisory Details Products Ac	lvisories							
vsing 1 products 2 voduct name duct name osoft Windows 8.1 nent > Advisories >	dvisory Details								
vsing 1 products 🦸 Product name duct name rosoft Windows 8.1									
vsing 1 products 🦸 Product name duct name osoft Windows 8.1									
roduct name duct name osoft Windows 8.1				Product details	Installations Advisories				
ising 1 products 🥻	<ul> <li>Vendor r Microsoft</li> </ul>	name 1	Patch version	Insecure installations 6	End of life installa 0	stions	Secure installations     0	Installations 6	
ising 1 products 🧋	Ve	endor name		Product status  Apply	Reset				
ising 1 products									- <b>T</b>
Shor 555 Overvi	Jevices	. routes							
"SA81995" Overvi	iew Devices	Products	Installations						
view Devices	Products A	dvisories							
nent » Advisories -	utuicony Dotoile								
	Microsoft Windows	0.1	82 Dev	vice details Installed products	Advisories Queue scan	Delete	Mar 12, 2016 10:20 AM	8.0.0.300	
vice Name	Operating System		System Score	Secure Products	Insecure Products	EOL Versions	Last Scanned	Inventory Source	
Vevices 11 Insecure l	Devices 11 Secure D	levices 0							*
"SA81927" Overvie	ew Devices	Products II	istallations						_
		Decident							
rview Devices	Products	visories							• 1
									-
)escription:									
dvisory Detail	s:								
Google Chrome	<u>61.x</u>			CPE	: N/A				
oftware									
Affected operat	ting system and	software							
CVE references			CVE-2017-5122   C	<u>VE-2017-5121</u>					
				,					
Secunia CVSS S	cores		Base: 10, Overall: 7 (AV:N/AC:L/Au:N/C:	7.4 C/I:C/A:C/E:U/RL:OF/RC:C)					
Solution Status			Vendor Patched						
Where			From remote						
Impact			Unknown, System a	ccess					
Zero Day			No						
Criticality			- High	ly critical					
Creation Date			2017-09-22						
Secunia Advisory	/ ID		SA79042						
	ne Multiple V	ulnerabil	ities						
Google Chron									
Google Chron	" Overview	Devices	Products	Installations					
"SA79042'									

## **Create Advisory Tickets**

From the **Assessment > Advisories > Advisory List** page, you can create advisory tickets to remediate vulnerabilities affecting your devices.

# Task

#### To create Advisory Tickets:

1. Select the appropriate advisory in the grid and click **Create Ticket**. When the **Create Ticket** pop-up window appears, the Secunia Advisory ID will be populated in the **Advisory** field.

Overview Devices Produ	ucts Advisories										
wsing 1-20 of 224 advisories 🦸											<b>7</b> ±
SAID Release Date	<ul> <li>Modified Date</li> </ul>	Title			Criticality	Zero Day	Solution Status	Where	CVSS Score	Devices	Products
SA83543 2018-06-04	2018-06-04	Apple iTunes Multiple \	fulnerabilities			No	Vendor Patched	From remote	8.8 v3	1	1
			Advisory details	Devices	Products	Installations	Create ticket				
Create ticket		×									
dvisory											
SA83543											
itatus											
Status		•									
Priority											
Priority		•									
Queue											
Queue		•									
Assigned to											
Assigned to		•									
Add comment											
Add comment											

- 2. From the **Status** drop-down list, select the appropriate status. The default ticket statuses are **Open**, **Handled**, **Closed**, or **Irrelevant**. See Default Ticket Statuses in Ticket Manager for more information.
- **3.** From the **Priority** drop-down list, select the appropriate priority. The default ticket priorities are **Low**, **Medium**, **High** or **Urgent**.
- 4. From the Queue drop-down list, select a queue to assign the ticket to.
- 5. From the Assigned to drop-down list, list, select an individual to assign the ticket to.
- 6. In the Add comment field, add an appropriate comment to the ticket (mandatory).
- 7. Click Save.

# **10** Patching

#### *Edition* • The Patching module is not available for Software Vulnerability Research.

The patching feature in Software Vulnerability Research remediates software vulnerabilities in third-party applications. Software Vulnerability Research provides Patch and Grouped Patch Libraries that list all patches available for your environment, provides patch templates and build packages to deploy patches, and tracks deployed patches.

- Patch Library
- Templates
- Packages
- Deployment
- Patching Tickets
- Manual Signatures



凤

Important • Before you can patch, the following Daemon for Windows activities must be completed first.

- Install the Daemon
- WSUS Configuration and Certificate Troubleshooting
- Saving Successful WSUS Self-Signed Certificates
- Create a Group Policy to Deploy Your Certificate

# **Patch Library**

The Patch Library page displays details of all patches available for your environment.

Patch Library Templa	ates Packa	ges Deployment											
owsing 1-20 of 74 patches 🧋													<b>.</b>
Affecting my environment	-	WE	Product ne	ame		Vendorname			Secure version		SA	D	
Has template	•											Apply	Reset
									Filter		-	Save	Delete
roduct	= \	fendor	÷ Sect	ire version	•	Edition	SAID	Criticalit	y	Has template	Las	t updated	
racle Java JRE	0	Dracle Corporation	8u17	1			SA82703			Yes	Ар	18, 2018 3:21 AM	

#### Task To view patches:

- 1. Open the Patching > Patch Library page.
- 2. Click ✓ to filter the patches by Affecting my environment (yes/no), CVE, Product name, Vendor name, Secure version, SAID, and Has template (yes/no). In the Patch Library grid, the default sorting view includes sorting first by the Vendor column (A-Z) and then by the Product column (A-Z).
- 3. Click the Apply or Reset buttons to apply or reset the page layout.
- 4. Click the **Save** or **Delete** buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.
- 5. Click an item in the grid to select View templates (if a template already exists), Create patch template or Build packages.
- 6. Click 🗳 to export the results to a CSV file.

To select and deploy patches in your environment, see Patch Template and Build Package.

# Templates

The **T**emplates page displays a list of Patch templates that you have created and saved. Each template is linked to the specific product version the template was created for.

Patchi	ng > Templates							0	Ð
Pate	ch Library Templates Pa	ckages Deployment							
Browsin	ng 7 templates 🦸							T Actions	-
Ten	nplate name	Architecture	▼ Language	÷				Delete selected templates Apply Reset	d,
						Fit	er	- Save Delete	I
	Template name	<ul> <li>Product</li> </ul>	Architecture	Edition	Languages	Created by	Created	Last updated	٥
	APR18_Oracle Java JDK	Oracle Java	IDK 32-bit/64-bit		-	YojanaY	Apr 18, 2018 4:48 AM	Apr 18, 2018 4:48 AM	
				Edit View pack	ages Delete				

Task

#### To view templates:

- 1. Open the **Patching > Templates** page.
- 2. Click 🗹 to filter the templates by Template Name, Architecture, or Language.
- 3. Click the Apply or Reset buttons to apply or reset the filters.
- 4. Click the **Save** or **Delete** buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.

- 5. Click an item in the grid to select Edit, View Packages, or Delete.
- 6. To delete multiple templates, select the appropriate templates in the grid and click the Actions button.
- 7. Click dependence of the results to a CSV file.

# **Packages**

The Packages page displays details of all packages available for your environment.

Patcl	ning > Packages														e	<b>}</b> -₹
Pa	tch Library Templates	Packages	Deployment													
Brow	sing 13 packages 🦸														🝸 🕹 Act	ions 🔺
	inguage	• Package	name		Vendor name			Package statu		Ŧ	Platform		*	Architecture	Publish selected pack Delete selected packa	ages Jh iges
														Apply	Reset	
											Filter		*	Save	Delete	
	Package name			÷ Ve	endor	٠	Status	Platform	Architecture	Minimum	version	Last status update		Template name		
	Mozilla Thunderbird_Automation to very	sion 52.7 English (U	5)	M	lozilla Foundation		Ready	All	32-bit	1.0.0.0		Apr 23, 2018 3:37 AM		Mozilla Thunderbi	ird_Automation	
	Mozilla Thunderbird_Automation to very	sion 52.7		14	lozilla Foundation		Ready	All	32-bit/64-bit	1.0.0.0		Apr 23, 2018 3:37 AM		Mozilla Thunderbi	ird_Automation	
					Details Dow	nlo	ad Create deploy	ment Vie	w deployments	Delete						

ĭ Task

#### To view packages:

- 1. Open the Patching > Packages page.
- 2. Click I to filter the packages by Language (select the required installation language or languages from the dropdown list), Package name, Vendor name, Package status (select Not ready, Building, Ready or Error building from the drop-down list), Platform (select All, Windows, Mac, Red Hat, Android or IOS from the drop-down list), and Architecture (select 32-bit, 64-bit or 32-bit/64-bit from the drop-down list).
- 3. Click the Apply or Reset buttons to apply or reset the filters.
- 4. Click the **Save** or **Delete** buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.
- 5. Click an item in the grid and select Details, Download, **Create deployment**, **View deployments**, or **Delete** to view the package deployment details for the selected item. Select the check boxes next to the grid items to select from the Actions drop-down menu.
  - **Details** provides information regarding the package's unique metadata and origin.
  - Download allows you to store the physical file for initial testing purposes before deploying it.
  - Create deployment provides options for where you want to publish the patches.
  - View deployments takes you to the Deployment menu. You can filter this view to show similarly deployed packages.
  - Delete packages.
- **6.** To publish or delete multiple packages, select the appropriate packages in the grid and click the appropriate option under the **Actions** button.

**Note** • If you choose to publish the selected packages, you must select the server(s) to publish the package to in Package Deployment.

**7.** Click **I** to export the results to a CSV file.

# Deployment

The Deployment page displays details of all patches published in your environment.

Patching > Deployment										8 -1
Patch Library Templates	Packages	Deployment								
Browsing 4 deployments 🦸										Y & Actions -
Package	Vendor		Server	•	From		То		Status	Delete selected deployments
									Apply	Reset
							Fit	2er	▼ Save	Delete
Package name		Vendor	Published to	Deployed to	Status	Count Installed	Count Failed	Count Pending	Count Not Applicable	Last status update 🔹
Apr20_Apple iTunes to version 12.7.4		Apple	And Personnel and Personnel and		Loaded	0	0	16	4	Apr 20, 2018 5:04 AM
			Information	Refresh status Upda	ate Deploym	ent Delete Deplo	yment			

Task

#### To view deployments:

- 1. Open the Patching > Deployment page.
- 2. Click 🔽 to filter the deployments by Package, Vendor, Server, From and To dates, and the Status Options:
  - Pending
  - Loaded
  - Completed
  - Failed
  - Pending Delete
  - Deleted
  - Waiting for signature
- 3. Click the Apply or Reset buttons to apply or reset the filters.
- Click the Save or Delete buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.
- Click an item in the grid, and you should see the options Information, Refresh status (of the Daemon), Update Deployment, or Delete Deployment.
- 6. To delete multiple deployments, select the appropriate deployments in the grid and click the **Actions** button.
- 7. Click 🗳 to export the results to a CSV file.

# Information

After clicking Information, you can view the package deployment details for the selected item.

Deployment Information - Chrome 70.x 31st Oct to version 70.x

Deployment inform	ation
Server	cm12sql
Groups	
Package name	Chrome 70.x 31st Oct to version 70.x
Product name	Google Chrome 69.x
Vendor name	Google
Status	Pending
Created	Oct 31, 2018 10:11 PM
Group Publish Deta	ils
Deployment tasks	
Task type	Push package to Patch Server
Created	Oct 31, 2018 10:11 PM
Result	New

## **Update Deployment**

If you need to see where a package has been published or you need to change the publishing options for one or more patches, click Update Deployment and the **Choose where to publish the patch(es)** dialog box will open. Make the needed changes and click OK.

# **Patching Tickets**

After you Create a Workflow Rule to Create a Patching Ticket, you can view and export patching ticket information and delete patching tickets.

Pat	tching	g > Ticke	ts > Ticket List										0 -1
	Patch	Library	Templates	Packages	Deployment	Tickets							
Ор	en tid	kets 17											
Bro	wsing	17 ticket	i										<b>Y</b> ±
L.		a 4	Ticket created	Queue	Status	Priority	Product	Vendor 🗢	Secure Version	Edition	Patch Criticality	SAID	Assigned to
	2	4862	2018-07-11	Default	Open	High	Adobe Reader XI	Adobe Systems	18.x (Continuous)			SA83983	
							Affected Devi	ices View Edit (	Delete				

Task

To view and export patching tickets:

- 1. Open the Patching > Tickets page.
- To filter the results by ticket status, select one of the bold ticket statuses in the upper-left-hand corner followed by a ticket count. The default ticket statuses are **Open**, **Waiting**, **Handled**, and **Irrelevant**. See Default Ticket Statuses in Ticket Manager for more information.
- 3. Click 🔽 to filter the results by ID, From and To dates, Queue, Priority, product, vendor, SAID, and Assigned User.
- 4. Click the Apply or Reset buttons to apply or reset the filters.

- 5. Click the **Save** or **Delete** buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.
- 6. Click a Secunia Advisory ID (SAID) to view detailed information related to the Advisory.
- 7. To view one ticket, click the appropriate ticket check box in the grid and select the Affected Devices (lists all devices affected by the ticket) or View, Edit, or Delete the ticket. To view multiple tickets, click the appropriate ticket check boxes in the grid and select an option from the Actions drop-down menu such as Delete multiple tickets (see Delete Patching Tickets) or Edit multiple tickets.
- 8. Click determined to export tickets to a CSV file.

## **Delete Patching Tickets**

To delete Patching Tickets, perform the following steps.

#### Task To delete patching tickets:

- 1. Open the Patching > Tickets page.
- 2. Insert a check mark in front of the ticket or tickets to delete.
- 3. To delete one ticket, select **Delete** under the listed ticket in the grid.
- 4. To delete multiple tickets, select Delete multiple tickets from the Actions drop-down menu.
- 5. When the "Are you sure you want to delete these tickets" pop-up window appears, click Yes.



# **Manual Signatures**

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

The following sections describe how to process a manual signature:

- Enable Manual Signatures
- Deploy the Agent for a Manual Signature
- Deploy a Patch Package for a Manual Signature
- Manual Signature Notifications

## **Enable Manual Signatures**

This section describes how to enable manual signatures and how to Share Unsigned and Signed .cab Files.

Task	То	enable manual signatures:
	1.	Connect a daemon to your Software Vulnerability Research account by going to <b>Settings &gt; Assessment &gt; Update</b> <b>Servers &amp; Daemon</b> .
	2.	Select a daemon.
	3.	Click the <b>More Info</b> action. In the pop-up, you will see a summary of the current state: the label <b>Digital signatures:</b> Automatic and the button Sign packages manually.
	4.	Toggle the <b>Sign packages manually</b> button to create the desired state: the label <b>Digital signatures: Manual</b> and th button <b>Sign packages automatically</b> .
		Daemon #73 Info ×
		Version: Daemon/8.0.0.305
		Daemon ID: 3b1109ff-22fa-4b4e-ab69-c2252fa7889d Machine ID:
		Digital signatures: Manual Sign packages automatically
		Created: 2018-02-12 06:49:40 Last connected: 2018-02-12 09:29:41

**Note** • The daemon will continue to process requests from the Software Vulnerability Research server while waiting for the signed . cab file, regardless how long it takes. However, if a new agent is released during this window, the process will deploy the older version of the agent.



**Note** • Enabling manual digital signatures changes the behavior of two Software Vulnerability Research patching processes: Deploy the Agent for a Manual Signature and Deploy a Patch Package for a Manual Signature. Both processes now require a manual step to sign a .cab file before it can be deployed to WSUS. Reverting to automatic digital signatures results in future packages being signed with the certificate that WSUS is configured to use, just like occurred before the introduction of manual signature support. In all cases, the signature that is applied to a .cab file must be trusted by downstream machines, or updates will not be applied.

## Share Unsigned and Signed .cab Files

To access unsigned and signed.cab files from other machines, create and share the following folders:

- Unsigned files (read only is fine): C:\ProgramData\Flexera Software\SVM\SVMPD IO\Unsigned
- Signed files (only useful if writable): C:\ProgramData\Flexera Software\SVM\SVMPD IO\Signed

**Note** • Altering or removing these shared folder names while a file is being signed will result in stale paths being shown in the Software Vulnerability Research user interface. Wait until no files are waiting for signatures before changing shared folder names.

# Deploy the Agent for a Manual Signature

To deploy the Agent for a manual signature, perform the following steps.

SK 10	То	deploy the agent for a manue	al signatur	e:				
	1.	Click Deploy Agent.						
		Name	Hostname		Status	Crea	ted	Last connected
		1. C 1. C 1.			Available	2018-	01-31	2018-02-05
			More Info	Schedule Refresh	View Servers & Groups	Deploy Agent	Delete Daemon	Disable Daemon
	2.	Select any target groups.						
	3.	Click Deploy Agent.						
		Daemon #73 Servers				×		
		✓ □ □	details					
		✓						
		Com	puters					

current beproyrigene

4. Once initiated, the daemon will download the current agent binary and build a .cab file containing it. Then a Sign Agent Package pop-up displays the location of the unsigned.cab file to deploy the agent and a location to place the signed copy of this .cab file.

Hos	stname			Status		Created
				Available		2018-01-31
More I	Info	Schedule Refresh	View Serv	ers & Groups	Sign Agent Pa	ackage
Manual Digita Sign Agent Pa	al Signat Ickage	ures				×
Unsigned file Get the unsigned	d file from \Outbox\a	this location: 8744c92-259f-4623-82a	b-363246e	57abe\agent-8.2.ca	b	
Copy Path C	Open Fold	der				
Signed file Place signed file in	in this loca	ation:				
W .	Inbox\a87	744c92-259f-4623-82ab-	363246e57	/abe		
Copy Path C	Open Fold	ler				
		CI	ose			

**Note** • These two locations have one or two buttons each. **Copy Path** will always be shown. This button copies the content of the box above it and enables you to open File Explorer and paste the path. You may also manually copy the path by selecting it and hitting CtrL+C or equivalent. If, as shown here, the machine running the daemon has been configured with the appropriate file shares, the paths will leverage this and **Open Folder** will be shown. In some browsers (notably Internet Explorer and Edge), **Open Folder** will open File Explorer to the path; in others, **Open Folder** may do nothing.

5. Copy the unsigned .cab file from the location mentioned under **Unsigned file** and invoke your organization's process for getting it signed. Once the .cab has been signed, copy the file into the folder mentioned under **Signed file**. The daemon will find the signed file, and, if the signature and chain of trust are verified, deployment to WSUS will continue.

# **Deploy a Patch Package for a Manual Signature**

To deploy a Patch Package for a manual signature, perform the following steps.

Task	То с	To deploy a patch package for a manual signature:									
	1. Navigate to Patching > Packages.										
	2.	Select a package.									
	3.	Click Create Deployment.									
	4.	Select any target groups.									
	5.	Click <b>OK</b> .									
	6.	If there are no packages, select a product in <b>Patching &gt; Patch Library</b> .									

- 7. Create a template if necessary, and click **Build Packages**. Once deployment is initiated, the daemon will download the patch package and build a.cab file containing it.
- 8. When the status Waiting for signature appears in the Status column under Patching > Deployment, click Sign Package (first screen shot below). Then a Manual Digital Signatures pop-up appears with the location of the unsigned.cab file and a location where a signed copy of this.cab file should be placed (second screen shot below).

Package name	Vendor	Published to	Deployed to	Status	Count Installed	Count Failed	Count Pending	Count Not Applicable	Last status update
nstall/Update 7-zip 15.x to 16.x		the second second second	OfflineSibling	Waiting for signature	0	0	0	0	Feb 2, 2018 12:53 PM
		Information	Sign Package	Refresh status	Update Deploymer	t Delete De	ployment		
Manual Digi	tal Sign	atures				×			
Install/Upda	te 7-zip	15.x to 16.x							
Unsigned file									
Get the unsign	ed file fro	m this location:					1		
C:\ProgramDa	ta\Flexera	Software\SVM\SVMPD	IO\Unsigned	\6dfb56f3-4963	-4e49-b277-49	b8834ed73			
Copy Path									
Signed file									
Place signed fil	e in this lo	ocation:							
C:\ProgramDa	ta\Flexera	Software\SVM\SVMPD	IO\Signed\6d	lfb56f3-4963-4e	49-b277-49b8	834ed732	]		
chartogramba	to a revero	- Soldiare Still Still S	io isigned too	105015 4505 40		00100702			
Copy Path									
		_							
			Close						
_									

**Note** • These two file locations have one or two buttons each. **Copy Path** will always be shown. This button copies the content of the box above it and enables you to open File Explorer and paste the path. You may also manually copy the path by selecting it and hitting Ctrl+C or equivalent. If, as shown here, the machine running the daemon has not been configured with the appropriate file shares, the paths will be local to the machine running the daemon, and **Open Folder** will not be shown.

9. Access the daemon machine to copy the unsigned .cab file from the location mentioned under **Unsigned file** and invoke your organization's process for getting it signed. Once the .cab has been signed, copy the file into the folder mentioned under **Signed file**. The daemon will find the signed file, and, if the signature and chain of trust are verified, deployment to WSUS will continue.



**Note** • If multiple patch packages are all waiting for signature, it is safe to place signed **.cab** files in their respective signed paths in any order. The daemon will deploy the packages as they arrive.

# **Manual Signature Notifications**

Typically, there is a pause between requesting to deploy an agent and the unsigned .cab file becoming available. To address this issue, you can notify the proper users that a .cab file is ready to be signed, where to get the .cab file and place it. To receive a notification, set up a rule in **Settings > Workflow Management > Rules**.

#### To create a rule to send a notification when a . cab file is ready to be signed:

- 1. Add a new rule by clicking the green plus sign in the upper-right hand corner.
- 2. Specify a rule name, such as Manual Signing, and optionally a description.
- 3. Select the Rule Trigger channel Patch and the trigger Package ready for manual signing.



4. Add and configure any desired actions, such as Email.



5. Enable the rule.

÷

Task

6. Save the rule.

Once the package is ready for your signing process, the configured notifications are sent. These notifications include links to the relevant part of the Software Vulnerability Research user interface (either to the Deployment or the Daemon). These notifications also include the unsigned and signed paths, if the medium permits, as there is no further need to visit the Software Vulnerability Research user interface to complete the manual signing process.

Chapter 10 Patching Manual Signatures



Edition • The Policy Manager module is not available for Software Vulnerability Research - Assessment Only.

You can use the **Policy Manager** pages to configure internal Compliance Policy Rules to associate with your account and view the details of breaches to your policies.

Overview

♬

- Policies
- Breaches

# **Overview**

Click a Policy name or Ticket number to view detailed information about the Policy or Ticket.

Click an item in the grid to view policy breaches, view, edit or delete a policy, or click 💶 to create a new policy and specify:

- Rule Name—Define a unique name for the Compliance Policy Rule.
- Apply Scope—Define if the rule should apply globally to all users or to a specific user and Watch List.
- Set Policy Rule Criteria (optional)—Define your tolerances for handling advisories based on the Ticket Priorities, Ticket Status, Criticality (Severity Rating), CVSS (Common Vulnerability Scoring System) Base Score and Threat Score. The interval starts from the date when the Advisory was added to the ticketing system.

Note • Set Policy Rule Criteria based on Threat Score (optional) requires purchase of Threat Intelligence Module

# **Policies**

You can use this page to create a new policy and specify the policy rules.

To create a new policy, perform the following steps:



, 8								-				
Policies Breaches												
Browsing 1 policies i												
Policy Name	Breached	Is disabled	Apply to all users and watch lists	User to apply to	Watch List to apply to	User Group to apply to	Created by	Last Updated	Created			
UBS testing pre-policy breach		No	Yes					2020-08-28	2020-08-28			
Breaches View Edit Disable Delete												
Image     1     of 1     Image     Image												

- 2. Add new Policy dialog box appears. Enter a unique name for the Compliance Policy Rule in the Rule Name field.
- 3. Click on the **Apply scope** drop-down and select the following from the list:
  - Apply to all Watch Lists and users
  - Apply only to one user
  - Apply only to one Watch List
  - Apply only to one User Group

To apply a scope for the specif User, Watch List, or User Group then select **Apply only to one user**, **Apply to one Watch List**, or **Apply only to one User Group** respectively.

- 4. The **Set Policy Rule Criteria** fields are optional and you can follow the dialog box instructions to create criteria to specifically fit your requirements.
- Select Enable / Disable Policy Breach Warning Email option and then select the number of days in the Send Policy Breach Warning Email Before field.

If you select this option, then you will be able to send a policy breach warning emails for applicable open or waiting tickets. This warning can be configured for priority based rule of the policy and will enable the ticket assignees to prioritize their tickets. You will be able to configure the number of days before the policy breach, to send such a warning.
Add new Policy		×
Define a unique name for this Compliance Policy Rule.		
Rule Name	Apply scope	
	Apply scope	Ţ
Set Policy Rule criteria based on 'Priority' (optional)	Low	Interval days
You can select your tolerance for handling an advisory based on the Priority. The interval starts from the date when the advisory was added to the ticketing	Medium	Interval days
system.	High	Interval days
	Urgent	Interval days
	Medium	Interval days
	Low-Medium	Interval days
	Medium-High	Interval days
	Medium-High	Interval days
Enable / Disable Policy Breach Warning Email	7	
Send Policy Breach Warning Email Before days		
Set Policy Rule criteria based on 'Solution Status' (optional)	Unknown	Interval days
You can select your tolerance based on each type of Solution Status. The interval starts from the date when the advisory was added to the ticketing system.	No Fix	Interval days

- 6. Click the Save button to begin receiving alerts regarding breaches to the policies you have created.
- 7. Click on any policy in the grid and select Breaches, View, Edit, Disable or Delete.

**Note** • The email notifications will include SLA days as defined in policy rule criteria for priority. If more than one policy is associated with a newly released advisory, the lowest defined SLA days, will be shown in the email.

# **Breaches**

The **Breaches** page displays details of active and inactive breaches to the policies you created. Click an item in the grid to view or edit the breach details. Click 4 to export the results to a CSV file.

Policy Manager :	Breaches					0 -0
Policies	Breaches					
Active breaches	ctive breaches 4483 Inactive breaches 19					
Browsing 1-20 of 4	488 breaches $i$					Ŧ
Policy	Ticket	Reason for Breach		Breached Date	Last Updated	Created
-	1	THE MARK THE MARK THAT IN THE MARK		2017-05-05	2017-08-14	2017-05-05
			View Edit			

Chapter 11 Policy Manager

Breaches



Use the **Analytics** pages to filter data contained in the widgets and to create dynamic reports on Advisories, Tickets, Devices and Products.

The Analytics widgets are dynamic, and you can segment information by clicking the individual chart legends or segments in any widget to alter the data displayed accordingly.

- Advisories
- Tickets
- Devices
- Products
- Reports
- LiveUpdate

# **Advisories**

The Advisories page displays widgets that contain information regarding:

- Secunia Advisories—Displays a month-by-month bar chart of the number of advisories based on your configured Watch Lists.
- Advisories by year—Displays a bar chart of the number of advisories based on your configured Watch Lists.
- Advisories by level of criticality—Displays a color coded pie chart of the criticality levels (Extremely critical, Highly critical, Less critical, Moderately critical, None (Rejected) and Not critical) of advisories based on your configured Watch Lists.
- Advisories by solution status—Displays a color coded pie chart of the solution status (None (Rejected), Partial Fix, Unpatched, Vendor Patched and Vendor Workaround) levels of advisories based on your configured Watch Lists.
- Advisories by attack vector—Displays a color coded pie chart of the attack vector (From local network, From remote, Local system, and None (Rejected)) of advisories based on your configured Watch Lists.

• Advisories by CVSS score—Displays a bar chart of the CVSS score intervals for the Advisories. The intervals follow standard mathematical notation, for example, (3, 4] means strictly greater than 3 and less than or equal to 4. The interval starts from the date when the advisory was added to the ticketing system.

The Analytics widgets are dynamic, and you can segment information by clicking the individual chart legends or segments in any widget - with the exception of Secunia Advisories and Advisories by year - to alter the data displayed in all widgets and the Advisory details grid accordingly.

[	4

**Note** • Click the *i* icon to see more information about the widget.



Task

#### To view analytics for advisories:

- 1. Open the **Analytics > Advisories** page.
- 2. Click 🔽 to filter the results by Watch List, From and To dates, and Criticality (select from drop-down menu).
- 3. Click the Apply or Reset buttons to apply or reset the filters.
- 4. Click the **Save** or **Delete** buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.
- 5. Click Save Layout to save the page layout. Adjusting the size of the widgets activates this function.



- **6.** In the example above, clicking the **Extremely critical** legend in the Advisories by level of criticality widget, and then clicking Refresh grid, displays the relevant data.
- 7. Click the legends or segments again to return to the original, unfiltered, information displayed.
- 8. Click a Secunia Advisory ID (SAID) to view the complete Advisory details, including (where applicable) the Creation Date, Criticality (Severity Rating), Zero Day (yes or no), Impact (Consequence), Where (Attack Vector), Solution Status, Secunia CVSS (Common Vulnerability Scoring System), CVE References, Affected operating system and software, Affected watch lists, Related tickets, Advisory Description, Reason for rating, Original advisory references and Changelog. Click Download PDF to save a copy of the advisory.

## **Advisories by Threat Score**

This page displays a bar chart of the number of advisories by threat scores.



**Note** • Please note the following:

- Advisory by threat score chart and Threat Score column in the grid requires purchase of the Software Vulnerability Research Threat Intelligence module
- To purchase this module, contact your sales representative or contact us online at: https://www.flexera.com/about-us/ contact-us.html
- For more details about the Threat Intelligence Modules, see our datasheet: https://www.flexera.com/media/pdfs/ datasheet-svm-threat-intelligence-module.pdf

# **Tickets**

The Tickets page displays widgets that contain information regarding:

- **Ticket performance**—Displays a month-by-month bar chart of the performance of ticket handling based on ticket priority.
- Ticket priority—Displays a color coded pie chart of the priority (High, Low, Medium, and Urgent of all tickets.
- Ticket status—Displays a color coded pie chart of the status (Open, Waiting, Handled and Irrelevant) of all tickets.
- Tickets queue—Displays a color coded pie chart of the number of tickets assigned to each queue you created.

The Tickets widgets are dynamic and you can segment information by clicking the individual chart legends or segments in any widget - with the exception of Ticket performance - to alter the data displayed in all widgets and the Ticket details grid accordingly.

**Note** • Click the *i* icon to see more information about the widget.

Analytics > Tickets Advisories Tickets Devices	Products Reports				8 √
Ticket Analytics 🦸					Save Layout
From	То	Ticket Queues	Status	Watch Lists	SAID
					Apply Reset
				Filter •	Save Delete
Ticket performance <i>f</i> * 10/weeks (14506) 6 2.000 4.000	0.000 E.000	10,000 12,000 44,000 <sup>1</sup>		Ticket queue #	Approval Default Exit test, workflow
Ticket priority #	Icket statu Low Medium Medium +righ Urgert	At QA Closed Intervant Open Bending deployment Waiting			

Task

#### To view analytics for tickets:

- 1. Open the Analytics > Tickets page.
- 2. Click T to filter the results by From and To dates, Ticket Queues, Status, Watch Lists, and SAID.
- 3. Click the Apply or Reset buttons to apply or reset the filters.
- 4. Click the **Save** or **Delete** buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.
- 5. Click Save Layout to save the page layout. Adjusting the size of the widgets activates this function.

# **Devices**

The Devices page displays widgets that contain information regarding:

- Devices by System Score—Displays a color-coded pie chart for devices grouped by system score.
- Devices by Criticality—Displays a color-coded pie chart for devices grouped by criticality levels.
- Devices by Attack Vector—Displays a color-coded pie chart for devices grouped by attack vector.
- **Devices by Solution Status**—Displays a color-coded pie chart for devices grouped by solution status.



The Devices widgets are dynamic, and you can segment information by clicking the individual chart legends or segments in any widget to alter the data displayed.

_	D
-	-
_	-
_	-

**Note** • Click the *i* icon to see more information about the widget.

# **Products**

The Products page displays widgets that contain information regarding:

- Products by Criticality—Displays a color-coded pie chart for products grouped by criticality levels.
- Products by Attack Vector—Displays a color-coded pie chart for products grouped by attack vector.
- Products by Solution Status—Displays a color-coded pie chart for products grouped by solution status.



The Products widgets are dynamic, and you can segment information by clicking the individual chart legends or segments in any widget to alter the data displayed.



**Note** • Click the *i* icon to see more information about the widget.

# Reports

You can generate reports based on the current state of all Device Groups, Devices, Products, Watch Lists, Advisories and Tickets. This convenient and powerful feature allows you to schedule reports to run at any time of the day, with any recurrence, and with no user interaction necessary.

The Reports page displays a list of reports that have been configured and scheduled for generation.

Click • and select either Add Research Report or Add Assessment Report to create a new report, or click an existing report in the grid to Edit, View Files or Delete the report. The reports are provided in PDF format and are sent to the assigned recipients based on your configuration.

#### Task To create a new Research report:

- 1. Click 🌆 and select Research Report.
- 2. Specify the Time Frame and Generation Schedule for the report. From the drop-down list, select:
  - **One-Time Report**—Generate only one report for a specific time frame.

**Note** • When searching for advisories within a specific date period for a One-Time Report, use the year, month, and date format. Example: To view only the July 2018 advisories, use the query **Start Date:** 2018.07.01 and **End Date:** 2018.07.31.

- **Recurring Report**—Generated based on the configured time frame and recurrence schedule.
- 3. Configure the Start Date and End Date for the report.

Time Frame and Generat	ion Schedule	
Specify the time frame / g	eneration schedule for the report, and confi	figure the details using the button to the right.
One-Time Report - Generate	e only one report for a specific time frame.	
Set the time frame for the generated immediately. Al Date chosen will be used f Start Date:	data used to generate the report. If the End Iso note, the End-Date is taken as 00:00 that for the report.	d-Date is in the future the report will be generated on that date, otherwise it will be It day, thus there will be no data occuring on that date. That is, only data prior to the End-

4. Select the Watch List(s) or Watch List Group(s) from which data will be used for the report from the drop-down list:

Watch Lists					
Specify the watch lists or watch list groups from which data will be used for the report.					
Watch List(s):	All Watch Lists	-	Watch List Group(s):	All Groups	•

5. Select the Relevant Advisories to be included in the report. The time frame configured above will be used for selecting the relevant advisories. You can optionally select an additional time frame to include for comparative purposes. You can select:

- Type of Advisory Statistics (choose from the drop-down list)
- Select Additional Time Frame for Comparison (choose from the drop-down list)

You can choose to include a detailed list of advisories in the report. You can further filter this option by a minimum criticality to refine the output:

- Include Detailed Advisory List
- Only Include Advisories:
  - with a Criticality Rating of: (choose from the drop-down list) or Above
  - with the following Attack Vectors (choose from the drop-down list)
  - with the following Solution Status (choose from the drop-down list)
  - with the following Impact Types (choose from the drop-down list)
- Sort Advisories List by: (choose from the drop-down list)

Relevant Advisories
Select the type of advisory statistics to be included in the report. The time frame configured above will be used for selecting the relevant advisories. On the right you can optionally select an additional time frame to include for comparative purposes.
Overall Advisory Statistics 👻
Select Additional Time Frame for Comparison: Year-To-Date
You can also choose to include a detailed list of advisories in the report. You can further filter this by a minimum criticality to refine the output.
Only Include Advisories
• with a Criticality Rating of Show All - or Above
with the following Attack Vectors 3selected
with the following Solution Status     4selected
with the following Impact Types     12 selected
✓ Sort Advisories List by: Criticality ▼

- 6. Specify the type of Tickets statistics to be included in the report:
  - Type of Tickets Statistics (choose from the drop-down list)
  - Include Action History

You can choose to include the Action History view in the report. Select the option here if desired, as well as the additional optional configuration parameters:

- Include Ticket Comments
- Only Include Tickets:
  - with a Criticality Rating of (choose from the drop-down list) or Above
  - with the following Attack Vectors (choose from the drop-down list)
  - with the following Solution Status (choose from the drop-down list)
  - with the following Impact Types (choose from the drop-down list)

Specify the type of tickets statistics to be included in the report:          Type of Tickets Statistics         You can choose to include the Action History view in the report. Select the option here if desired, as well as the additional optional configuration parameters:         Include Action History         Include Ticket Comments         Only Include Tickets:	Tickets	
Type of Tickets Statistics         You can choose to include the Action History view in the report. Select the option here if desired, as well as the additional optional configuration parameters:         Include Action History         Include Ticket Comments         Only Include Tickets:	Specify the type of tickets statistics to b	e included in the report:
You can choose to include the Action History view in the report. Select the option here if desired, as well as the additional optional configuration parameters:  Include Action History Include Ticket Comments  Only Include Tickets:	Type of Tickets Statistics	•
with a Criticality Rating of Show All     or Above     with the following Attack Vectors     3selected	You can choose to include the Action H You can choose to include the Action H Include Action History Include Ticket Comments Only Include Tickets: . with a Criticality Rating of . with the following Attack Vector	story view in the report. Select the option here if desired, as well as the additional optional configuration parameters:
with the following Solution Status     4selected	• with the following Solution State	is 4selected
with the following Impact Types     12 selected	• with the following Impact Types	12 selected

7. Select the User Groups to receive the generated report form the drop-down list.

Re	cipient List	
You	u must select at least one recipient for the generated report.	
S	elect User Group	-

8. Specify the **General Configuration Options** (PDF File name, Report Title, and Generate CSV advisory data) for the generated report:

General Configuration Options
Here you can specify a custom output file name for the generated report.
Set the file name for the PDF report file generated.
PDF Filename:
Here you can specify a custom title for the front page of the report.
Set the report title.
Report Title: Custom Report
Generate CSV advisory data

**9.** Click **Save**. Once saved, you and the specified recipients will begin to receive notifications and reports based on your configuration.

#### **Creating a New Assessment Report**

To create a new Assessment Report, perform the following steps.



To create a new Assessment Report:

- 1. Click 🛃 and select Assessment Report.
- 2. Specify the Time Frame and Generation Schedule for the report. From the drop-down list, select:

- **One-Time Report** Generate only one report for a specific time frame.
- **Recurring Report** Generated based on the configured time frame and recurrence schedule.
- 3. Configure the **Start Date** and **End Date** for the report.



4. Select the **Device Groups** from which data will be used for the report from:

Device Groups	
Specify the device groups from which data will be used for the repo	ort.
✓	
🗸 🚰 local	
🗸 🚰 secunia	
Computers	
✓	
✓	
🗸 🗁 EMEA	
✓ 🚰 HQR	
Y 🚰 Client Machines	
WKS	

5. Select the Device statistics from the drop-down list to be included in the report. You can select multiple statistics:

Devices	
Select the type of device statistics to be included in the report.	
Type of Device Statistics	*
Devices by Criticality	
Devices by Attack Vector	
Devices by Solution Status	
Devices by System Score	

6. Select the **Product** statistics from the drop-down list to be included in the report. You can select multiple statistics:

#### Products

Select the type of product statistics to be included in the report.

Type of Product Statistics	*
Vulnerable Products by Criticality	
Vulnerable Products by Attack Vector	
Vulnerable Products by Solution Status	
Products by Security Status	

- 7. Select the **Relevant Advisories** to be included in the report. The time frame configured above will be used for selecting the relevant advisories. You can optionally select an additional time frame to include for comparative purposes. You can select:
  - Type of Advisory Statistics (choose from the drop-down list)
  - Select Additional Time Frame for Comparison (choose from the drop-down list)

You can choose to include a detailed list of advisories in the report. You can further filter this by a minimum criticality to refine the output:

- Include Detailed Advisory List
- Only Include Advisories:
  - with a Criticality Rating of: (choose from the drop-down list) or Above
  - with the following Attack Vectors (choose from the drop-down list)
  - with the following Solution Status (choose from the drop-down list)
  - with the following Impact Types (choose from the drop-down list)
- Sort Advisories List by: (choose from the drop-down list)

Relevant Advisories
Select the type of advisory statistics to be included in the report. The time frame configured above will be used for selecting the relevant advisories. On the right you can optionally select an additional time frame to include for comparative purposes.
Overall Advisory Statistics 👻
✓ Select Additional Time Frame for Comparison: Year-To-Date ▼
You can also choose to include a detailed list of advisories in the report. You can further filter this by a minimum criticality to refine the output.  Include Detailed Advisory List  Only Include Advisories:
with the following Attack Vectors     Show All     or Above
• with the following Solution Status 4 selected -
with the following Impact Types     12 selected
✓ Sort Advisories List by: Criticality

- 8. Specify the type of Tickets statistics to be included in the report:
  - Type of Tickets Statistics (choose from the drop-down list)
  - Include Action History

You can choose to include the Action History view in the report. Select the option here if desired, as well as the additional optional configuration parameters:

- Include Ticket Comments
- Only Include Tickets:
  - with a Criticality Rating of (choose from the drop-down list) or Above
  - with the following Attack Vectors (choose from the drop-down list)
  - with the following Solution Status (choose from the drop-down list)
  - with the following Impact Types (choose from the drop-down list)

Tickets
Specify the type of tickets statistics to be included in the report:
Type of Tickets Statistics 🔹
You can choose to include the Action History view in the report. Select the option here if desired, as well as the additional optional configuration parameters: Include Action History Include Ticket Comments Only Include Tickets: • with a Criticality Rating of Show All • or Above • with the following Attack Vectors 3selected • with the following Solution Status 4selected • with the following Impact Types 12 selected •

9. Select the User Groups to receive the generated report form the drop-down list.

Recipi	ient List	
You m	ust select at least one recipient for the generated report.	
Select	t User Group	-

**10.** Specify the **General Configuration Options** (PDF File name, Report Title, and Generate CSV device, advisory and product data) for the generated report:

General Configuration Options
Here you can specify a custom output file name for the generated report.  Set the file name for the PDF report file generated.  PDF Filename:
Here you can specify a custom title for the front page of the report.  Set the report title.  Report Title: Custom Report
<ul> <li>Generate CSV device, advisory and product data</li> <li>Generate CSV insecure and EOL installation data (WARNING! Selecting this option will generate a large amount of data, and cause increased report creation time).</li> </ul>

**11.** Click **Save**. Once saved, you and the specified recipients will begin to receive notifications and reports based on your configuration.

# LiveUpdate

As in our previous LiveUpdate capability, Software Vulnerability Research natively accounts for new vulnerability data based on existing scan data. After you have scanned your system, the scanned data is stored in Software Vulnerability Research's database. LiveUpdate automatically runs in the background to identify any new advisories that have come in since you last scanned your system. As soon as new vulnerabilities are added to the Secunia Vulnerability Research Database, LiveUpdate will reference your latest scan results against it. As a result, you'll find out immediately if you're affected without having to run another scan.



Important • LiveUpdate is limited to your current scanning filters for devices and products.

Chapter 12 Analytics LiveUpdate

# **Ticket Manager**

The Ticket Manager page lists all issued tickets. Use this page to:

- View and Change Tickets Status and Priority
- Create Tickets in Ticket Manager
- Delete Tickets in Ticket Manager
- Default Ticket Statuses in Ticket Manager

# **View and Change Tickets Status and Priority**

The following is a view of Change Tickets status and priority.

Ticket Man	Ticket Manager						
Open ticket	Open tickets 🎫 Walting tickets 😰 Handled tickets 🗊 Irrelevant tickets 🚺 Custom tickets 🗊						
Browsing 1-3	20 of 347 tic	kets i					Y 🕂 ± Actions -
ID		From	То	Queue		Priority	▼ Assigned user ▼
							Apply Reset
						Filter	✓ Save Delete
	ld	Ticket created	Ticket type	Queue	Status	Priority	Assigned to
	350	2018-06-04	Advisory	Readers	Open	High	
	349	2018-06-04	Advisory	Patches	Open	High	
				View Edit Delete			

To view and change ticket status and ticket priority, perform the following steps.

#### Task

To view and change ticket status and ticket priority:

- 1. Open the Ticket Manager page.
- 2. To filter the results by ticket status, select one of the bold ticket statuses in the upper-left-hand corner followed by a ticket count. The default ticket statuses are **Open**, **Waiting**, **Handled**, and **Irrelevant**.
- 3. Click 🔽 to filter the results by ID, From and To dates, Queue, Priority, and Assigned User.

- 4. Click the Apply or Reset buttons to apply or reset the filters.
- 5. Click the **Save** or **Delete** buttons to save or delete filters. You can save only one row on both the desktop and mobile UI.
- 6. To view one ticket, click the appropriate ticket check box in the grid to View, Edit, or Delete the ticket. To view multiple tickets, click the appropriate ticket check boxes in the grid and select an option from the Actions drop-down menu such as Delete multiple tickets (see Delete Tickets in Ticket Manager) or Edit multiple tickets.
- 7. Click 🗳 to export tickets to a CSV file.
- 8. Click 🍱 to Create Tickets in Ticket Manager.

# **Create Tickets in Ticket Manager**

To create Tickets in Ticket Manager, perform the following steps.

# Task

#### To create tickets in Ticket Manager:

- 1. Open the Ticket Manager page.
- 2. Click 🎫 to create a ticket.

Create ticket ×	
Advisory	
Q Search by SAID or title	
Status	
Open -	
Priority	
Low -	
Queue	
Default -	
Assigned to	
Assigned to -	
Add comment	
Add comment	
Cancel Save	

- **3.** From the **Status** drop-down list, select the appropriate status. The default ticket statuses are **Open**, **Handled**, **Closed**, or **Irrelevant**. See Default Ticket Statuses in Ticket Manager for more information.
- 4. From the **Priority** drop-down list, select the appropriate priority. The default ticket priorities are **Low**, **Medium**, **High** or **Urgent**.
- 5. From the **Queue** drop-down list, select a queue to assign the ticket to.
- 6. From the Assigned to drop-down list, list, select an individual to assign the ticket to.

- 7. In the Add comment field, add an appropriate comment to the ticket (mandatory).
- 8. Click Save.

# **Delete Tickets in Ticket Manager**

To delete Tickets in Ticket Manager, perform the following steps.

# Task To delete tickets in Ticket Manager: 1. Open the Ticket Manager page. 2. Insert a check mark in front of the ticket or tickets to delete. 3. To delete one ticket, select Delete under the listed ticket in the grid.

Ticket Manag	ger					6 J
Open tickets	Open tickets 💵 Waliting tickets 🛐 Closed tickets 🕮 Irrelevant tickets 🗊 Pending deployment tickets 🔋 At QA tickets 💈					
Browsing 1-20	of 21456 tickets 🦸					🔻 🕂 Actions -
ID		From To	<b></b>	Queue	Priority	Assigned user
						Apply Reset
					Filter	▼ Save Delete
	Id	<ul> <li>Ticket created</li> </ul>	Queue	Status	Priority	<ul> <li>Assigned to</li> </ul>
	21715	2018-05-29	Default	Open	Medium	100
			View Edi	it Delete		

4. To delete multiple tickets, select **Delete multiple tickets** from the **Actions** drop-down menu.

1	Ticket Manager						0 -D	
0	Open tickets 💷 🖉 Valting tickets 🛐 Closed tickets 💷 Irrelevant tickets 🚯 Pending deployment tickets 🔋 At QA tickets 💈							
E	Browsing 1-20 o	f 21457 tickets 🦸					Ŧ	+ Ł Actions 🔺
		ld 🗢	Ticket created	Queue	Status 💠	Priority	Assigned to	Edit multiple tickets
	•	21716	2018-05-29	Default	Open	Medium		Delete multiple tickets
	•	21715	2018-05-29	Default	Open	Medium		$\bigcirc$

5. When the "Are you sure you want to delete these tickets" pop-up window appears, click Yes.



# **Default Ticket Statuses in Ticket Manager**

The default ticket statuses are used to run and display reports. While you are free to configure the ticket statuses, priorities and queues as you see fit, Flexera needs to know your equivalent "open" statuses to be able to correctly report the statistics.

The following are the default ticket statuses:

#### Table 13-1 • Default Ticket Statuses

Status	Description	
Open Tickets	An Open Ticket is one for which no action has yet been triggered.	
Waiting Tickets	A ticket is marked as Waiting when it has been decided that an action needs to be taken at a later stage.	
Handled Tickets	A ticket is considered Handled when the appropriate action has been taken.	
Irrelevant Tickets	A ticket is considered Irrelevant when it has been closed and is no longer considered of importance to you.	



The Settings pages allow the main Administrator account holder to create and manage other accounts.

**Note** • Administrators can access the **Settings** pages, and any changes made will effect all users. Depending on the rights given to a User Group, some users may also have access to some of the Settings pages.

Use the **Settings** pages to:

- View details of your Account License Status, Account Options and Security Policy
- Perform User Management tasks
- Configure SSO Settings.
- View, create and add Vulnerability Management for Watch List Groups and subscriptions, Ticket queues, statuses and priorities
- Create and edit Workflow Management Rules, Ticket Queues, Ticket Status and Ticket Priorities.
- View and edit Assessment configurations for the Update Servers & Daemon, Scan Configuration, and Downloads.
- View the API Access token generation page.
- View Logs for tracking details of all activities taken by users related to your account.

# Account

Use the Account pages to view your license information, manage your Account options, and edit your security policies.

- License Status
- Account Options
- Security Policy

## **License Status**

Use the **License Status** page to view your license information, including the expiration date, the modules that you are entitled to use according to your subscription, detailed license attributes, and the number of licenses available, which is tracked as the number of used users.

## **Account Options**

Use the **Account Options** page to edit your account settings and manage settings that apply to all users, for example, show or hide rejected advisories.



## **Security Policy**

You can edit your security policy by selecting the appropriate box below and clicking Update.

Account -	User Management 👻
Edit your securit	y policy 🧯
Enable passwo	ord expiration.
🖉 Disable two fa	ctor authentication for sub-users.
Undata	

**Note** • Two factor authentication is considered as a best practice for the application.

# **User Management**

The **User Management** pages display the Users, User Groups, and Roles associated with your account. You can create active Users up to the license limit of your account.

- Users
- User Groups

- Roles
- SSO Settings

## Users

The **Users** page displays the users associated with your account and, if applicable, the User Groups the user belongs to. Click • and enter the required information to add a new user.

Settings > User N	Management > U	Jsers						<b>9</b> - <b>1</b>
Account -	User Manage	ement 👻	Vulnerability Manage	ement 🗸	Workflow Management 🗸	As	sessment	- API - Logs -
Browsing 1-20 of 2	18 users į							Q Search by username or email address
Username 🗢 💠	First Name	Last Name	Job Title	Email Address	÷	Active	Blocked	Groups
	and the second se	-	Contract Contractor			Yes	No	Administrators
					Edit	Reset tv	o factor logi	in Disable Delete

A valid email address is required for creating a new user. After a user is created, we will send an email to their email address. After clicking the link in the email, the user will be able to set the password for the account. After successfully registering the a account, the user can then log on. Only active users are counted with regards to enforcing the user count. If the user has reached their user count limit, they can disable an unused user to recover a license and create another user.

In addition, if an account has for example five licenses and five active users, the user can create the sixth user. The additional user will be disabled by default when created, and the user will not be able to activate their account until the account manager handles the license issue.

Click 🗳 to download a CSV file containing details of all Users associated with your account.

Click a Username in the list and select Edit, Reset two factor login, Disable, or Delete.



Note • Depending on the user profile, the Reset two factor login option may not be available.

#### **Blocked Users**

When user enters a wrong credentials for **seven** times during login to the Software Vulnerability Research application, their credentials will get blocked.

To unblock the blocked users, follow the below steps:



#### To unblock blocked users:

- Locate the list of user account details in Settings > User Management > Users. In the Blocked column, Yes will be marked for the respective users.
- 2. Select the user details and click Unblock button.
- 3. Now in the Blocked column, Yes will be changed to No.

			rability wanagement *	Norkflow Management + Assessment + A	API + Logs +		
wsing 1-20 of 34 use	ers į			Q, Se	arch by username or email	address	
ername 🔺	First Name	Last Name	Job Title	Email Address	Active :	Blocked	Groups
hisek3_test	abhisek	sular	dev	abhiseisular-3@gmail.com	No	No	
luhan	Arish	Mohan		Abhan@fererasoftware.com	Yes	No	Administrators
rad_only	anal	only	GA	heballarusha@gmail.com	No	No	read only for subscribe
NE	Asha	Japprakash	Sr. Quality Analyst	ajayaprakash@fererascflicare.com	Yes	No	Administrators, advisory reader
dar	Abhisek	Sular	Senior Developer	anular@fererandhrane.com	Yes	No	Administrators, Advisory Approve Managers, advisory manager
dar_on	abhisek	sular	dev.	anutar@flevera.com	No	No	Administrators
why .	848	Kally	PM	BKely@ferera.com	Yes	No	Administrators
(anged)	Donna	Vianpach	Tech Viller	dvampach@fererasofkram.com	Yes	Yes	Administrators

Note • Only an Admin user can unblock the blocked users

## **User Groups**

Users can be grouped into User Groups, and different user profiles can be assigned to the different User Groups. It is also possible to share data between User Groups for easier collaboration within your organization. There is no limit to the number of User Groups that can be created.

```
Settings > User Management > User Groups
```

Account - L	Jser Management 👻 🕚	Vulnerability Management 👻	Workflow Management 👻
Browsing 1-20 of 49 g	roups i		
Name	Description	Roles	
Administrators	Have full power over the account and users.	Super Administrator	
Advisory Approve Managers	Can approve advisories before being assigned to ticketing system	Advisory Manager	
advisory manager	can approve advisry before assigned to to ticket	Advisory Manager	
advisoryManager_group	advisoryManager group	Advisory Manager	
advisory pdf	can read advisory pdf attachments	Advisory PDF attachments	
advisory reader	can read advisory	Advisory Reader	
Advisory Reader Only	Testing	Advisory Reader	
ALL Role_Group	ALL Role Test	Advisory Manager, Analytics Manager, As Manager, Scan Manager, Ticket Manager	sset List Manager, Patch Manager, Policy r, User Manager

The **User Groups** page displays the User Group Name, Description, Roles and Users associated with the group. Click • and enter the required information to add a new Group. You can select the role or roles to apply to the group from the drop-down list.

User groups can be linked to one or several predefined User profiles for access control.

Click a User Group in the grid to **Edit** or **Delete** the User Group or Users to add or delete users to/from the User Group.

## Roles

The **Roles** page displays details of the available User Group Roles. Roles are predefined and cannot be changed.

Note • Administrator and API User Management users can access complete data of the API.

Settings > User	Management > Roles							?	→]
Account 🗸	User Management 🗸	Vulnerabilit	y Management 👻	Workflow Management 🗸	Assessment 🗸	API 👻	Logs 🗸		
Browsing 1-20 of 3	32 roles į								
Name		÷	Description						
Advisory Manager			Can approve advisories	before being assigned to tickets.					
Advisory PDF attac	hments		Can receive advisory PD	F attachments					
Advisory Reader			Can read advisory inform	nation.					
Analytics Manager			Can create custom reports						
Analytics Reader			Can view general reports	3					
API Advisories sea	rch		Provides access to the A	PI Advisories search					
API developer			Can add/remove API tok	ens for data access.					
API Limited advisor	ies search		Provides limited access to the API Advisories search, accesses only ticket related advisories						
API Product databa	se access		Provides access to the A	PI Product database access					
API Ticket manage	ment		Provides access to the API Ticket management						
API User managem	ent		Provides access to the A	PI User management					
API Watch List man	agement		Provides access to the A	PI Watch List management section					

## **SSO Settings**

On the Settings > User Management tab, you can specify SSO Settings.

#### **IDP Configuration Instructions**

Under SSO Settings on the Settings > User Management tab, you can specify the following IDP Configuration Instructions settings.

Table 14-1 •	550	Settings		Configuration	Instructions
Table 14-1	220	Jettings	וטו /	configuration	manuchons

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

#### Table 14-1 • SSO Settings / IDP Configuration Instructions

Setting	Description
Service Provider Metadata URL	Lists the Service Provider Metadata URL.

## **Service Provider Configuration**

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

Table 14-2 • SS	O Settings	/ Service Pi	rovider	Configuration
-----------------	------------	--------------	---------	---------------

Description
Select this option to enable Single Sign-On.
If you are using Single Sign-On at your organization, select this option to disable standard login options for all of your users (except root).
Select this option if you want to upload the IDP metadata XML file.
Select this option if you want to enter the identity provider metadata URL into the <b>IDP Metadata URL</b> field.
Select this option to automatically create new users.
Specify the default group for new users.

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

# **Vulnerability Management**

The Vulnerability Management pages display the settings for Watch List Groups and Watch List Subscriptions.

- Watch List Groups
- Watch List Subscriptions

## Watch List Groups

Use **Watch List Groups** to group Watch Lists, for example All XYZ Products, together. Click 🔹 to create a new Watch List Group or click a Watch List Group in the grid to edit or delete the group.

## Watch List Subscriptions

This page displays the Watch Lists Subscription details including Watch List, Watch List Owner, Subscriber, Enforced by admin, Email Notification level and SMS notification level.

Admin user can add, edit or delete subscriptions to the created watch list.

#### Task Add Subscription to Watch List

- 1. Open the Settings > Vulnerability Management > Watch List Subscriptions page.
- 2. To add a new subscription, Click <a>Image: The Add subscription</a> tab opens.

Software	e Vulnerability Rese	arch Settings > \	/ulnerability Management > Watch Li	st Subscriptions	<u>ب</u>	8 -1
	Account 👻 Us	ser Management 👻	Vulnerability Management 👻	Workflow Management	- Assessment - API - Lo	gs 🕶
Dashboard	Browsing 1-20 of 97 wa	tch list subscriptions 🦸				+
4151	Watch List Name	Watch List Owner	Add subscription	× Email notificat	tion level SMS notification level	
- 🕂 -	15march	PDhillon3		None	None	
Notifications	15march	PDhillon3	Watch List	Not Critical and	I Above None	
	2prod	PDhillon3	Watch List	None	None	
	2 prodssss1234	PDhillon3		Rejected and A	bove Extremely Critical	
Vulnerability	2 prodssssssss	PDhillon3	Subscriber	Rejected and A	Above Extremely Critical	
manager	2v1pv	PDhillon3	Subscriber	- Extremely Critic	cal Extremely Critical	
<b>A</b>	2v1pv	PDhillon3	Empil petification level	Extremely Critic	cal Extremely Critical	
	2v1pv	PDhillon3	Email notification level	Extremely Critic	cal Extremely Critical	
Research	2v1pv	PDhillon3	Not Critical and Above	Extremely Critic	cal Extremely Critical	
	2v1pv	PDhillon3	SMS notification level	Extremely Critic	cal Extremely Critical	
்	2v1pv	PDhillon3		Extremely Critic	cal Extremely Critical	
Assessment	2v1pv	PDhillon3	None	Extremely Critic	cal Extremely Critical	
_	2v1pv	PDhillon3		Extremely Critic	cal Extremely Critical	
<b>£</b>	2v1pv	PDhillon3		Extremely Critic	cal Extremely Critical	
<u>*</u>	2v1pv	PDhillon3	Cancel S	Extremely Critic	cal Extremely Critical	
~¥	2v1pv	PDhillon3	syoun res	Extremely Critic	cal Extremely Critical	
Settings	2v1pv	PDhillon3	BKelly Yes	Extremely Critic	cal Extremely Critical	

- 3. Watch List created as shown in Create Watch Lists will appear in the Watch List drop down, Select the watch list.
- 4. Add a required user from the **Subscriber** drop down.
- 5. Select any of the below Email notification level from the drop down based on the requirement
  - Extremely Critical
  - Highly Critical and Above
  - Moderately Critical and Above
  - Less Critical and Above
  - Not Critical and Above

- Rejected and Above
- None
- 6. Select any of the below SMS notification level from the drop down based on the requirement:
  - Extremely Critical
  - Highly Critical and Above
  - Moderately Critical and Above
  - Less Critical and Above
  - Not Critical and Above
  - Rejected and Above
  - None
- 7. Click Save to add the subscription to the watch list.
- 8. List of added subscriptions will appear in the Settings > Vulnerability Management > Watch List Subscriptions, Admin user can edit or delete any existing subscription from the list.
- 9. Select the required subscription from the list, you can see the **Edit** and **Delete** button.

🔒 Softv	ware Vulnerability Res	earch	Settings > Vulnerability Managen	nent > Watch List Subscriptions				s 0 -1
(7)	Dashboard		Account - User Manager	ment - Vulnerability Management -	Workflow Management		•	
			Browsing 1-20 of 97 watch list subscri	iptions 🦸				+
Ê	Notifications	415)	Watch List Name	Watch List Owner	Subscriber	Enforced by admin	Email notification level	SMS notification level
			15march	PDhillon3	asutar	No	None	None
	Vulnerability Manager					Edit Delete		
			15march	PDhillon3	PDhilon3	Yes	Not Critical and Above	None
0			2prod	PDhillon3	Ashaj	No	None	None
a.	Research		2 prodssss1234	PDhilon3	Ashaj	No	Rejected and Above	Extremely Critical
			2 prodesesses	PDhillon3	Ashaj	No	Rejected and Above	Extremely Critical
2			2vtpv	PDhillon3	Ashaj	No	Extremely Critical	Extremely Critical
•	Assessment		2v1pv	PDhillon3	SVMTestRoot	Yes	Extremely Critical	Extremely Critical
_			2v1pv	PDhillon3	mmarino	Yes	Extremely Critical	Extremely Critical
ىكر	Patching		2v1pv	PDhilon3	LMalliu	Yes	Extremely Critical	Extremely Critical

- 10. Click Delete button to delete the selected subscription from the list.
- 11. Click Edit button to edit the Subscriber, Email notification level and SMS notification level of the selected subscription.

Edit subscription - 15march	×
Subscriber	
BKelly	Ŧ
Email notification level	
None	•
SMS notification level	
None	•
Cancel Save	
	4

Note • You can subscribe a user only once to the Watch List

# **Workflow Management**

Workflow Management allows you to set up detailed workflows that align with processes already in use within your organization. There is no limit to the number of Workflows that can be created.

Use the Workflow Management pages to create and edit Rules, Ticket Queues, Ticket Status and Ticket Priorities.

7

Rules

r

- Ticket Queues
- Ticket Status
- Ticket Priorities

## **Rules**

Rules can partially or fully automate workflow. They can only be created by an Administrator and must contain at a minimum one trigger and one action. For a list of rule triggers and actions, see Rule Channels, Triggers, and Actions. If needed, you can configure many different options into one rule.

Settings > Work	flow Management > Rule	5		₽ -1	
Account 🗸	User Management 👻	Vulnerability Management 👻	Workflow Management 👻	Assessment - API - Logs -	
Browsing 1-5 of 1	ō rules 🦸			Q Search by keyword	Reset
Approve advi	sories notification 💈			Z Edi	t 💼 Delete
	Advisory released for a Watch List with approval flow.	> 🌲 Notify +	Email		
Create tickets	1			🖉 Edi	it 💼 Delete
	Advisory released for a Watch List.	Create	Change ticket + assignment	L Notify + E	

To create a rule, see Create a Workflow Rule - Overview.

Workflow Rules can be created for many tasks. You can customize your workflow rule or use one of the Software Vulnerability Research Default Workflow Rule Examples.

The Rule channels, their associated triggers, and available actions are shown in the following table.

#### Table 14-3 • Rule Channels, Triggers, and Actions

Channel	Trigger	Action			
Channel Advisory	<ul> <li>Advisory for Watch List approved</li> <li>Any Watch List or select a Watch List from the drop-down list</li> <li>Any Watch List Group or select a Watch List Group from the drop-down list</li> <li>Select Advisory Condition or select a Advisory Condition from the drop down list</li> <li>Advisory for Watch List changed</li> <li>Any Watch List or select a Watch List from the drop-down list</li> <li>Any Watch List or select a Watch List Group from the drop-down list</li> <li>Any Watch List Group or select a Watch List Group from the drop-down list</li> <li>Select Advisory Condition or select a Advisory Condition from the drop down list</li> <li>Select Advisory Condition or select a Advisory Condition from the drop down list</li> <li>Select Advisory Condition or select a Advisory Condition from the drop down list</li> <li>Advisory released for a Watch List with approval flow</li> <li>Any Watch List Group or select a Watch List Group from the drop-down list</li> <li>Select Advisory Condition or select a Watch List Group from the drop-down list</li> <li>Any Watch List Group or select a Watch List Group from the drop-down list</li> <li>Select Advisory Condition or select a Advisory Condition from the drop down list</li> <li>Advisory released for a Watch List</li> <li>Any Watch List or select a Watch List from the drop-down list</li> <li>Any Watch List Group or select a Watch List Group from the drop-down list</li> <li>Any Watch List Group or select a Watch List Group from the drop-down list</li> <li>Select Advisory Condition or select a Watch List Group from the drop-down list</li> <li>Any Watch List Group or select a Watch List Group from the drop-down list</li> <li>Any Watch List Group or select a Watch List Group from the drop-down list</li> <li>Product version end-of-life</li> <li>Notify for all, default only for my tracked product</li> </ul>	<ul> <li>Action</li> <li>Email</li> <li>SMS</li> <li>Notify</li> <li>Create Advisory for Watch List</li> <li>Create ticket</li> <li>Change ticket assignment</li> <li>Change ticket queue</li> <li>Change ticket status</li> </ul>			
	<ul> <li>Notify for all, default only for my tracked product versions (select Yes or No from the drop-down list)</li> </ul>				

#### Table 14-3 • Rule Channels, Triggers, and Actions (cont.)

Channel	Trigger	Action
<b>Advisory</b> (continued)	<ul> <li>Advisory Threat for Watch List changed</li> <li>Any Watch List or select a Watch List from the drop-down list</li> <li>Any Watch List Group or select a Watch List Group from the drop-down list</li> <li>Select Advisory Condition or select a Advisory Condition from the drop down list</li> <li>Skip trigger if score decreases (Select Yes or No from the drop down list)</li> </ul>	
Analytics	PDF Report Generated	<ul> <li>Email PDF report</li> <li>Email</li> <li>SMS</li> <li>Notify</li> </ul>
Patch	<ul> <li>Patch available, with template</li> <li>Patch available, without template</li> <li>Patch affecting my environment (select Yes or No from the drop-down list)</li> </ul>	<ul> <li>Email</li> <li>SMS</li> <li>Notify</li> <li>Patch - Create packages</li> <li>Patch - Publish packages</li> <li>Create ticket</li> </ul>
Policy	• Policy Breached	<ul><li>Email</li><li>SMS</li><li>Notify</li></ul>
Release Notes	New Release arrived	• Email

Channel	Tri	gger	Action			
Ticketing	٠	Ticket assigned to me	•	Email		
	•	Ticket changed	•	SMS		
		• Changed by me (select Yes or No from the drop-down list)	•	Notify Create ticket		
	•	Ticket created	•	Change ticket status		
	•	Ticket priority changed	•	Change ticket queue		
	•	Ticket queue changed	•	Change ticket assignment		
	•	Ticket status changed				
User	•	Password changed	•	Email		
		• User (select from the drop-down list)	•	SMS		
	•	User Logged in	•	Notify		
		• User (select from the drop-down list)				

Note • The available actions will vary depending on the channel and trigger you select.

## **Default Workflow Rule Examples**

Software Vulnerability Research includes several Default Workflow Rules:

- Create a Workflow Rule to Send an Advisory and Ticket Information After Approval
- Create a Workflow Rule to Create a Patching Ticket
- Create a Workflow Rule to Send a New Release Notes Notification to Non-Administrators

#### Create a Workflow Rule to Send an Advisory and Ticket Information After Approval

Workflow Rules can be created for many tasks. For example, the Workflow Rule below can be used when Flexera issues an advisory for a Watch List that requires management approval and the communication of management's approval and ticket information to all Watch List users using email, PDF attachments, and SMS.

Task	Create a Workflow Rule to send an advisory and ticket information after approval				
	1. Follow steps 1-3 from the task Create a Workflow Rule.				

- 2. From the drop-down Rule Trigger List:
  - Select Advisory from the Channel list

- Select Advisory released for a Watch List from the Trigger list
- Enter the appropriate Watch List and Watch List Group information
- Select Advisory Condition
- Click Save
- 3. For actions, select **Create Ticket** and **Send email**. When an advisory is released, a ticket is created and The Watch List Group users will receive an email with the ticket information and the Advisory as a PDF attachment. See the following screen shot for details.

Se	ttings <b>&gt;</b> Worl	kflow Management > Rules											8	-
	Account 👻	User Management 👻	Vulnerability Management 👻	Workflow Management 🗸	Assess	sment <del>-</del>	API 👻	Logs 👻						
Bro	owsing 2 rules	i			Q,								× + Re	set
:	SVM-300 Adv	isory created 🧃											🗭 Edit 🧴 Dele	te
		Advisory released for a Watch List.	Create	Change ticket + assignment	Â.	Notify	+	$\sim$	Email	+	<b>SHS</b>	SMS		>
	Thoose Rule Trig	zger			ge 1	of 1 Þ 🖡	ж							
	Advisory			*			-							
	Advisory for Wate	ch List changed		-										
	Any Watch List			-										
	Any Watch List Gr	roup		•										
	Select Advisory Co	ondition 🔺		× +										
	Advisory Title co	ontains	Save											
	Advisory Unitica Advisory Where	a la	Cancel											
	Advisory Solutio	on Status	Cancer											
	Advisory Zero D	Day												
	Advisory CVE(s)													
	Advisory CVSS S	Score												
	Advisory Threat	t Score												
	Advisory Initial	Release Date												
	Advisory Currer	nt Release Date												

### 

**Note** • Customized workflow rules for Watch Lists take precedence over non-customized workflow rules using the following hierarchy from most important to least important:

- Rule for a specified watch list
- Rule for a watch list group
- General rule with no watch list or watch group

For example, if a watch list is in a customized workflow rule with a watch list selected and in a rule with a watch group selected, only the rule specified for the watch list will execute.

However, when you have two identical customized workflow rules that affect the same watch list or the same watch list group, the system will not know which rule takes precedence. Therefore, neither customized workflow rule will execute.



**Note** • The PDF attachment option is set at the user level. Any user wishing to receive PDF advisory information needs to select this option from the **User Profile** page. Under **Personal settings** ensure the following options have been enabled: **Receive normal emails** for Advisory type email and **Yes** for Attach advisory PDF. See the screen shot below for details.

	Personal settings	
	Advisory type email (default normal item):	Receive normal emails -
	Attach advisory PDF (default no): Yes	-
Settings	Cancel Save	
User Profile	© 2015 – 2018 Flexera. All rights reserved. <u>Terms_an</u>	d Conditions Data Privacy

#### Create a Workflow Rule to Create a Patching Ticket

You can create a Workflow Rule to create a ticket for when a new patch is available.

## Task

#### Create a Workflow Rule to create a patching ticket:

- 1. Select either rule: Patch available no profile notification or Patch Available with custom profile and click Edit.
- 2. Click Add action.
- 3. When the Choose Action pop-up window appears, click Create ticket.
- 4. Enter the **Ticket Status** and **Ticket Queue** information and click Save. Add any additional actions required and save the rule.
- 5. To view and export patching ticket information, see Patching Tickets in the Patching module or in the Ticket Manager.

#### Create a Workflow Rule to Send a New Release Notes Notification to Non-Administrators

You can create a Workflow Rule to notify non-administrators of the latest Software Vulnerability Research release notes.



Note • All administrator accounts are configured to receive release note notification emails in the Notifications module.



- 2. Enter the appropriate users to Notify.
- 3. Click Email.

## **Ticket Queues**

This page displays the Ticket Queue details.

Settings > Workflow Management > Ticket Queues									
Account -	User Management 👻	Vulnerability Management 🗸	Workflow Management 👻	Assessment -	API 👻	Logs 🗸			
Browsing 3 queues				+					
Queue		Visible by all users			User Groups				
Default		Yes							
Edit Dek									
Approval		No			Advisory App	rove Managers			
Test		No							
			F	🖌 📢 Page 🔤 1	of 1 🕨 🔛				

Ticket Queues can be used for sharing and limiting access to tickets for users. You can create ticket queues that are relevant to a limited subset of your users (for instance only for Linux administrators or for Windows administrators) and use Rules to create tickets from special Watch Lists directly on those ticket queues.

Click a queue in the list to edit or delete the queue or click 💶 to add a new ticket queue.

## **Ticket Status**

This page displays the **Ticket Status** values.

Settings > Workflow Management > TicketStatus									-₹D
Account -	User Management 👻	Vulnerability Management 👻	Workflow Management 👻	Assessment -	API 👻	Logs 👻			
Browsing 4 statuse	s Ź								+
Status		Default ticket status					Number of tickets		
Open		Open					4699		
Waiting		Waiting					1		
Handled		Handled					0		
Irrelevant		Irrelevant					0		
			E.	K 🛠 Page 1 o	1 22 22				

Click 🚺 to add a ticket status. The default values are:

- Open
- Waiting
- Handled
- Irrelevant

You can click any ticket status that you have added to edit it or delete statuses that do not have tickets assigned.

## **Ticket Priorities**

This page displays the Ticket Priority values.

Settings > Workflow Management > Ticket Priorities								2	-10
Account +	User Management 👻	Vulnerability Management 👻	Workflow Management 👻	Assessment 👻	API 👻	Logs 👻			
Browsing 4 priorities 🦸							1	+	
Priority		Default ticket priority					Number of tickets		
Low		Low					2331		
Medium		Medium					1344		
High		High					1000		
Urgent		Urgent					25		
Het 📢 Page 🚺 of 1 🍉 🔛									

Click 💶 to add a ticket priority. The default values are:

Low
- Medium
- High
- Urgent

You can click any Ticket Priority that you have added to edit or delete priorities that do not have tickets assigned.

# Assessment

Edition • These Assessment settings are not available for Software Vulnerability Research.

Under **Assessment**, you can Update Servers & Daemon, perform a Scan Configuration, and perform Downloads of current and older versions of agent installers, agents, and daemons.

- Update Servers & Daemon
- Scan Configuration
- Downloads

### **Update Servers & Daemon**

This page displays details of all Windows Server Update Services (WSUS) servers and how to install, configure and troubleshoot the Software Distribution Daemon for Windows in your environment.

- Daemon Resources
- Daemon and WSUS Troubleshooting
- Certificate Configuration
- Certification Authorities

#### **Daemon Resources**

This section explains:

- Daemon Software Requirements
- Certificate Configuration
- Daemon Command Line Switches

#### **Daemon Software Requirements**

The Software Distribution Daemon for Windows has the following software requirements.

- 64 Bit Operating System. Windows 7 +
- Windows Server Update Services (WSUS) administrative console needs to be installed. You need to install the admin tools version that corresponds to your WSUS server.

- Access Privileges to run the Daemon as a service
- Access Privileges to makes changes to the WSUS server
- .Net 4.52
- Internet Connection SSL 443/TCP to https://app.flexerasoftware.com/

#### **Daemon Log File Size**

As the Daemon runs, it logs important actions, warnings, and errors. When logging to a file, the size and backup strategy of this file are controlled by the registry values named LogFile, LogMaxKB, and LogBackup. LogFile specifies the name of the active log file. LogMaxKB specifies the size at which the log file is backed up and restarted. LogBackup specifies a date string format that is appended to the name of the log file to create each backup file. If LogMaxKB is 0 or negative, the log file grows forever. If LogBackup is empty, the current log is instead discarded when it grows past the specified size.

The screen shot below lists the default settings for the Daemon log.

Name	Туре	Data
ab) (Default)	REG_SZ	(value not set)
ab LogBackup	REG_SZ	-yyyyMMdd-HHmm
ab LogFile	REG_SZ	<commonapplicationdata>\Flexera Software\SVM\svmpd.log</commonapplicationdata>
ab LogLevel	REG_SZ	Verbose
ab LogMaxKB	REG_SZ	16384

#### **Daemon Command Line Switches**

Software Vulnerability Research has the following daemon command line switches.

- Help
- Help Text
- Force Daemon to Poll the Server for New Tasks
- Force Daemon to Poll the Server for New Tasks
- Daemon Command Line to Create WSUS Certificate
- Ask Daemon to Display Where an Update Will Be Applied

#### Help

To access the help command line switch type:

svmpd.exe help

#### **Help Text**

To access the help text command line switch type:

```
SVM Package Daemon Copyright (C) 2012-2017 Flexera Software LLC. All rights reserved.
Usage: svmpd.exe ACTION [OPTIONS]
ACTION is one of:
```

NewCert: Create a WSUS publishing certificate Scan: Scan a WSUS server for data ServiceCommand: Send the service a custom command ShowPackageStats: Get installation statistics for a package, by group UseCert: Set the WSUS publishing certificate Version: Show version information Or help [ACTION]: Get detailed help for ACTION All actions support the following global flags in any location: /cl: One of LogAlways, Critical, Error, Warning, Informational, Verbose Set the level for console logging /output or /o: <String> Save output to specified file /format or /f: One or more of Raw, Indent, Compress Control JSON output format. Compress only works with /output. /wsus: <Uri> Override the WSUS server

#### Force Daemon to Poll the Server for New Tasks

To force the daemon to poll the server for new tasks type:

svmpd.exe servicecommand polltasksnow

#### **Daemon Command Line to Create WSUS Certificate**

To create a WSUS certificate, type the following Daemon command line:

sympd.exe newcert

#### Ask Daemon to Display Where an Update Will Be Applied

The following Daemon command line displays where an update will be applied. svmpd.exe showpackagestats bc5f5d64-f2aa-4c6d-bd3f-8cf9915cfb82 After typing the above command line, you will see the following output.

```
{
    "server_name": "svm-w16-wsus.svm.flexdev.com",
    group_id": "af6f2ec0-b1ce-4344-9f61-9e3e0cb6cda3",
    "group_name": "Windows 8.1",
    "approvals": [
      {
        "by": "SVM\\JSmith",
        "at": "2017-05-25T20:58:57.213Z",
        "action": 0,
        "is_optional": false
     }
    ],
    "not_applicable": 0,
    "pending": 4,
    "installed": 0,
    "failed": 0
 },
    "server_name": "svm-w16-wsus.svm.flexdev.com",
    "group id": "a0a08746-4dbe-4a37-9adf-9e7652c0b421",
    "group_name": "All Computers",
```

```
"approvals": [
    {
      "by": "SVM\\JSmith",
      at": "2017-05-25T20:58:57.193Z",
      "action": 0,
      "is_optional": false
    }
  ],
  "not_applicable": 1,
  "pending": 18,
  "installed": 0,
  "failed": 1
},
{
  "server_name": "svm-w16-wsus.svm.flexdev.com",
  "group_id": "b73ca6ed-5727-47f3-84de-015e03f6a88a",
  "group_name": "Unassigned Computers",
  "approvals": [
    {
      "by": "SVM\\JSmith",
      "at": "2017-05-25T20:58:57.2Z",
      "action": 0,
      "is_optional": false
    }
  ],
  "not_applicable": 0,
  "pending": 2,
  "installed": 0,
  "failed": 0
},
{
  "server_name": "svm-w16-wsus.svm.flexdev.com",
  "group_id": "8b4b8cf9-4d99-48fc-93ce-bdb16ce624e1",
  "group_name": "Windows 7",
  "approvals": [
    {
      "by": "SVM\\JSmith",
      "at": "2017-05-25T20:58:57.21Z",
      "action": 0,
      "is_optional": false
    }
  ],
  "not_applicable": 0,
  "pending": 8,
  "installed": 0,
  "failed": 1
},
{
  "server_name": "svm-w16-wsus.svm.flexdev.com",
  "group_id": "57c2d480-05c5-4a2a-9a18-df11281559ca",
  "group_name": "Windows 10",
  "approvals": [
    {
    "by": "SVM\\JSmith",
    "at": "2017-05-25T20:58:57.203Z",
    "action": 0,
```

```
"is_optional": false
}
],
"not_applicable": 1,
"pending": 4,
"installed": 0,
"failed": 0
}
```

### **Daemon and WSUS Troubleshooting**

This section provides troubleshooting for the following topics:

- Daemon Configuration
- WSUS Configuration and Certificate Troubleshooting
- Daemon Logging

#### **Daemon Configuration**

If the User Account you have set up does not have the ability to run a service, the following error message will appear:



¢

#### Task To troubleshoot the configuration of the Daemon:

- 1. Leave the error message up.
- 2. Go to the Services applet and find the Flexera Software Vulnerability Research Daemon.
- 3. Right click Properties.
- 4. Go to the Log On tab and set the same user, which will trigger Windows to add that account to the correct group. When the Services window appears, click OK.
- 5. Go back to the error message and click Retry to complete the installation.

#### WSUS Configuration and Certificate Troubleshooting

If you enter the incorrect WSUS server settings in the registry, you will see an error message like the one below.

```
c:\Program Files\Flexera Software\SVM Daemon≻svmpd.exe scan Groups
System.NotSupportedException
Error providing service IWsusApi
```

Before you enter the correct registry key and WSUS Server, make sure the service is STOPPED. Otherwise, the registry key value will be erased when you do stop the service, and you will need to reenter the registry key.

To create WSUS certificates, see:

- Daemon Command Line to Create WSUS Certificate
- Saving Successful WSUS Self-Signed Certificates

#### **Daemon Logging**

Logs are written here:

C:\ProgramData\Flexera Software\SVM

📊   📝 📑 =   SVM									
File Home Share View									
← → → ↑ 📙 > This PC > Local Disk (C:) > ProgramData > Flexera Software > SVM									
📥 Quick access	Name	^	Date modified	Туре	Size				
Desktop	* svmpd	5	5/15/2017 2:51 PM	Text Document	1 KB				

You can customize the following logging level settings.

- Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Flexera\SVMPD
- LogLevel: Can be Informational, Verbose
- WSUSServer: Scheme, URL and Port for WSUS. Example: http://svm-w16-wsus.svm.flexdev.com:8530/

#### File Edit View Favorites Help 🗸 💻 Computer Name Data Туре - HKEY CLASSES ROOT ab (Default) REG\_SZ (value not set) HKEY\_CURRENT\_USER AccountAuthTo... 01019198908c81ef89330d2f013d0fe051f3619a2a34c... REG SZ HKEY LOCAL MACHINE ab LogBackup REG SZ -vvvvMMdd-HHmm BCD0000000 ab LogFile REG SZ <CommonApplicationData>\Flexera Software\SV... HARDWARE REG\_SZ LogLevel Informational SAM ab LogMaxKB REG\_SZ 16384 SECURITY ab LogMethod REG SZ File SOFTWARE 👲 RefreshToken REG\_SZ 01019198908c81ef89330d6d013d0ffd51f3619a2a34... Classes **ab** ServerHost REG\_SZ uat-agent.app.flexerasoftware.com Clients ServerPort REG\_DWORD 0x000001bb (443) Flexera ab SvmLastPolled REG\_SZ 5/16/2017 10:41:20 AM +00:00 GUID SVMPD ab SvmLastPollSuc... REG SZ 5/16/2017 10:41:21 AM +00:00 Intel SymPollPeriod 00:10:00 REG SZ Microsoft ab SvmServer REG\_SZ https://uat-agent.app.flexerasoftware.com/api/ ODBC ab TempToken REG\_SZ 010191985fe956c489330d6d013d0ffd51f3619a2a34... Partner ab WsusServer REG SZ http://svm-w16-wsus.svm.flexdev.com:8530/ Policies 2 RegisteredApplication WOW6432Node Classer

#### **Successful Publishing Log Example**

Below is an example of a successful publishing log.

```
[5/24/2017 6:07:51 PM|I] Flexera Software SVM Package Daemon: Terminating {
```

```
"SvmServer": "https://uat-agent.app.flexerasoftware.com/api/",
```

```
"WsusServer": "http://svm-w16-wsus.svm.flexdev.com:8530/",
```

```
"AccountAuthToken":
```

📑 Registry Editor

"01019198908c81ef89330d2f013d0fe051f3619a2a34c53dd23821f3b009cb8872a0381e4daa4a05e3368c4a534aca36e48680 b22522c73cb0003ea65febcbd27687dd5d8b8e31fd4bfcab6c7afc2d128b46f501a92fd51423f9f51277f15ad9cdc5a9b20c051 71d415709cfaba76978d39bc5294439cf70024f47273f787a9797705737c78be366efaa19450d6dbd9783ff2cc7", "RefreshToken":

"01019198908c81ef89330d6d013d0ffd51f3619a2a34c53dd23821f3b009cb8872a0381e0570bd60d58c8c78e9b82c1e2554a3 4780d032670fd350336f859188fbc1e60a368d6337761dc797d374a696fcedea1ee1260e4a05b4d02156a025075e1933c80de07

```
f382b0d33e4f96f3a92fc4e55b19d9384d441373b6bbd7d75eda8c119b7a47a706b3008468c58c23f6df268516f", "TempToken":
```

"010191985fddb4f489330d6d013d0ffd51f3619a2a34c53dd23821f3b009cb8872a0381eeaff654ba8173863126de272ea85b4 ad685fd33b6ee34fc804ebe454fe6c61202a42b832079127b9af1dde7d1aae210f34cd5a79666516aedeceb14a0452f7858f223 920b457408c8dcabbb97da41e6b17ad32140a757dd3fbaf33742032b988c7d0ec366e83528d84a7c4cdd38aa712",

```
"GUID": "dbbad2b3-b298-4f01-ad4b-717df294f6f2",
"LogMethod": "File",
"LogLevel": "Verbose",
"LogFile": "<CommonApplicationData>\\Flexera Software\\SVM\\svmpd.log",
"LogMaxKB": "16384",
"LogBackup": "-yyyyMMdd-HHmm",
"SvmLastPolled": "5/24/2017 6:01:54 PM +00:00",
"SvmLastPollSuccess": "5/24/2017 6:01:54 PM +00:00",
"SvmPollPeriod": "00:10:00"
}
--- Configuration Ends ---
[5/24/2017 6:07:52 PM|I] Flexera Software SVM Package Daemon: Initializing
```

[5/24/2017 6:11:56 PM|I] Cached new 6e16403a-042f-49db-9106-7d0fab21d4b9.sdp at C:\ProgramData\Flexera
Software\SVM\SVMPD Cache\6e16403a-042f-49db-9106-7d0fab21d4b9.sdp; file is unsigned; hash
768B93104B08C65C4FD17F4BB621437C569DC5E0

Deployment Information - Install/Update Google Chrome 49.x to 58.x Default	×
installer	

Deployment inform	ation						
Server	svm-w16-wsus.svm.flex.dev.com						
Groups	Windows 7						
Package name	Install/Update Google Chrome 49.x to 58.x Default installer						
Product name	Google Chrome 49.x						
Vendor name	Google						
Status	Building						
Created	May 24, 2017 1:10 PM						
Deployment tasks							
Task type	Push package to Patch Server						
Created	May 24, 2017 1:10 PM						
Result	Success						
Daemon	708e0a8b-a0c6-4fce-b8eb-4f97be901933						

Close

### **Certificate Configuration**

Certificates are saved based on the certificate process used:

- Saving Successful WSUS Self-Signed Certificates
- Saving Manual Self-Signed Certificates

#### Saving Successful WSUS Self-Signed Certificates

A successful WSUS self-signed certificate must be saved in the following three locations: Trusted Root Certification, Trusted Publishers, and WSUS. The "Trusted Root Certification Authority" should contain the relevant Root certificate.



Not copying the certificate's public key to any one of the three locations (in particular the Trusted Publishers location), or not having the private key in the WSUS location, may cause publishing to fail with the following error message.

[5/22/2017 7:03:30 PM|C] Task execution faulted (id: adc97f47-5c41-442b-b19d-f266a2d8adec): Verification
 of file signature failed for file:

\\win2008r2sccm12.isas.flexdev.com\UpdateServicesPackages\6e16403a-042f-49db-9106-7d0fab21d4b9\bbee425c-fa3d-46dd-a703-065fd184fe86\_1.cab

- InvalidOperationException: Verification of file signature failed for file: \\win2008r2sccm12.isas.flexdev.com\UpdateServicesPackages\6e16403a-042f-49db-9106- 7d0fab21d4b9\bbee425c-fa3d-46dd-a703-065fd184fe86\_1.cab
  - at Microsoft.UpdateServices.Internal.BaseApi.Publisher.VerifyAndPublishPackage()
  - at Microsoft.UpdateServices.Internal.BaseApi.Publisher.PublishPackage(String sourcePath, String additionalSourcePath, String packageDirectoryName)
  - at System.Threading.Tasks.Task.Execute()
  - at FlexeraSoftware.SVM.Daemon.WsusApi.PublishPackageAsync()
  - at FlexeraSoftware.SVM.Daemon.PublishPackageWorkItem.PublishPackageAsync()
  - at FlexeraSoftware.SVM.Daemon.DaemonWorkItem.ExecuteTasks()
- --- Stack Trace Ends ---

#### **Troubleshooting Options for WSUS Self-Signed Certificate Error Message**

You have two options to create the new certification if this error message appears:

c:\Program Files\Flexera Software\SVM Daemon>svmpd.exe newcert

System.InvalidOperationException

This WSUS server cannot issue a self-signed certificate. To import a signing certificate into the WSUS server, use one of the following supported methods:

- - 2. Use a real certificate, and use the sympd.exe option UseCert.

SetSigningCertificate(string, string)

#### Saving Manual Self-Signed Certificates

The certificate used to sign packages must be saved on the machine with the Software Distribution Daemon for Windows (SVMDaemonINstall.msi).

藩 Console1 - [Console Root\Certificates (Local Compu	ter)\Trusted Publishers\Certificates]					-	□ ×
Tile Action View Favorites Window Help							- 8 ×
🗢 🔿 🙍 🚮 🦌 🗞 🗶 🖬 🛃 🛅							
🤗 Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Actions	
✓ ☐ Certificates (Local Computer)	🛱 WSUS Publishers Self-signed	WSUS Publishers Self-signed	6/12/2022	Code Signing	<none></none>	Certificates	<b></b>
> Personal Trusted Root Certification Authorities	🛱 WSUS Publishers Self-signed	WSUS Publishers Self-signed	6/13/2022	Code Signing	<none></none>	More Actions	•
> iii Enterprise Trust	Flexera Software LLC	Symantec Class 3 SHA256 Code Si	11/21/2018	Code Signing	<none></none>	Flower College U.C.	
> intermediate Certification Authorities						Flexera Software LLC	-
✓ I Trusted Publishers						More Actions	+
Certificates							
> iii Untrusted Certificates							
> Initial Party Root Certification Authorities							
Trusted People							
Client Authentication Issuers							
> Preview Build Roots							
> 🚞 Other People							
> 🚞 Remote Desktop							
Certificate Enrollment Requests							
Smart Card Trusted Roots							
Trusted Devices							
> iii Web Hosting							
> 📔 Windows Live ID Token Issuer							
> 🚞 WSUS							

### **Certification Authorities**

If you see the following Windows Update 800b0109 error message, this means your WSUS certificate is not installed on the machine trying to install the update.



Console1 - [Console Root\Certificates (Local Computer)\Trusted Publishers\Certificates]									
See File Action View Favorites Window Help									
🗢 🔿 🙍 🖬 🤞 💺 🖬 😹									
Console Root	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly	Actions			
Certificates (Local Computer)     Personal	WSUS Publishers Self-signed	WSUS Publishers Self-signed	5/24/2022	Code Signing	<none:< td=""><td>Certificates</td><td>-</td></none:<>	Certificates	-		
a 📔 Trusted Root Certification Autho	13					More Actions	•		
Certificates						WSUS Publishers Self-signed	-		
<ul> <li>Enterprise Trust</li> <li>         ■ Trusted Publishers         ■ Certificates         ■ Untrusted Certificates         ■ Trusted People         ■ Trusted People         ■ McAfee Trust         ■ Smart Card Trusted Roots         ■ Trusted Devices     </li> </ul>						More Actions	•		

# **Scan Configuration**

Use this page to view, configure and edit the:

- Scan Configuration
- Microsoft Update Options
- Add Custom Scan Paths

Account - User Ma	anagement 🗸	Vulnerability Management 👻	Workflow M	anagement 👻	Assessment +	API 👻	Logs 👻		
Scan Configuration				Microsoft Upda	ate Options				
Define the default scan age Scan Type Minimal scan Scan day(s) Sunday, Monday, Frid Scan time	ent behaviour Jay, Tuesday, Satu	irday, Wednesday, Thursday	Configure the behaviour of the Windows Update (WUA) Check for missing security updates from Microsoft System Center Check for missing security updates from Windows Update Update Server Type Official Microsoft Update Update Proxy Settings						
12 : 10 Edit	12 : 10				Use default WUA proxy settings Edit				
Custom scan paths	Custom scan paths								
Note: Mixing Block list and	d Allow list rules is n	ot supported. Allow list will take preced	ence.						
Туре	Path			Filen	ame		Created		\$
Block List		am Files\7-Zip		shatn	0.608		2020-08-07		
KK KK Page 1 of 1 🕨 🕅									

### **Scan Configuration**

Click Edit and select:

- Scan type (select Disabled (do not scan), Minimal scan, Optimal scan or Full scan from the drop-down list). For details, see Scan Types.
- Scan day(s) (select the day or days to perform scans from the drop-down list)
- Scan time



**Note** • The selected Scan Type does not overwrite custom scan paths you create, which are saved to every Scan Agent you have deployed to your environment.

### **Microsoft Update Options**

Click Edit and select:

- Configure the behavior of the Windows Update (WUA) (select Check for missing security updates from Windows Update. If your organization blocks updates from Windows Update, select Check for missing security updates from Microsoft System Center).
- Update Server Type (select OS Default, Managed Windows Update, Official Windows Update, Official Microsoft Update or Use offline method (CAB) from the drop-down list):
  - **OS Default:** allows the Windows Update Agent on a device being scanned to use whatever option is currently registered. This option can be controlled by enterprise policy settings or locally on the machine, depending on the environment the device is running in.
  - **Managed Windows Update:** the SVMScan.exe agent will request a check for updates through an enterprise managed WSUS instance. On machines not configured through WSUS, this check for updates will result in the error: 0x80244011 "WUServer policy value is missing in the registry".

- **Official Windows Update:** the SVMS can. exe agent will request a check for updates through the public Windows Update server. This check will only return updates related to Windows.
- Official Microsoft Update: the SVMScan.exe agent will request a check for updates through the public Windows Update server. This check will return a superset of the "Windows Update server" results that include Windows updates and updates for Microsoft products such as Office (non App-V, non App-X installs only) and MSVC redistributables.
- Use offline method (CAB): you should implement the .cab file scanning of windows update for clients that are not connected to the Internet and cannot access WSUS or MU/WU. In such situations, Microsoft provides a .cab file that can be used to scan the system. There are limitations to this feature:
  - You are responsible for placing the file in a location accessible by Windows Update Services. The file must be on the local file system; placing the file on a shared drive is not supported by Windows Update Services.
  - The alternate scan data source (.cab file) only includes high priority updates (security bulletins, critical updates, update rollups) and some service packs. It does not include optional updates (such as updates, feature packs, and tools) and some service packs. If a machine uses this source for scanning, then it is likely that fewer patches will be detected.
  - Software Vulnerability Research should be run as administrator.
- Update Proxy Settings (select Use default WUA proxy settings, Use the same proxy as http or Use a custom proxy for WUA from the drop-down list).
- If you selected Use a custom proxy for WUA, enter the Proxy Settings domain port.

### **Add Custom Scan Paths**

Click 💶 to add custom scan paths. Select the Type (Allow list or Block List) from the drop-down list, enter the Filename and Path and click Save.



**Note** • Mixing block List and allow list rules is not supported. Allow List will take precedence.



**Note** • All paths must be hard coded paths. Example: C:\Users\Public\Libraries

Add new custom path ×							
Туре							
Allow List	•						
Filename							
Filename							
Path		_					
Path							
Cancel	Save						

## Downloads

This page displays the Software Vulnerability Research download links for:

- Vulnerable Software Discovery Tool Installer for Windows
- Vulnerable Software Discovery Tool for Windows
- Software Distribution Daemon for Windows
- Vulnerable Software Discovery Tool for Mac
- Vulnerable Software Discovery Tool for Red Hat Linux 7 RPM
- Vulnerable Software Discovery Tool for Red Hat Linux 6 RPM

You can select Show older versions, click an item in the list, and select Download.

To download and deploy the appropriate item below, see Agent Deployment and Daemon Deployment.



# API

Use the API page to view your API Access token generation page, XML Feeds, and Service Providers.

XML feed shows advisory information for tickets created. If no tickets are created, no advisory information will appear in the XML feed. XML feed is not connected to **Historic Advisories** in the **Vulnerability Manager** module.

To access the Software Vulnerability Research APIs, see https://api.app.flexerasoftware.com/api/. For additional API information, see the Software Vulnerability Research API Help Library:

https://docs.flexera.com/svr/api/Default.htm

# Logs

Use the **Logs** pages to track details of all activities taken by users related to your account, such as:

- Logins
- Tickets
- Watch Lists
- Email Logs
- SMS Logs
- Service Calls

## Logins

The Logins page displays the Date, User, IP Address and User Agent details for all successful logins.

Click 🔽 to filter the results displayed by User and From and To dates

Click 🚨 to export Logins to a CSV file.

### Tickets

The **Tickets** page displays the **Date**, **Ticket**, **Change Type**, **Change Description** and **User** details for all ticket changes related to your account.

Click **I** to filter the results displayed by **User**, **Ticket ID** and **From** and **To** dates.

Click 🖪 to export Tickets to a CSV file.

### Watch Lists

The Watch Lists page displays the Date, Watch List, Change Type, Change Description and User for all Watch List changes related to your account.

Click 🔽 to filter the results displayed by User, Watch List, and From and To dates.

Click a Watch List name to view the details of the Watch List.

Click 🖪 to export Watch Lists to a CSV file.

## **Email Logs**

The **Email Logs** page displays the history of sent emails including Date, User, Email Category, Email Address, Status, and Subject.

Click **I** to filter the results displayed by **User** and **From** and **To** dates.

Click 🗳 to export Email Logs to a CSV file.

### **SMS Logs**

The **SMS Logs** page displays the history of sent SMS, including Date, User, SMS Category, Phone Number, Status, and Message.

Click **I** to filter the results displayed by **User** and **From** and **To** dates.

Click 🗳 to export SMS Logs to a CSV file.

# **Service Calls**

If service calls were made, the **Service Calls** page displays the history of changes, including **Date**, **Provider**, **URL**, **Method**, **Ref\_object\_id**, **Status code**, **Our entity**, and **Call status**.

Click C to resend failed service calls.

Click 🔽 to filter the results displayed by **From** and **To** dates.

Click do export Service Calls to a CSV file.

Chapter 14 Settings

Logs



Use the **User Profile** page to view and edit your account information, including your password, personal details, preferences, security settings, and personal settings.

After saving your phone number, you need to validate your phone number. Otherwise you will not receive SMS notifications for the advisories.

If you change your email address, you need to validate your email address immediately after. Otherwise you will not receive an email notification.

User Profil	e					?	
Username:							
Change Pas	sword						
Personal De	etails						
Title:	•						
First Name	:						
Last Name:							
Email:		Change	Email				
Phone Num	nber:						
Country:	United States	Ţ					
Preference	S						
Language:	English	~					
Timezone:	America/Chicago	Ŧ					
Security Se	ttings						
Two-factor	authentication: Enabled	ł					
Two-factor	authentication using SI	MS:					
Two-factor	authentication using to	oken:					
Personal se	ttings						
Advisory ty	pe email (default norm	al item): Select		-			
Attach advi	isory PDF (default no):	Select		<b>7</b>			
Edit							
© 2015 – 201	8 Flexera. All rights reserved	. Terms and Condition	ns <u>Data Privacy</u>		FLEX	216	Ξ

Figure 15-1: User Profile Page



# **About Secunia Advisories**

This section includes the following articles:

- CVSS (Common Vulnerability Scoring System)
- CVE References
- Where (Attack Vector)
- Criticality (Severity Rating)
- Impact (Consequence)

# CVSS (Common Vulnerability Scoring System)

The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities (see https://nvd.nist.gov/vuln-metrics/cvss).

CVSS enables IT managers, vulnerability bulletin providers, security vendors, application vendors, and researchers to all benefit by adopting this common language of scoring IT vulnerabilities.

CVSS consists of three groups: Base, Temporal, and Environmental. Each group produces a numeric score ranging from 0 to 10, and a Vector; a compressed textual representation that reflects the values used to derive the score.

- The Base group represents the intrinsic qualities of a vulnerability.
- The Temporal group reflects the characteristics of a vulnerability that changes over time.
- The Environmental group represents the characteristics of a vulnerability that are unique to any user's environment.

For details on interpreting a CVSS vector, refer to https://www.first.org/cvss/specification-document.

Secunia Advisories include a Secunia derived CVSS score and vector, as well as a link to an implementation of the NIST CVSS calculator so that a user can adjust temporal and environmental metrics for advisories that match your Watch Lists. For more information, see CVSSv3 Score.

The National Vulnerability Database (NVD) CVSS score/vector for each relevant CVE contained in an Advisory is also shown, and is similarly linked to the NIST CVSS calculator.

### **CVSSv3 Score**

On May 18, 2018 Flexera's Secunia Research began entering all new CVSS scores using the v3 standard. After a CVSSv3 score is entered, the score appears in the User Interface (UI), API, XML, email notifications, and PDF reports.

#### In the User Interface

The CVSSv3 score is noted with a green "v3" after the score.

X Vulneral	bility Manager > 🗙														Θ	- ø ×
← → C ê Secure   https://ust.app.fieeerasoftware.com/#/wn/licketing/										t 🔾 🖬 🖬 🗄						
Software Vulnerability Manager Vulnerability Manager > Ticketing											0 -D					
Ø	Dashboard	board Watch Lists & Advisories + Ticketing Approve Advisories														
Ļ	Notifications	(074)	Open ticke Browsing 1	-20 of 38 tickets	ting tickets	38 Clos	ed tickets 2	Irrelevant ticket	:s 10 Pe	nding deployment tickets 🔋 At QA tick	ets 🛛				1	Y + ±
	16.d		ID				From		1	To 🛍	Queue	*	Priority	•	Watch List	•
	vumerability manager		SAID				Criticality		•	Solution status 🔹	65	6.5	Assigned user	-	Apply	Reset
	Research												Filter	-	Save	Delete
			Id	<ul> <li>Ticket created</li> </ul>	Queue	Status	Priority	Watch List	SAID	C Title		Criticality 0	Securia Advisory published	Solution status	CVSS/Custom Score	Assigned to
the second se	Assessment		15841	2018-04-03	Default	Open	Low	b_test	SA82369	IBM Aspera faspex Multiple Vulnerabilities		-	2018-04-03	Vendor Patched	6.5 v3	asutar
			15840	2018-04-03	Default	Open	Low	testMarch15	SA82369	IBM Aspera faspex Multiple Vulnerabilities		-	2018-04-03	Vendor Patched	6.5 v3	Preeti011
يكر 💫	Patching		15838	2018-04-03	Default	Open	Low	Subscription_301	SA82369	IBM Aspera faspex Multiple Vulnerabilities		-	2018-04-03	Vendor Patched	6.5 v3	PDhillon3
			15837	2018-04-03	Default	Open	Low	SVM-162watchlist	SA82369	IBM Aspera faspex Multiple Vulnerabilities		-	2018-04-03	Vendor Patched	6.5 v3	PDhillon3
			15836	2018-04-03	Default	Open	Low	All Advisories	SA82369	IBM Aspera faspex Multiple Vulnerabilities		-	2018-04-03	Vendor Patched	6.5 v3	JSkorski
	Policy Manager	4628	13914	2018-03-14	Default	Open	Low		SA81990	Microsoft SharePoint Foundation 2013 Securit	y Bypass Vulnerability		2018-03-14	Vendor Patched	6.5	pdhillon
			13913	8 2018-03-14	Default	Open	Low	All Advisories	SA81990	Microsoft SharePoint Foundation 2013 Securit	y Bypass Vulnerability	-	2018-03-14	Vendor Patched	6.5	JSkorski
	Appletics		13912	2018-03-14	Default	Open	Low		SA81990	Microsoft SharePoint Foundation 2013 Securit	y Bypass Vulnerability	_	2018-03-14	Vendor Patched	6.5	pdhillon
9	Analytics		13911	2018-03-14	Default	Open	Low	Subscription_301	SA81990	Microsoft SharePoint Foundation 2013 Securit	y Bypass Vulnerability		2018-03-14	Vendor Patched	6.5	PDhillon3
			13910	2018-03-14	Default	Open	Low	SVM-162watchlist	<u>SA81990</u>	Microsoft SharePoint Foundation 2013 Securit	y Bypass Vulnerability		2018-03-14	Vendor Patched	6.5	PDhillon3
			13909	2018-03-14	Default	Open	Low	FNMS_Import	SA81990	Microsoft SharePoint Foundation 2013 Securit	y Bypass Vulnerability	_	2018-03-14	Vendor Patched	6.5	SVMTestRoot
			13908	3 2018-03-14	Default	Open	Low	Tier1 Vendors	SA81990	Microsoft SharePoint Foundation 2013 Securit	y Bypass Vulnerability	_	2018-03-14	Vendor Patched	6.5	SVMTestRoot
			13907	2018-03-14	Default	Open	Low	Mostl/Yanted	SA81990	Microsoft SharePoint Foundation 2013 Securit	y Bypass Vulnerability		2018-03-14	Vendor Patched	6.5	mkoppen
			11907	2018-02-07	Default	Open	Medium		SA81512	Mageia update for php-smarty			2018-02-07	Vendor Patched	6.5	pdhillon
			11896	2018-02-07	Default	Open	Medium	Subscription_301	SA81512	Magela update for php-smarty		_	2018-02-07	Vendor Patched	6.5	PDhillon3
			11895	2018-02-07	Default	Open	Medium	SVM-162watchlist	SA81512	Mageia update for php-smarty			2018-02-07	Vendor Patched	6.5	PDhillon3
			11894	2018-02-07	Default	Open	Medium	All Advisories	SA81512	Mageia update for php-smarty			2018-02-07	Vendor Patched	6.5	JSkorski
			10788	2018-01-23	Default	Open	Medium	AllAdvisoryList_AJ	SA81247	Debian update for smarty3			2018-01-23	Vendor Patched	6.5	PDhillon3
			10785	5 2018-01-23	Default	Open	Medium	All Advisories	<u>SA81247</u>	Debian update for smarty3			2018-01-23	Vendor Patched	6.5	JSkorski
- Q.	Settings		10779	2018-01-23	Default	Open	Medium		SA81247	Debian update for smarty3			2018-01-23	Vendor Patched	6.5	pdhillon
										20 🔺 H4 44 Pa	ge 1 of 2 🕨 🙌					
2	User Profile		@ 2015 _ 201	18 Elevera All rights	s reserved. Ten	ms and Co	onditions Data	Privace							FI	<mark>₽</mark> ×₽га

#### In the API

API calls returning CVSS data return a second set of values for CVSSv3, so that you can programmatically differentiate between CVSSv2 and CVSSv3 scores. When CVSSv3 scores are available, the cvss\_score value is blank and the value will appear as cvss3\_score. The label cvss\_score represents CVSSv2 (it was not renamed to avoid breaking existing scripts).

```
"cvss_info": {
    "cvss_vector": "",
    "cvss_base_score": 0,
    "cvss_overall_score": 0
},
    "cvss_score": "0.0",
    "cvss_vector": "",
    "cvss_vector": ",
    "cvss_linfo": {
        "cvss_vector": "CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:0/RC:C",
        "cvss_base_score": 7.8,
        "cvss_overall_score": 6.8
},
    "cvss3_score": "7.8",
    "cvss3_vector": "CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:0/RC:C",
    "cvss3_vector": "7.8",
    "cvss3_score_ui": "7.8",
```

#### In the XML

A change to the schema is necessary to add specific values for CVSSv3 scores. As with the json API values above, a second cvss3 labeled value was added to distinguish v3 scores. Depending on how any scripts or processes consuming this data parse the information, **this has the potential to result in a breaking change.** 

<cvss\_base\_score>0</cvss\_base\_score> <cvss\_overall\_score>0</cvss\_overall\_score> <custom\_cvss\_overall\_score>0.0</custom\_cvss\_overall\_score> <custom\_cvss\_vector></custom\_cvss\_vector> <cvss3\_base\_score>7.8</cvss3\_base\_score> <cvss3\_overall\_score>6.8</cvss3\_overall\_score> <cvss3\_vector>CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</cvss3\_vector> <custom\_cvss3\_overall\_score>5.9</custom\_cvss3\_overall\_score>

#### **In Email Notifications**

Emails contain CVSSv2 (displayed as CVSS) and CVSSv3 (displayed as CVSS3) labels. The CVSSv3 value will be empty until a v3 value is entered, at which time the v2 (CVSS) value will be empty.

Criticality	Moderately critical
Release Date	09/12/2020
Last Update	09/12/2020
Solution Status	Vendor Patched
SAID	<u>SA99320</u>
CVSS	0.0 (AV:N/AC:L/E:U/RL:OF/RC:C)
CVSS3	9.0 CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C
Impact	DoS, Privilege escalation, Exposure of sensitive information, Security Bypass
Where	From local network
Threat Score	2 (Last Updated 2020-12-09)

#### **In a PDF Report**

PDF reports containing CVSS values will show CVSSv2 (displayed as CVSS) or CVSSv3 (displayed as CVSS3) as appropriate.

Criticality	- Moderately critical
Impact	System access
Where	From remote
Solution Status	Vendor Patched
Secunia CVSS Scores	CVSS3 Base: 7.8 , Overall: 6.8 CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

# **CVE References**

A CVE (Common Vulnerabilities and Exposures) name represents a unique, standardized name and description for a given vulnerability or exposure.

Searching on a CVE reference (for example CVE-2009-3793 or simply 2009-3793) will find all Secunia Advisories in the database that list that particular CVE as a reference.

Res	earch > A	Advisory Datal	base > A	dvisories											<u>ب</u>
A	dvisory I	Database 👻	Pro	ducts Da	tabas	e 🕶									
rov	wsing 16 a	dvisories 🧃							Q Sea	rch by keywo	rd				Y
3	Zero Day		•	Impact		•	CVE-2020-949	SAID	From			То		Criticality	
	Solution s	▼ Where	•	CVSS Score	еM	CVSS Score M	Threat Score I	Threat Score I	Advisory ty	pe	•			Apply	Reset
												Filter	•	Save	Delet
_	SAID	Release	Modifi	ied 💠	Title				Criticality 🖨	Zero Day	Solution status	Where	CVSS Score	Threat Score	Type
ב	<u>SA97626</u>	2020-09-21	2020-0	9-21	Amazoi	n Linux update for	httpd			No	Vendor Patched	From remo	te 9.8 v3	19	Secunia Advisory
								View Advisory	Create ti	cket					
]	<u>SA97650</u>	2020-09-19	2020-0	9-19	Amazoi	n Linux update for	mod_http2			No	Vendor Patched	From remo	te 7.5 v3	18	Secunia Advisory
]	<u>SA97718</u>	2020-09-17	2020-0	9-17	Oracle	Solaris Apache H	TTP Server Multiple	e Vulnerabilities	_	No	Vendor Patched	From remo	te 9.8 v3	18	Secunia Advisory
]	<u>SA97717</u>	2020-09-17	2020-0	9-17	Oracle Vulnera	Solaris Multiple T ibilities	hird Party Compon	ents Multiple		No	Vendor Patched	From remo	te 9.8 v3	23	Secunia Advisory
	<u>SA97533</u>	2020-09-15	2020-0	9-15	Red Ha	t update for httpd	24-httpd		_	No	Vendor Patched	From remo	te 7.5 v3	17	Secunia Advisory
	<u>SA97677</u>	2020-09-11	2020-0	9-11	Red Ha	t update for httpd	2.4			No	Vendor Patched	From remo	te 7.5 v3	17	Secunia Advisory
]	<u>SA97611</u>	2020-09-11	2020-0	9-11	IBM I A	pache HTTP Serv	er Denial of Service	e Vulnerability		No	Vendor Patched	From remo	te 7.5 v3	17	Secunia Advisory
	<u>SA97319</u>	2020-09-03	2020-0	9-03	SUSE (	pdate for apache	2			No	Vendor Patched	From remo	te 7.5 v3	19	Secunia Advisory

An Advisory can contain more than one CVE reference, and not every Advisory has an associated CVE reference.

×

#### Amazon Linux update for httpd - CVE

CVE	CVSS*	Threat Score	Threat Reason					
CVE-2020-9490	CVSS v2: 5.0 (AV:NAC:L/Au:N/C:N/I:N/A:P) CVSS v3: 7.5 CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	17	Linked to Historical Cyber Exploit Historically Linked to Penetration Testing Tools Recently Linked to Penetration Testing Tools					
Description* Apache HTTP Ser HTTP/2 PUSH a re	Description' Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.							
Threat Intel Mod The CVE threat so • Linked to I • Historically • Recently L	Threat Intel Module The CVE threat score of 17 was based on the following triggers: Linked to Historical Cyber Exploit Historically Linked to Penetration Testing Tools Recently Linked to Penetration Testing Tools							
The threat score v	as last updated on 2020-09-20.							
References*								
SUSE	http://lists.opensuse.org/opensuse-security-announce/2020-08/msg00071.	<u>ntml</u>						
Other Reference	https://lists.apache.org/thread.html/r5debe8t82/28a00a4a68bc904dd6c354/	3001080601010457	<u>9138bri@%3Cdev.nttpd.apacne.org%3E</u>					
Other Reference	https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2020-9490	505-0-0600h 474	040-74@#20desthemd another applied					
Other Reference	https://lists.apache.org/thread.html/r99911a/609/6010180662eaaec2aa3c320	1525C3e01Ca98D4/	2240271@%3Cdev.httpd.apache.org%3E					
Other Relefence	http://lists.apache.org/thread.html/r625de9b2b2455a8/1515a15900419109c0	10C7702693601Ea40	Jours 7 200%3 Cole V. https://apache.org%3E					
Eedora	http://lists.opensuse.org/opensuse-security-announce/2020-08/lists.fedor	num						
Gentoo	https://ists.redoi.aproject.org/archives/ist/package-announce@iists.redoi	aproject.org/mess						
Debian	https://www.debian.org/security/2020/dsa.4757							
Eedora	nttps://www.debian.org/security/zuzurdsa-4/3/							
Other Reference								
Ubuntu	https://usn.ubuntu.com/4458-1/							
CVE-2020-11993	CVSS v2: 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)	2	Linked to Historical Cyber Exploit					
CVE-2020-11984	CVSS v2: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)	2	Linked to Historical Cyber Exploit					

#### NOTE:

\* The information is written and maintained by CVE MITRE.

The data on this page reflects neither the opinions of Secunia or the results of our research.

Back

# Where (Attack Vector)

The following are Where (Attack Vector) values.

#### **Local System**

Local system describes vulnerabilities where the attack vector requires that the attacker is a local user on the system.

#### **Local Network**

From local network describes vulnerabilities where the attack vector requires that an attacker is situated on the same network as a vulnerable system (not necessarily a LAN).

This category covers vulnerabilities in certain services (for example, DHCP, RPC, administrative services, and so on), which should not be accessible from the Internet, but only from a local network and optionally a restricted set of external systems.

#### Remote

From remote describes vulnerabilities where the attack vector does not require access to the system nor a local network.

This category covers services, which are acceptable to expose to the Internet (for example, HTTP, HTTPS, SMTP) as well as client applications used on the Internet and certain vulnerabilities, where it is reasonable to assume that a security conscious user can be tricked into performing certain actions.

# **Criticality (Severity Rating)**

The following are Severity Rating values.

#### **Extremely Critical**

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

#### **Highly Critical**

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

#### **Moderately Critical**

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

This rating is also used for vulnerabilities allowing system compromise on LANs in services like SMB, RPC, NFS, LPD and similar services that are not intended for use over the Internet.

#### **Less Critical**

This value is typically used for cross-site scripting and local privilege escalation vulnerabilities.

This rating is also used for vulnerabilities allowing exposure of sensitive data to local users.

#### **Not Critical**

This value is typically used for very limited privilege escalation vulnerabilities and locally exploitable Denial of Service vulnerabilities.

This rating is also used for non-sensitive system information disclosure vulnerabilities (for example, remote disclosure of installation path of applications).

# Impact (Consequence)

The following are Consequence values.

#### **Brute Force**

Used in cases where an application or an algorithm allows an attacker to guess passwords in an easy manner.

#### **Cross-Site Scripting**

Cross-Site Scripting vulnerabilities allow a third party to manipulate the content or behavior of a web application in a user's browser, without compromising the underlying system.

Different Cross-Site Scripting related vulnerabilities are also classified under this category, including "script insertion" and "cross-site request forgery".

Cross-Site Scripting vulnerabilities are often used against specific users of a website to steal their credentials or to conduct spoofing attacks.

#### **DoS (Denial of Service)**

This includes vulnerabilities ranging from excessive resource consumption (for example, causing a system to use a lot of memory) to crashing an application or an entire system.

#### **Exposure of Sensitive Information**

Vulnerabilities where documents or credentials are leaked or can be revealed either locally or remotely.

#### **Exposure of System Information**

Vulnerabilities where excessive information about the system (for example. version numbers, running services, installation paths, and similar) are exposed and can be revealed from remote and, in some cases, locally.

#### Hijacking

Covers vulnerabilities where a user session or a communication channel can be taken over by other users or remote attackers.

#### **Manipulation of Data**

This includes vulnerabilities where a user or a remote attacker can manipulate local data on a system, but not necessarily be able to gain escalated privileges or system access.

The most frequent type of vulnerabilities with this impact are SQL-injection vulnerabilities, where a malicious user or person can manipulate SQL queries.

#### **Privilege Escalation**

Covers vulnerabilities where a user is able to conduct certain tasks with the privileges of other users or administrative users.

This typically includes cases where a local user on a client or server system can gain access to the administrator or root account, thus taking full control of the system.

#### **Security Bypass**

Covers vulnerabilities or security issues where malicious users or people can bypass certain security mechanisms of the application. The actual impact varies significantly depending on the design and purpose of the affected application.

#### Spoofing

Covers various vulnerabilities where it is possible for malicious users or people to impersonate other users or systems.

#### **System Access**

Covers vulnerabilities where malicious people are able to gain system access and execute arbitrary code with the privileges of a local user.

#### Unknown

Covers various weaknesses, security issues, and vulnerabilities not covered by the other impact types, or where the impact is not known due to insufficient information from vendors and researchers.



# **Appendix A - Threat Intelligence**

Software Vulnerability Research Threat Intelligence directs your attention towards the vulnerabilities affecting your watch lists.

In a world where there are more than 18,000 new vulnerabilities every year, being smart about prioritizing remediation efforts is essential. Leveraging our optional Threat Intelligence Module, another valuable layer of insight is provided to help you understand which of the vulnerabilities affecting your environment are actually being exploited in the wild.

Industry reports, including Gartner shows that between 6%-10% of the vulnerabilities disclosed each year actually are exploited in the wild. Turns out that most of these have medium CVSS scores, which are typically overlooked by organizations. With the insights provided by threat intelligence, it is possible better optimize the time spent remediating software vulnerabilities. Avoid spending time and resources in patching vulnerabilities that do not have evidence of exploitation, and favor those that do. Prioritization is crucial for effective risk mitigation and resource utilization.

Leveraging machine learning, artificial intelligence, and human curation from thousands of sources in the open, deep and dark web, our Threat Intelligence Module augments Software Vulnerability Research's vulnerability intelligence with a Threat Score that provides the ultimate prioritization tool for your busy desktop operations teams.

This appendix explains how the Software Vulnerability Research Threat Intelligence module helps the enterprises to manage their resources and Patching Vulnerabilities more effectively, the following topics are discussed in this section:

- Evidence of Exploitation
- Criteria for the Threat Score Calculation
- Threat Score Calculation Examples
- Threat Intelligence Data for Operations and Security
- Threat Intelligence for Research



**Note** • Please note the following:

- Secunia Advisory Threat Scores and Vulnerability (CVE) Threat Scores are each calculated as described in the Criteria for the Threat Score Calculation section (an Advisory score is not determined by simply adding related CVE Threat Scores).
- For pricing and availability, please contact your sales representative or contact us online at: https://www.flexera.com/about-us/contact-us.html

• For more details about the Threat Intelligence Modules, see our datasheet: https://www.flexera.com/media/pdfs/datasheet-svm-threat-intelligence-module.pdf

# **Evidence of Exploitation**

There are 10 primary rules that can impact the assigned Threat score and they are:

- It has been linked to remote access Trojan
- It has been linked to ransomware
- It has been linked to penetration testing tools
- It has been linked to malware
- It has been linked to an exploit kit
- It has been linked to a cyber exploit
- It has been linked to an exploit wild
- It has been linked to POC verified
- It has been linked to vulnerability developed tools
- It has been linked to verified intelligence

# **Criteria for the Threat Score Calculation**

Triggered rules increase the score by the values identified in the chart below based on the highest severity level triggered.

Table A-1 • Rules, Severity and Value

Rule	Severity	Value
Recently Linked to Remote Access Trojan	Medium	+2
Historically Linked to Remote Access Trojan	Low	+1
Recently Linked to Ransomware	Medium	+2
Historically Linked to Ransomware	Low	+1
Recently Linked to Penetration Testing Tools	Medium	+2
Historically Linked to Penetration Testing Tools	Low	+1
Recently Linked to Malware	Medium	+2
Historically Linked to Malware	Low	+1
Recently Linked to Exploit Kit	Medium	+2

#### Table A-1 • Rules, Severity and Value

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

The rule with the highest criticality determines the point range and the starting value for the Threat Score. The ranges for each are as follows:

#### Table A-2 • Criticality - Ranges

Criticality	From	То
Very Critical	71	99
Critical	45	70
High	24	44
Medium	13	23
Low	1	12

#### Table A-2 • Criticality - Ranges

Criticality	From	То
None	0	0

**Note** • when assigning a Threat Score to the SAID, we do not simply add up the scores for each associated vulnerability, but rather follow the same rules outlined here to calculate the Security Advisory threat score.

# **Threat Score Calculation - Examples**

Some examples to explain how we would arrive at a Threat Score.

#### Example 1

A SAID has two CVEs; two come back as exploited.

#### **Triggered Rules**

The following rules are triggered:

- CVE1 triggers
  - Historically Linked to Remote Access Trojan
  - Recent remote code execution POC verified
- CVE2 triggers
  - Historically Linked to Exploit Kit

The Threat Score would be 51.

#### **Calculating the Score**

The criticality range is set by the most critical rule triggered, which is critical. This sets the score's maximum and minimum range as between 45 and 70.

Item	Value
Base Score	+45
Recent remote code execution POC verified	+4
Linked to Recent Cyber Exploit	+1
Historically Linked to Remote Access Trojan	+1
Threat Score (Sum of above values)	51

#### **Example 2**

A SAID has seven CVEs; and all come back as exploited.

#### **Triggered Rules**

The following rule is triggered by all CVEs:

- CVE1, CVE2, CVE3, CVE4, CVE5, CVE6 and CVE7 triggers
  - Recently Linked to Malware

The Threat Score would be 23.

#### **Calculating the Score**

The criticality range is set by the most critical rule triggered, which is critical. This sets the score's maximum and minimum range as between 13 and 23.

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

#### **Example 3**

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

#### **Triggered Rules**

The following rule is triggered:

- CVE1 triggers
  - Historically exploited in the wild

The Threat Score would be 27.

#### **Calculating the Score**

The criticality range is set by the most critical rule triggered, which is high. This sets the score's maximum and minimum range as between 24 and 44.

Item	Value
Base Score	+24

Item	Value
Historically exploited in the wild	+3
Threat Score (Sum of above values)	27

#### **Example 4**

A SAID has many CVEs, none come back as exploited.

The score would be **0** because there are no rules triggered.

#### **Advisory with Multiple Vulnerabilities**

An advisory Threat Score is based upon each of the CVEs included in an Advisory as specified above. In Software Vulnerability Research, the vulnerabilities that have exploits are indicated with a red circle for easier identification.

# Threat Intelligence Data for Operations and Security

Software Vulnerability Research and Software Vulnerability Research cater to different audiences with different needs. Software Vulnerability Research (for operations) provides what is needed for Operations to better prioritize remediation efforts. Whereas Software Vulnerability Research (for security) provides more detail to meet the needs of security teams.

Table A-3 • Software Vulnerability Manager vs. Software Vulnerability Research

Software Vulnerability Manager	Software Vulnerability Research		
Offers a Threat Score at the Advisory level	Offers a Threat Score at the Advisory level		
	• Offers a Threat Score at the vulnerability level, within the advisory		
	• Offers a list of which rules were triggered to arrive at the Threat Score displayed		

# **Threat Intelligence for Research**

The user who purchased the Software Vulnerability Research Threat Intelligence Module, can see the threat intelligence add on feature in the following places:

- Dashboard > Dashboard with Threat Intelligence Module
- Research > Advisories > Advisories with Threat Score
- Analytics > Advisories > Advisories by Threat Score