



# **SOAR-TVM Module**

## **Rapid7 Nexpose Integration Guide**

Document Version: 2017.11.15 | November 2017

Rsam © 2017. All rights reserved

[Privacy Policy](#) | [Terms of Service](#)

# Contents

- Overview ..... 3
- Getting Rapid7 Nexpose Data into Rsam ..... 4
  - Importing Data from Rapid7 Nexpose Security Console ..... 4
  - Importing Data Using a Nexpose XML File ..... 7
  - Manage Import Maps ..... 10
- Appendix: Predefined Import Maps ..... 11
  - V:NEXPOSE\_XML (V.3) - Tests ..... 11
  - V:NEXPOSE\_XML (V.3) - Services ..... 13
- Appendix: Rsam Documentation ..... 15
  - Inline Help ..... 15

## Overview

---

Rsam's Security Operations Analytics Reporting-Threat and Vulnerability Management solution (SOAR-TVM) provides an integrated approach to manage a broad spectrum of risks across the enterprise. Integrating Nexpose with Rsam allows you to import asset and vulnerability data into one centralized location that can be supplemented with information from other data sources used across the organization. The aggregation of this data gives context to your vulnerability and compliance results, driving prioritization of risk mitigation efforts and provides deeper insights and a simplified way of reporting on overall organizational risk.

# Getting Rapid7 Nexpose Data into Rsam

The guide outlines the steps to import the Rapid7 Nexpose data using the API or an XML report downloaded from Nexpose Security Console and is broken into the following sections. The following methods allow you to get the Rapid7 Nexpose data into Rsam:

- **Import from Nexpose using Nexpose Security Console** – Imports vulnerabilities using the audit report template. The Nexpose Security Console API uses the defined Nexpose audit template to generate the vulnerability report to be imported into Rsam. The user cannot select a different Nexpose report template using this API.
- **Import from Nexpose using Nexpose Security Console v2** – Imports assets or vulnerabilities using any XML or CSV report created in your Nexpose console. This allows customers to use any Nexpose XML template, custom XML template or SQL query to define which data elements will be available for import.

This also provides you the ability to define report filters within the Nexpose report itself, rather than using the filter in Rsam’s Import to filter the data during import. Rsam recommends filtering the data at the data source to optimize the import performance.

- **Import using a Nexpose XML Report File** – Imports assets and vulnerabilities using the report template exported from the Nexpose console.

## Importing Data from Rapid7 Nexpose Security Console

To import Nexpose asset or vulnerability data into Rsam, perform the following steps:

1. Log in to Rsam as administrator and navigate to **Records > Import Records**.
2. Select **New** from the **Import Profile** drop-down list. A profile can be saved and scheduled to import vulnerabilities at regular intervals.

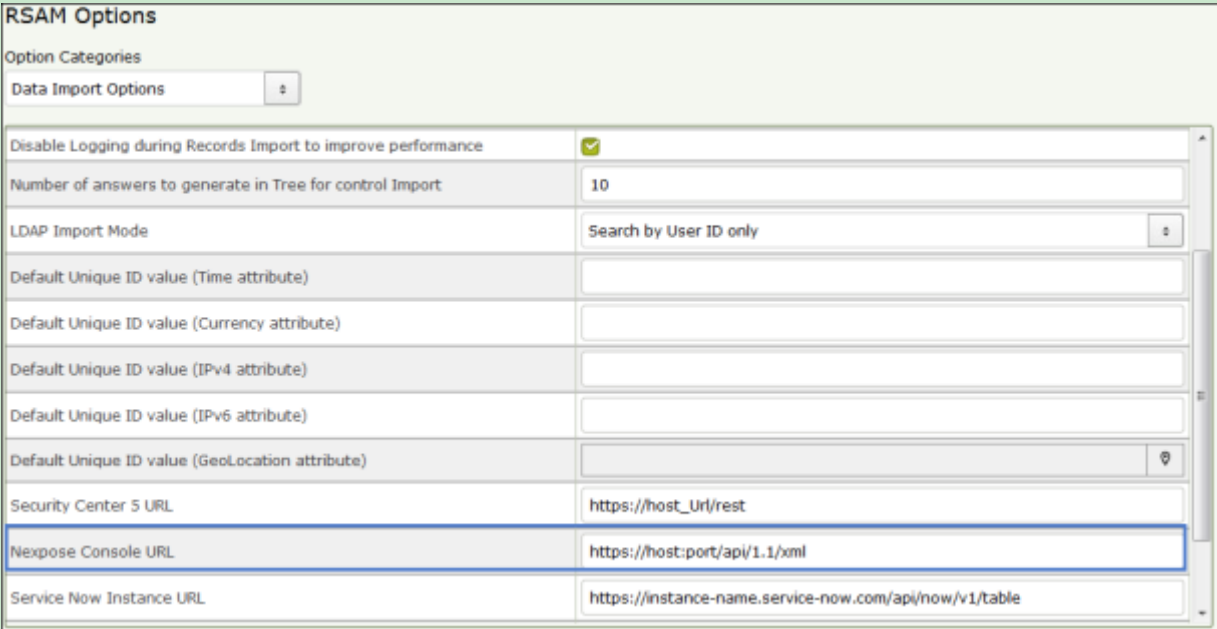


The image shows a screenshot of a web interface element labeled "Import Profile:". It consists of a rectangular box with a light gray border. Inside the box, there is a white text input field that is currently empty. To the right of the input field is a small, square button with a downward-pointing arrow, indicating a dropdown menu.

3. Select **Nexpose Security Console** or **Nexpose Security Console v2** from the **Source** drop-down list.

4. Update the **Nexpose Security Console URL** with the hostname and port number of your Nexpose console. The remainder of the URL must not be altered.

**Note:** The Nexpose Console URL can be pre-populated by specifying it in the Data Import Options category of RSAM Options available in the Administration module.



RSAM Options	
Option Categories	
Data Import Options	
Disable Logging during Records Import to improve performance	<input checked="" type="checkbox"/>
Number of answers to generate in Tree for control Import	10
LDAP Import Mode	Search by User ID only
Default Unique ID value (Time attribute)	
Default Unique ID value (Currency attribute)	
Default Unique ID value (IPv4 attribute)	
Default Unique ID value (IPv6 attribute)	
Default Unique ID value (GeoLocation attribute)	
Security Center 5 URL	https://host_url/rest
<b>Nexpose Console URL</b>	<b>https://host:port/api/1.1/xml</b>
Service Now Instance URL	https://instance-name.service-now.com/api/now/v1/table

5. Enter an **User ID** for the console.
6. Enter **Password** for the User ID.
7. Complete the fields based on the source selected:

- **Nexpose Security Console**

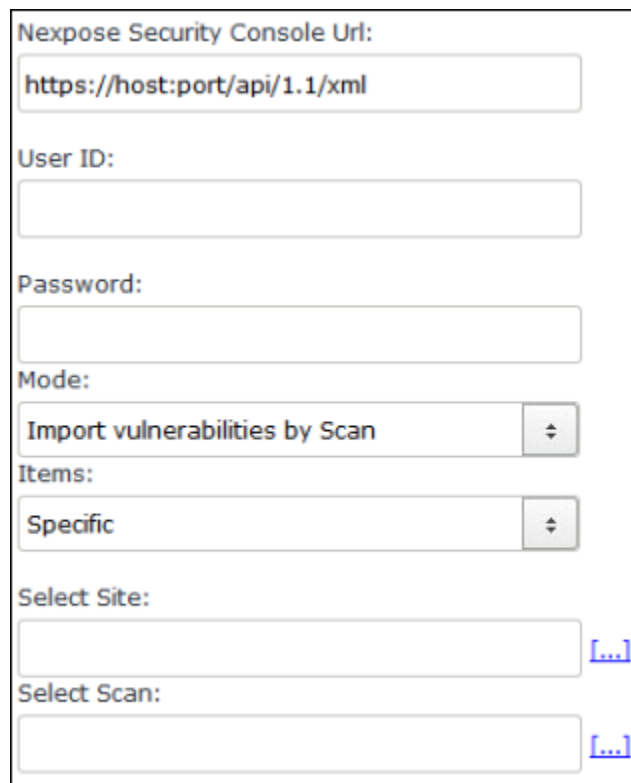
- a. Select any of the following import modes from the **Mode** drop-down list:

- **Import Vulnerabilities by Scan** - Imports vulnerabilities found in that scan.
- **Import Vulnerabilities by Asset Group** - Imports all current vulnerabilities for the selected asset group.
- **Import Vulnerabilities by Site** - Imports all current vulnerabilities for the selected site.

- **Import Vulnerabilities by Asset** - Imports all current vulnerabilities for the selected asset.

**Note:** The fields mentioned below appear or disappear based on the mode.

- Select **Specific** or **Last** from the **Items** drop-down list.
- Click [\[...\]](#) associated with the **Select Site** field and select a desired site to import all current vulnerabilities.
- Click [\[...\]](#) associated with the **Select Asset** field and select a desired asset to import all current vulnerabilities.
- Click [\[...\]](#) associated with the **Select Scan** field and select a desired scan.
- Click [\[...\]](#) associated with the **Select Asset Group** field and select a desired asset group.



The screenshot shows a configuration form for the Nexpose Security Console. It includes the following fields and controls:

- Nexpose Security Console Url:** A text input field containing the URL `https://host:port/api/1.1/xml`.
- User ID:** An empty text input field.
- Password:** An empty text input field.
- Mode:** A dropdown menu currently set to **Import vulnerabilities by Scan**.
- Items:** A dropdown menu currently set to **Specific**.
- Select Site:** An empty text input field with a blue [\[...\]](#) link to its right.
- Select Scan:** An empty text input field with a blue [\[...\]](#) link to its right.

- **Nexpose Security Console V2**

Click the [\[...\]](#) icon associated with the **Select Report** field and select any of the available report. Here, all XML and CSV reports that have been generated will be available for selection.

LIST OF REPORTS FOR USER TO SELECT		
Report Name	Report Status	Report Generation Date
audit report	Generated	04/14/2016 18:32:14
Nexpose Supplemental Data	Generated	03/11/2016 09:30:03
Vuln Report	Generated	12/31/2015 13:18:08
Workstation Query	Generated	03/11/2016 09:29:01
Workstation Query-Copy	Unknown	
XML2.0	Generated	04/14/2016 18:33:38

- Click **Import Now**. The vulnerabilities are imported.

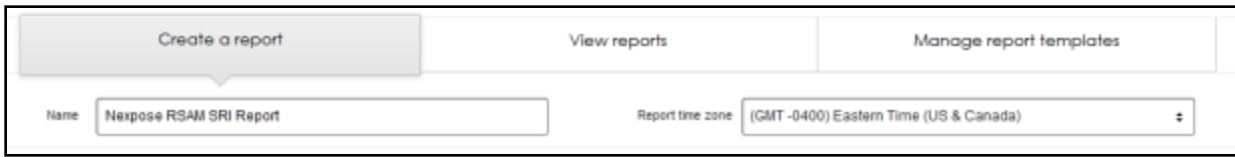
## Importing Data Using a Nexpose XML File

To import data using a Nexpose XML file, perform the following steps:

- Log in to the Nexpose web console.



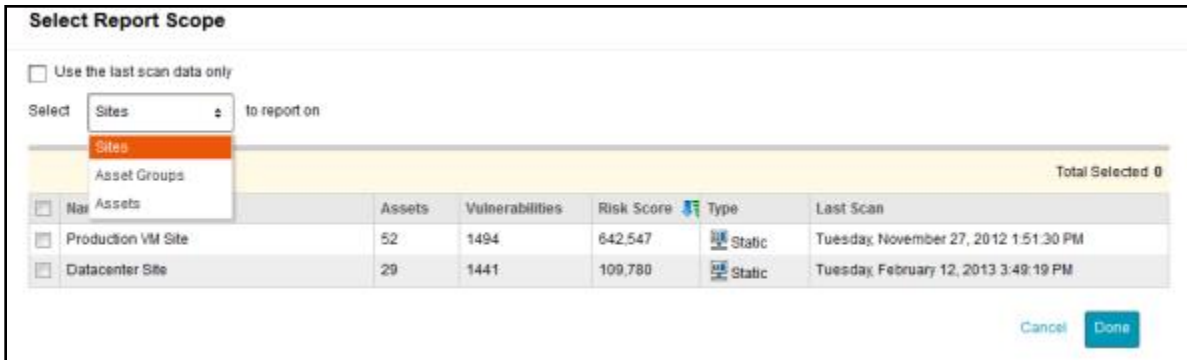
- From the menu bar, click **Reports**.
- Click **Create a report**.
- Specify a report name in the **Name** field.



5. Under the **Template** section, select the **Export** filter.
6. Slide through the report templates horizontally and locate the 'XML Export 2.0" report, and then select it. The report template is marked as **Selected**.



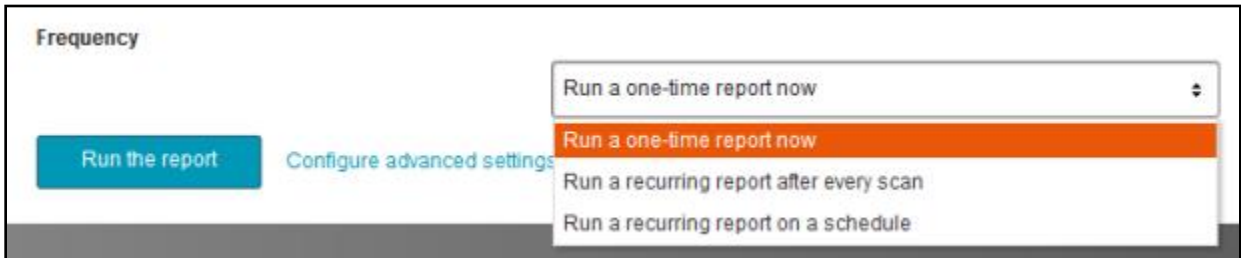
7. Under the **Scope** section, select **Select Sites, Assets or Asset Groups**.
8. Under the **Select Report Scope** section, select **Sites, Asset Groups, or Assets** to report



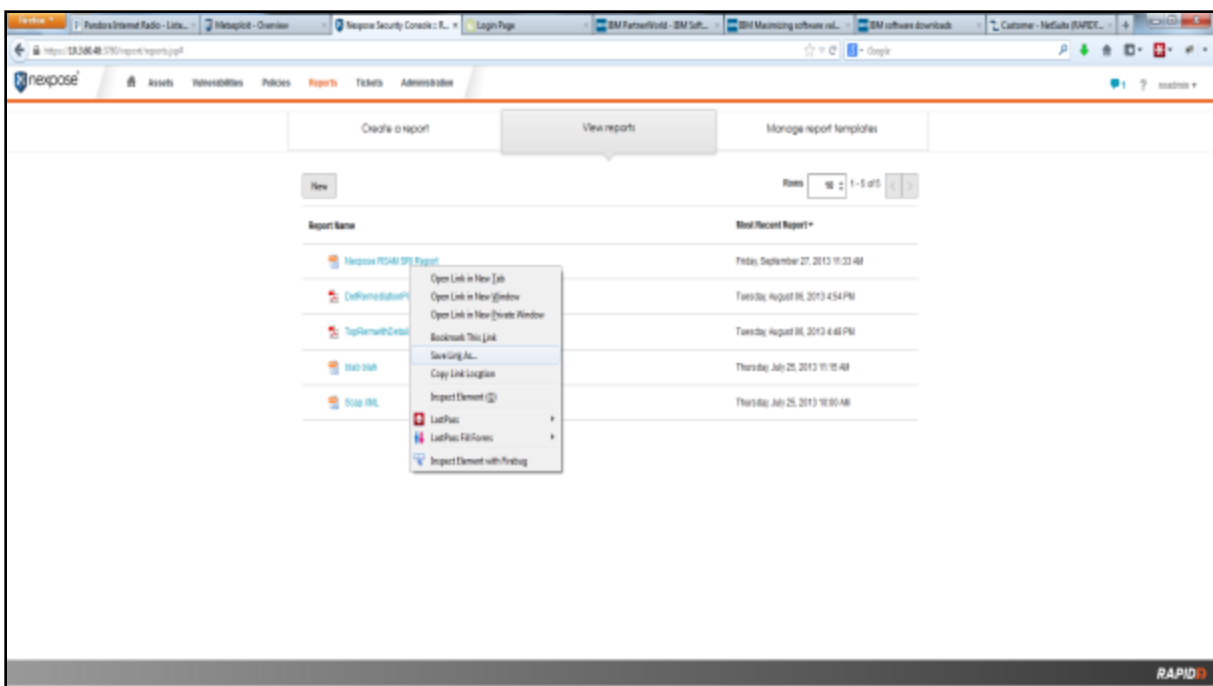
9. From the **Select Report Scope** option, select the appropriate filter to view either Sites, Asset Groups, or Assets.
10. Click **Done** when complete.



11. Under the **Frequency** section, select the desired frequency at which you want to generate the report. As part of this document, we will run the report once, so, we will select **Run a one-time report now**.
12. Click the **Run the Report** button.



13. Click **View reports**.
14. Right-click on the report name and select **Save Link As** from the context menu.



15. Click the option that will allow you to save the report file.
16. Log in to Rsam as administrator and navigate to **Records > Import Records**.
17. Select **XML** from the Source and complete all the necessary fields.

**Notes:**

1. If you are importing from file share, make sure the file is listed with the full UNC path.
2. If you are importing more than one file, set the File Mask to .\*extension.

## Manage Import Maps

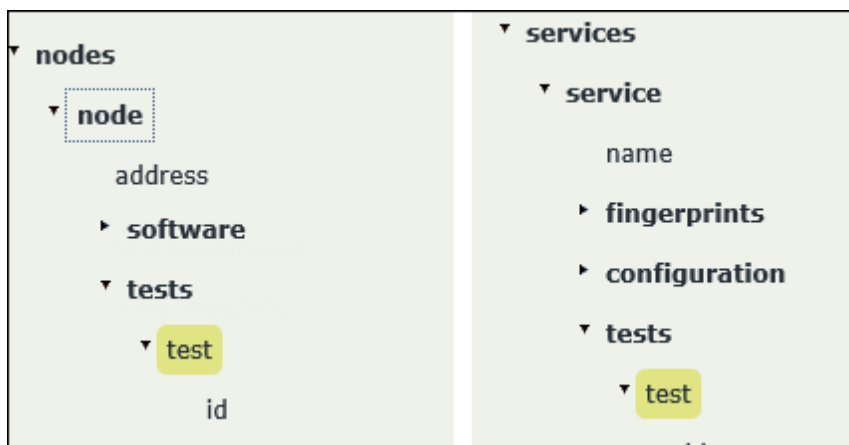
Refer to the [Appendix: Predefined Import Maps](#) section for the list of predefined maps available for each import mode listed above.

Refer to the document titled *Supplemental Integration Guide – Managing TVM Import Mappings* for more information on reviewing and updating the predefined maps.

## Appendix: Predefined Import Maps

This section describes import maps used for Nexpose integration. Note that reports created using the "XML Export 2.0" template available in Nexpose breaks out vulnerabilities associated with running services into a different section of the XML report. The following import maps are available in Rsam to help you import the applicable set of vulnerabilities.

- Nexpose\_XML (v.3) - Tests
- Nexpose\_XML (v.3) - Services



### V:NEXPOSE\_XML (V.3) - Tests

This map imports vulnerabilities and misconfigurations associated with the operating system. This map uses the following two export filters: Vulnerable-Version & vulnerable-exploited.

Rsam Attribute	Path
Host Architecture	node/fingerprints/os/arch
Host OS Certainty	node/fingerprints/os/certainty
Host Device Class	node/fingerprints/os/device-class
Host Family	node/fingerprints/os/family
Host OS	node/fingerprints/os/product
Host Vendor	node/fingerprints/os/vendor

<b>Rsam Attribute</b>	<b>Path</b>
<b>Host Version</b>	node/fingerprints/os/version
<b>Host IP Address</b>	nodes/node/address
<b>Host MAC address</b>	nodes/node/hardware-address
<b>Host Name - NetBIOS</b>	nodes/node/names/name
<b>Host Status</b>	nodes/node/status
<b>Scan End Time</b>	scans/scan/endTime
<b>Scan ID</b>	scans/scan/id
<b>Scan Name</b>	scans/scan/name
<b>Scan Start Time</b>	scans/scan/startTime
<b>Vulnerability ID</b>	nodes/node/tests/test/
<b>Vulnerability Name</b>	vulnerabilityDefinitions/vulnerability/title
<b>Description</b>	vulnerabilityDefinitions/vulnerability/description
<b>Fix/Resolution</b>	VulnerabilityDefinitions/vulnerability/solution
<b>Severity - Native (numeric)</b>	VulnerabilityDefinitions/vulnerability/severity
<b>Severity - PCI</b>	vulnerabilityDefinitions/vulnerability/pciSeverity
<b>Published</b>	vulnerabilityDefinitions/vulnerability/published
<b>Reference - General</b>	VulnerabilityDefinitions/vulnerability/references
<b>CVSS: Base Score</b>	vulnerabilityDefinitions/vulnerability/CVSSscore
<b>CVSS: Vector Summary</b>	vulnerabilityDefinitions/vulnerability/cvssVector
<b>Tags</b>	vulnerabilityDefinitions/vulnerability/tags

## V:NEXPOSE\_XML (V.3) - Services

This map imports vulnerabilities associated with services running on the host. This map uses the following two export filters: Vulnerable-Version and vulnerable-exploited.

Rsam Attribute	Type
<b>Host Architecture</b>	node/fingerprints/os/arch
<b>Host OS Certainty</b>	node/fingerprints/os/certainty
<b>Host Device Class</b>	node/fingerprints/os/device-class
<b>Host Family</b>	node/fingerprints/os/family
<b>Host OS</b>	node/fingerprints/os/product
<b>Host Vendor</b>	node/fingerprints/os/vendor
<b>Host Version</b>	node/fingerprints/os/version
<b>Host IP Address</b>	nodes/node/address
<b>Host MAC address</b>	nodes/node/hardware-address
<b>Host Name - NetBIOS</b>	nodes/node/names/name
<b>Host Status</b>	nodes/node/status
<b>Scan End Time</b>	scans/scan/endTime
<b>Scan ID</b>	scans/scan/id
<b>Scan Name</b>	scans/scan/name
<b>Scan Start Time</b>	scans/scan/startTime
<b>Vulnerability ID</b>	nodes/node/endpoints/endpoint/services/service/tests/test/
<b>Vulnerability Name</b>	vulnerabilityDefinitions/vulnerability/title
<b>Description</b>	vulnerabilityDefinitions/vulnerability/description
<b>Fix/Resolution</b>	VulnerabilityDefinitions/vulnerability/solution

<b>Rsam Attribute</b>	<b>Type</b>
<b>Severity - Native (numeric)</b>	VulnerabilityDefinitions/vulnerability/severity
<b>Severity - PCI</b>	vulnerabilityDefinitions/vulnerability/pciSeverity
<b>Published</b>	vulnerabilityDefinitions/vulnerability/published
<b>Reference - General</b>	VulnerabilityDefinitions/vulnerability/references
<b>CVSS: Base Score</b>	vulnerabilityDefinitions/vulnerability/CVSSscore
<b>CVSS: Vector Summary</b>	vulnerabilityDefinitions/vulnerability/cvssVector
<b>Tags</b>	vulnerabilityDefinitions/vulnerability/tags

# Appendix: Rsam Documentation

## Inline Help

To get familiar with the specific Rsam features used in this configuration, refer the Rsam Help, Rsam Administrator Help, or both. The Online help you can access depends on your user permissions.

### Procedure:

1. Sign in to your Rsam instance. For example, sign in as **Example Administrator** user. Enter **Username** as **r\_admin** and **Password** as **password**.
2. Mouse hover over **Help** and select an Online help in the menu that appears. Depending on your user permissions, you will be able to access the Rsam Help, Rsam Administrator Help, or both.

The following image shows the Rsam Administrator Help, opened from the **Example Administrator** user account.

