



SOAR-TVM Module

Tenable Security Center Integration Guide

Document Version: 2017.11.22 | November 2017

Rsam © 2017. All rights reserved

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

Contents

| | |
|--|----|
| Overview | 3 |
| Getting Tenable Security Center Data into Rsam | 4 |
| Import Vulnerabilities | 4 |
| Import Assets..... | 7 |
| Manage Import Maps..... | 9 |
| Appendix: Pre-Defined Import Maps | 10 |
| TENABLE_SECURITY_CENTER5_API (V.1 - SCAN BASED)..... | 10 |
| TENABLE_SECURITY_CENTER5_API (V.1 - CUMULATIVE)..... | 12 |
| TENABLE_SECURITY_CENTER5_ASSET_API (V.1)..... | 13 |
| Appendix: Rsam Documentation | 15 |
| Inline Help | 15 |

Overview

Rsam's Security Operations Analytics Reporting-Threat and Vulnerability Management (SOAR-TVM) solution provides an integrated approach to manage a broad spectrum of risks across the enterprise. The integration of Tenable Security Center v5 with Rsam SOAR-TVM provides you with deeper insight into their overall organizational risk based on the vulnerabilities on their assets. With the information centralized in one location, it is very simple and easy to report on overall risk mitigation efforts.

Rsam provides a direct connection to your Tenable Security Center v5 console, allowing you to import asset information and all scan results—passed and failed—from specific scans or cumulatively import open vulnerabilities across all scans. Alternatively, you can download CSV or a Tenable .NESSUS file from Security Center v5 and import the data manually into Rsam SOAR-TVM. Each variation of Security Center output provides a slightly different XML structure, and Rsam provides mappings for each format.

Getting Tenable Security Center Data into Rsam

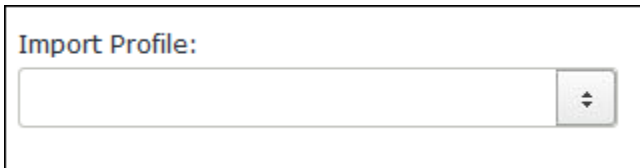
This document will guide you through the steps necessary to configure Rsam SOAR-TVM to successfully import data from Tenable Security Center 5 (SC5). The following methods are available to get the Tenable Security Center data:

- Security Center vulnerabilities via API – Scan-Based
- Security Center vulnerabilities via API – Cumulative
- Security Center Assets

Import Vulnerabilities

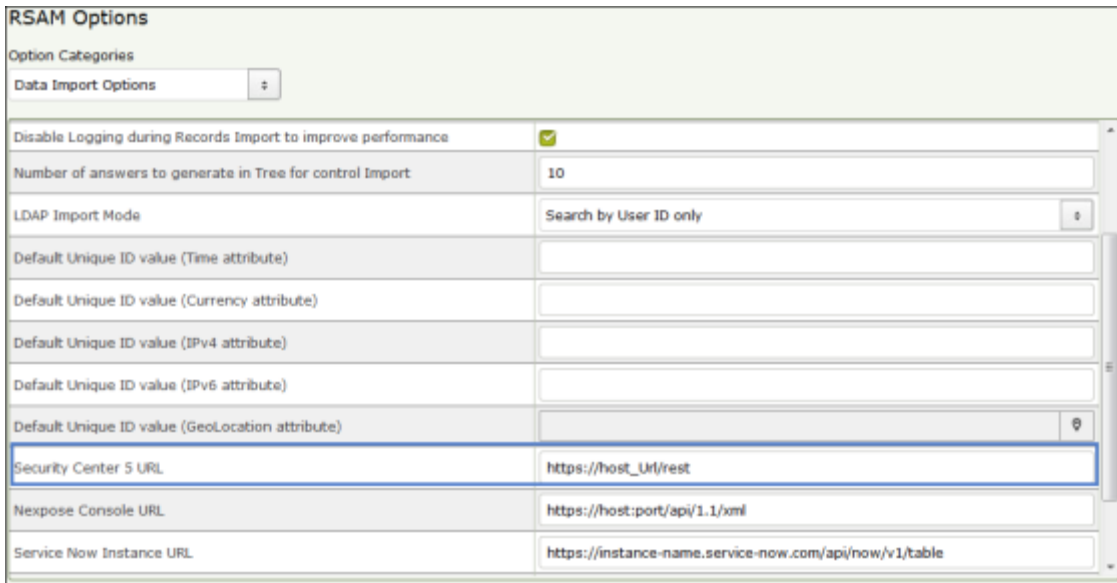
Perform the following steps to import vulnerabilities:

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.

A screenshot of a web form element. It features a label 'Import Profile:' in blue text above a white rectangular input field. To the right of the input field is a small grey button with a downward-pointing arrow, indicating a dropdown menu.

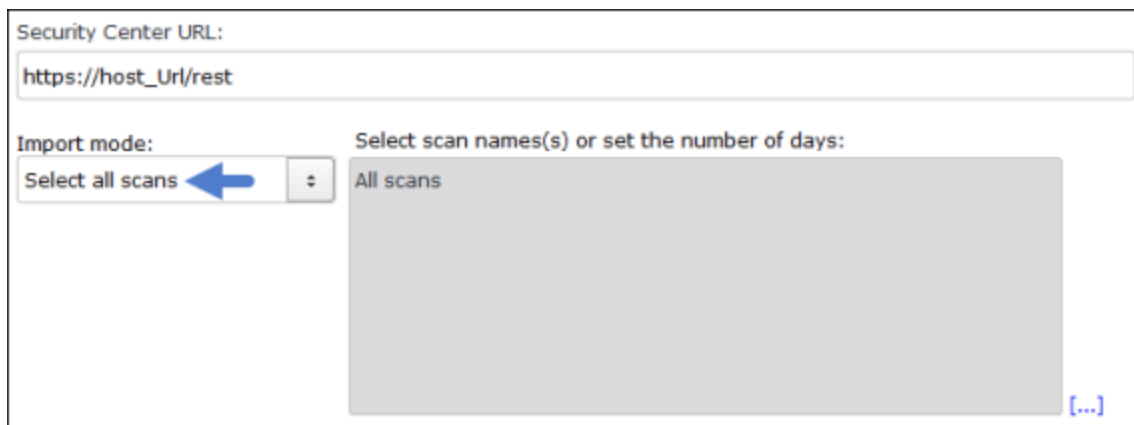
3. Select **Tenable Security Center 5** from the **Source** drop-down list.

Note: The Security Center URL can be pre-populated by specifying it in the **Data Import Options** category of RSAM Options available in the Administration module. Be sure to enter **/rest** after the URL.



| 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 S URL | https://host_url/rest |
| Nexpose Console URL | https://host:port/api/1.1/xml |
| Service Now Instance URL | https://instance-name.service-now.com/api/now/v1/table |

4. Enter an **User ID** for the console.
5. Enter **Password** for the User ID.
6. Enter **Security Center URL**. Be sure to enter `/rest` after the URL.
7. Select any of the following mode to import vulnerabilities.
 - **Select All Scans** – Returns latest scan results from every scan in Tenable Security Center.



Security Center URL:
https://host_url/rest

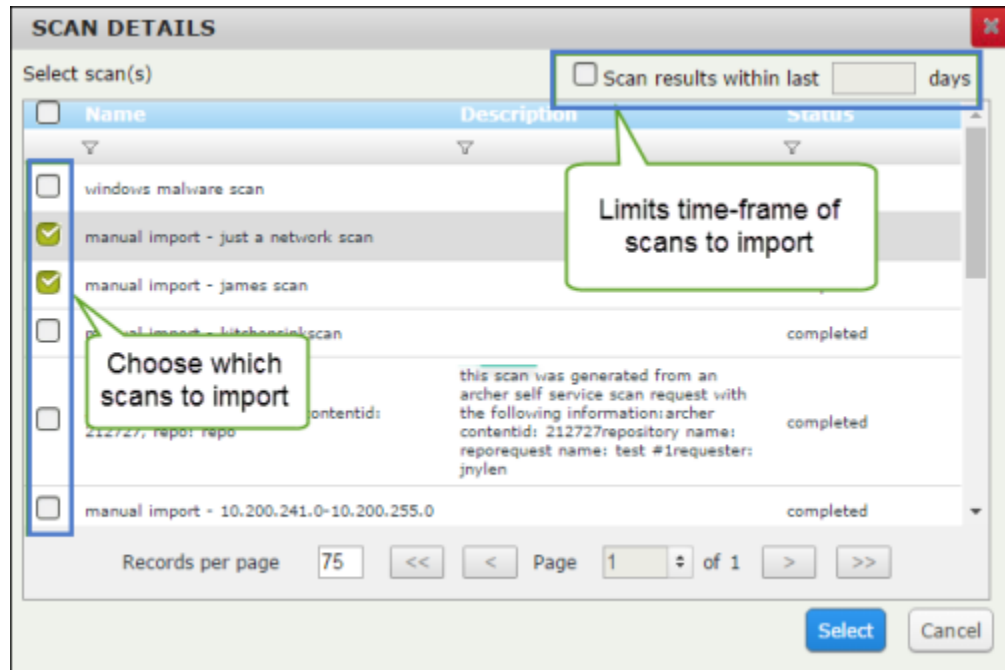
Import mode:
Select all scans

Select scan names(s) or set the number of days:
All scans

If you have selected this mode, go to step 8.

- **Select Specific Scans** – Rsam fetches the latest scan results from Tenable Security Center and allows you to select desired scans.
If you have selected this mode, perform these steps:

- a. Select the [...] icon.
- b. In the **SCAN DETAILS** dialog that opens, select the individual scans to import. The latest completed scan results will be returned. Selecting the *Scan results within last x days* checkbox will return scan results from all scans that have completed within the specified number of days selected.



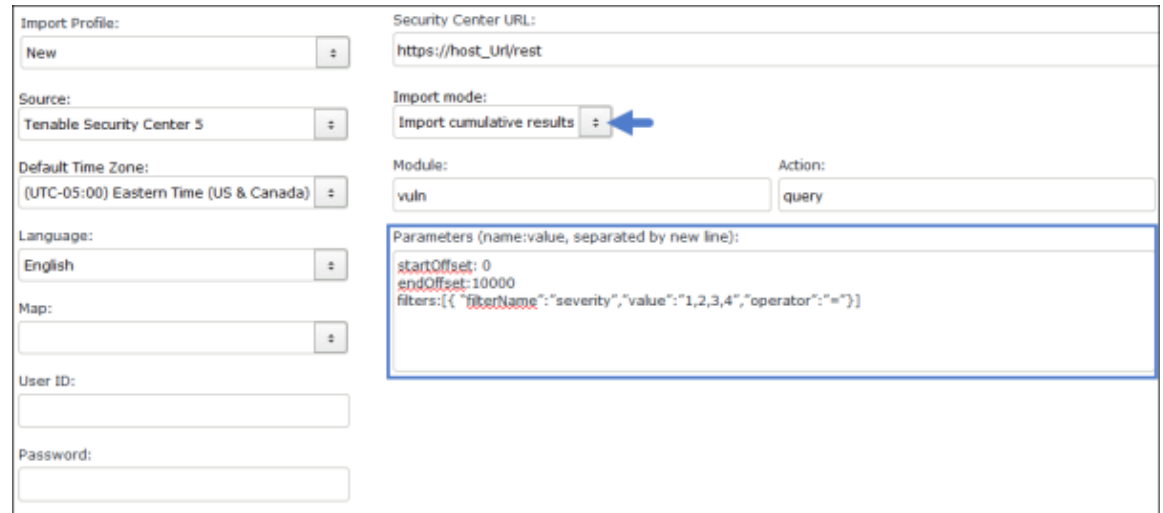
- c. Click **Select**.
 - d. Go to step 8.
- **Import Cumulative Results** – Rsam will return all open vulnerabilities from every scan result in Tenable Security Center 5. Query parameters can be used to filter the results returned to cater to your needs.

If you have selected this mode, perform these steps:

- a. Selecting this mode populates the *Module* field with **vuln** and the *Action* field with query. Retain the values for these two fields.
- b. In the *Parameters* box, specify how many records must be returned. All the text entered in the *Parameters* box is case sensitive. Read through the following table and then complete the parameters.

| Parameter | Description |
|----------------|-----------------------------------|
| startOffset: 0 | This is required. Always set to 0 |

| Parameter | Description |
|---|---|
| endOffset:10000 | This is required. Enter the desired number of records to return. |
| filters:[{"filterName": "severity", "value": "1,2,3,4", "operator": "="}] | This is optional. One or more query filters. Include the filter option, value and operator using the Tenable defined syntax. This example allows customer to filter on vulnerabilities with a severity greater than 0 (Informational). |



Note: The complete list of filters is available from Tenable. Rsam has NOT tested all of the possible filter options or the validity of the values passed to each filter.

If an invalid filter option is entered, Rsam may indicate this as an error message and will not allow you to create/customize a map to import data. If an invalid value is passed to a valid filter option, Rsam will not display an error, however, the results returned by the Security Center API may not be accurate and complete. If you have any questions or encounter any errors for filters, please contact Tenable Support.

- c. Go to step 8.
- 8. Click **Import Now** to import the results, **New Map** to create an import map, or **Customize** to allow you to edit the selected map and/or save the import profile.

Import Assets

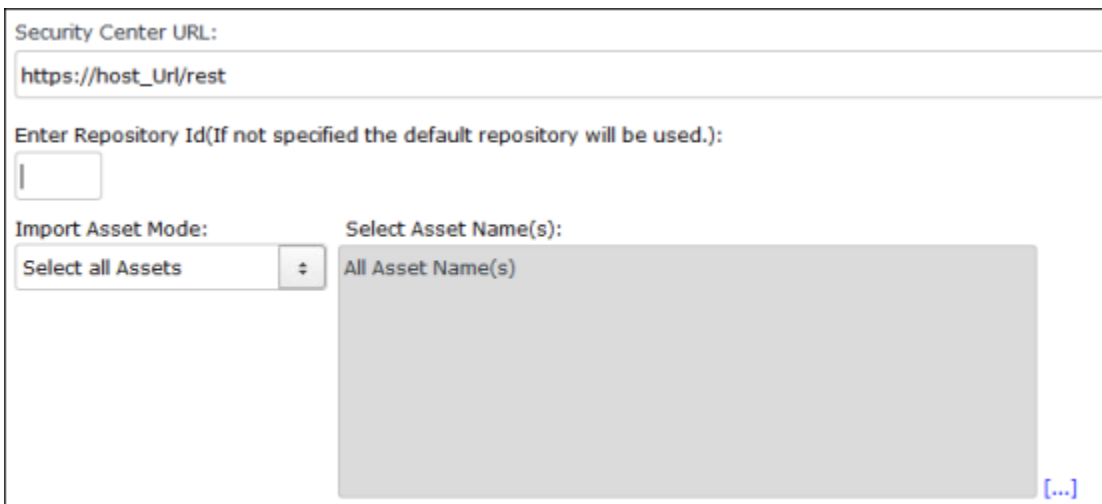
Perform the following steps to import assets:

- 1. Log in to Rsam as administrator and navigate to **Assessments > Import Objects**.

2. Select **New** from the **Import Profile** drop-down list. A profile can be saved and scheduled to import vulnerabilities at regular intervals.
3. Select **Tenable Security Center 5** from the **Source** drop-down list.

Note: The Security Center URL can be pre-populated by specifying it in the Data Import Options category of RSAM Options available in the Administration module. Be sure to enter `/rest` after the URL.

4. Enter an **User ID** for the Tenable Security Center 5.
5. Enter **Password** for the User ID.
6. Enter **Security Center URL**. Be sure to enter `/rest` after the URL.
7. Select any of the following mode to import vulnerabilities.
 - **Select All Assets** – Returns all assets in Security Center.
 - **Select Specific Assets** – Rsam fetches a list of asset groups associated with open vulnerabilities and allows you to select the asset groups to import.
 - **Import Cumulative Results** – You can also choose to import assets based on open vulnerabilities from every scan result in Tenable SC5. Query parameters can be used to filter the results returned to cater to your needs. For more details, refer to the Import Cumulative Results portion under the Importing Vulnerabilities section.



9. Click **Import Now** to import the results, **New Map** to create an import map, or **Customize** to allow you to edit the selected map and/or save the import profile.

Manage Import Maps

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

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

Appendix: Pre-Defined Import Maps

This section describes import maps used for Tenable Security Center integration. The following import maps are available in Rsam to help you import vulnerabilities and assets.

- TENABLE_SECURITY_CENTER5_API (V.1 - SCAN BASED)
- TENABLE_SECURITY_CENTER5_API (V.1 - CUMULATIVE)
- TENABLE_SECURITY_CENTER5_ASSET_API (V.1)

TENABLE_SECURITY_CENTER5_API (V.1 - SCAN BASED)

| Rsam Attribute | Path |
|------------------------------------|--|
| Port | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Report/ReportHost/ReportItem/port |
| Protocol | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Report/ReportHost/ReportItem/protocol |
| Severity - Native (numeric) | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Report/ReportHost/ReportItem/severity |
| Vulnerability ID | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Report/ReportHost/ReportItem/pluginID |
| Vulnerability Name | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Report/ReportHost/ReportItem/pluginName |
| Reference - Bugtraq | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Report/ReportHost/ReportItem/bid |
| CPE | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Report/ReportHost/ReportItem/cpe |
| Related CVE Entries | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Report/ReportHost/ReportItem/cve |
| CVSBase Score | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Report/ReportHost/ReportItem/cvss_base_score |
| CVSTemporal Score | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Report/ReportHost/ReportItem/cvss_temporal_score |

| Rsam Attribute | Path |
|----------------------------|---|
| Exploitable | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Report/ReportHost/ReportItem/exploit_available |
| Exploit Ease | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Report/ReportHost/ReportItem/exploitability_ease |
| Plugin Modify Date | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Report/ReportHost/ReportItem/plugin_modification_date |
| Plugin Publish Date | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Report/ReportHost/ReportItem/plugin_publication_date |
| Plugin Type | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Report/ReportHost/ReportItem/plugin_type |
| Script Version | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Report/ReportHost/ReportItem/script_version |
| Fix/Resolution | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Report/ReportHost/ReportItem/solution |
| Reference - OSVDB | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Report/ReportHost/ReportItem/osvdb |
| Actual Result | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Report/ReportHost/ReportItem/plugin_output |
| Exploit Source | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Report/ReportHost/ReportItem/edb-id |
| Description | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Report/ReportHost/ReportItem/synopsis |
| Risk | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Report/ReportHost/ReportItem/description |
| Reference - General | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Report/ReportHost/ReportItem/xref |
| Family ID | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Report/ReportHost/ReportItem/pluginFamily |
| Scan Name | /TENABLE_SECURITY_CENTER5/NessusClientData_v2/Policy/policyName |

TENABLE_SECURITY_CENTER5_API (V.1 - CUMULATIVE)

| Rsam Attribute | Path |
|------------------------------------|--|
| Vulnerability ID | /CUMULATIVE_DETAILS/response/results/pluginID |
| Severity - Native (numeric) | /CUMULATIVE_DETAILS/response/results/severity/id |
| Vulnerability Name | /CUMULATIVE_DETAILS/response/results/pluginName |
| Port | /CUMULATIVE_DETAILS/response/results/port |
| Protocol | /CUMULATIVE_DETAILS/response/results/protocol |
| Host IP Address | /CUMULATIVE_DETAILS/response/results/ip |
| Date Last Found | /CUMULATIVE_DETAILS/response/results/lastSeen |
| Date Discovered | /CUMULATIVE_DETAILS/response/results/firstSeen |
| Exploitable | /CUMULATIVE_DETAILS/response/results/exploitAvailable |
| Exploit Ease | /CUMULATIVE_DETAILS/response/results/exploitEase |
| Family ID | /CUMULATIVE_DETAILS/response/results/family/id |
| Repository ID | /CUMULATIVE_DETAILS/response/results/repository/id |
| Plugin Modify Date | /CUMULATIVE_DETAILS/response/results/pluginModDate |
| Plugin Publish Date | /CUMULATIVE_DETAILS/response/results/pluginPubDate |
| CPE | /CUMULATIVE_DETAILS/response/results/cpe |
| CVSBase Score | /CUMULATIVE_DETAILS/response/results/baseScore |
| Exploit Source | /CUMULATIVE_DETAILS/response/results/exploitFrameworks |
| Fix/Resolution | /CUMULATIVE_DETAILS/response/results/solution |
| Actual Result | /CUMULATIVE_DETAILS/response/results/pluginText |
| Description | /CUMULATIVE_DETAILS/response/results/synopsis |
| Risk | /CUMULATIVE_DETAILS/response/results/description |

| Rsam Attribute | Path |
|----------------------------|--|
| Host Name - DNS | /CUMULATIVE_DETAILS/response/results/dnsName |
| Host Name - NetBIOS | /CUMULATIVE_DETAILS/response/results/netbiosName |
| Host MAC Address | /CUMULATIVE_DETAILS/response/results/macAddress |
| CVSTemporal Score | /CUMULATIVE_DETAILS/response/results/temporalScore |
| Script Version | /CUMULATIVE_DETAILS/response/results/version |
| Reference - CVE | /CUMULATIVE_DETAILS/response/results/cve |
| Reference - OSVDB | /CUMULATIVE_DETAILS/response/results/xref |
| Reference - General | /CUMULATIVE_DETAILS/response/results/seeAlso |
| Reference - Bugtraq | /CUMULATIVE_DETAILS/response/results/bid |
| Plugin Type | /CUMULATIVE_DETAILS/response/results/checkType |
| Related CVE Entries | /CUMULATIVE_DETAILS/response/results/cve |

TENABLE_SECURITY_CENTER5_ASSET_API (V.1)

| Rsam Attribute | Path |
|----------------------------|--|
| Host IP Address | /TENABLE_SECURITY_CENTER5/ASSET_DETAILS/response/ip |
| Host Name - NetBIOS | /TENABLE_SECURITY_CENTER5/ASSET_DETAILS/response/netbiosName |
| Host Name - DNS | /TENABLE_SECURITY_CENTER5/ASSET_DETAILS/response/dnsName |
| Host OS | /TENABLE_SECURITY_CENTER5/ASSET_DETAILS/response/os |
| Last Scanned Date | /TENABLE_SECURITY_CENTER5/ASSET_DETAILS/response/lastScan |
| Host MAC Address | /TENABLE_SECURITY_CENTER5/ASSET_DETAILS/response/macAddress |



| Rsam Attribute | Path |
|---------------------------------------|--|
| Last Authenticated Scan Date | /TENABLE_SECURITY_CENTER5/ASSET_DETAILS/response/lastAuthRun |
| Last Unauthenticated Scan Date | /TENABLE_SECURITY_CENTER5/ASSET_DETAILS/response/lastUnauthRun |

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.

