



SOAR-TVM Module

Qualys Integration Guide

Document Version: 2018.05.03 | May 2018

Rsam © 2018. All rights reserved

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

Contents

Solution Summary	4
Introduction	5
Prerequisites for using the Qualys API Integration	5
Qualys Limit of Concurrent API Calls	5
or! Bookmark not defined.	Err
Accessing the Qualys API	8
Importing Assets.....	9
Qualys Online Report v2	9
Import Host List Mode	10
Import Host List Using Tags Mode.....	11
Import Using Saved Report Mode.....	12
Import Using Custom API Call.....	13
Qualys Online Report	14
Manually Entered API Calls	15
Importing Vulnerabilities	17
Qualys Online Report v2	17
Import Current Vulnerabilities	18
Import Using Saved Report	19
Import Using Custom API Call.....	19
Qualys Online Report.....	19
Import Vulnerabilities using Saved Reports.....	20
Import Vulnerabilities using Templates	21
Import Vulnerabilities using Raw Data	22
Import Qualys Tickets.....	23
Importing using a Downloaded Qualys Results XML file	24
Importing Vulnerabilities for High-Volume Devices.....	25
Importing Qualys Knowledgebase.....	27
Importing Policy Compliance Data	29
Qualys Online Report v2	29
Import Compliance Controls.....	29
Import Compliance Scan Results.....	30
Managing Maps	32
Appendix 1: Predefined Import Maps	33

Asset Import Maps	33
V: QUALYS_HOST_LIST_API (v.1)	33
H: QUALYS_AUTHENTICATION_API (v.1)	34
H: QUALYS_ASSET_GROUP_API (v.1)	34
H: QUALYS_ASSET_LIST_API (v.1)	35
H: QUALYS_ASSET_SEARCH_API (v.1)	35
H: QUALYS_ASSET_IMPORT – Saved Report (v.1)	36
H: QUALYS_ASSET_DATA_REPORT_API (v.1)	36
Vulnerability Import Maps	37
V: QUALYS_CURRENT_VULN_API (v.1)	37
V: Qualys_XML (v.3 – Saved Reports)	38
V: QUALYS_XML (v.4 – Template)	39
Qualys Ticket Maps	41
V: QUALYS_TICKET_XML (v.2)	41
Qualys High-Volume Import Maps	42
V: QUALYS_SUMMARY_XML (v.1)	42
Knowledgebase Import Maps	43
V: QUALYS_KB_API (v.1)	43
Compliance Import Maps	47
Compliance Results	47
Compliance Controls	48
Appendix 2: Qualys User Permissions	49
Importing Assets	49
Importing Vulnerabilities	49
Importing Compliance Data	50
Importing KnowledgeBase	50
Appendix 3: Qualys API Calls	51
Appendix 4: Qualys Report Template Configuration	52
Qualys Saved Report	52
Qualys Template	53
Appendix 5: Rsam Documentation	56
Inline Help	56

Solution Summary

Rsam's Security Operations Analytics Reporting Threat and Vulnerability Management solution (TVM) provides an integrated approach to managing a broad spectrum of risks across the enterprise. Our integration with Qualys' Cloud Platform allows companies to import asset, security and compliance data stored in Qualys 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 providing deeper insight into and a simplified way of reporting on overall organizational risk.

Rsam provides a direct connection to your Qualys console, allowing you to import any Qualys data accessible via the Qualys API. This includes data such as assets, vulnerabilities, tickets and policy compliance results. Data can also be imported using predefined Qualys templates, saved reports or raw scan results.

Rsam also offers the ability to import the Qualys Knowledgebase and compliance controls for a given policy into an Rsam library. A common use case for importing these libraries is to allow customers to add custom scoring attributes, security team comments, recommended solutions, mitigating controls, and/or modify default severity ratings for an individual Qualys ID (QID). When Qualys vulnerability or policy compliance data is imported, they are linked to appropriate record in the Rsam library and can be referenced by simply displaying the data and/or copying over pertinent data into the imported records.

Another feature Rsam offers is the ability to summarize imported Qualys vulnerability data by QID for high-volume devices (e.g., workstations, network devices). Where a typical vulnerability import will create a single record for each vulnerability present on an asset, the summary import only creates one record per vulnerability (QID) with a count of how many devices are affected by this vulnerability. It will also record the IP addresses and machine names of all affected devices, to allow for searches and reporting.

All API connections include a user-friendly interface to filter the data you'd like to import or you can enter a custom API call using Qualys' defined API calls and parameters. Alternatively, customers can download XML files from Qualys and import those manually.

Rsam offers this out-of-the-box configuration in our TVM baseline module, including predefined import maps to allow for a customer to utilize any of the import options.

Introduction

This document will guide you through the steps necessary to configure Rsam TVM to successfully import Qualys data. The guide outlines the universal steps to access the API and is then broken into sections for each import mode:

- Importing Assets
- Importing Vulnerabilities
- Import High-volume vulnerabilities
- Import Knowledgebase
- Import Policy Compliance Data

Prerequisites for using the Qualys API Integration

Your Qualys account representative must enable your instance with the ability to use API connections

The user account required to connect to the Qualys console has API Access set to 'Yes'. This can be reviewed in your Qualys console's User management section.

General Information	
Name:	[REDACTED]
Role:	Manager
Business Unit:	Unassigned
GUI Access:	Yes
API Access:	Yes

Data returned by import modes is based on the user's role and corresponding permissions. Please reference Appendix 2 for a listing of the user permissions applicable to the different import modes.

Adjust the session timeout for the Qualys user account, if necessary. Timeouts are set to 60 minutes by default, but can be increased in the Qualys user interface under Users → Setup → Security.

Adjust the number of Host tags to be returned by the API when filtering imports based on tag, if necessary. The default value is set to 300. This update is done in SQL by updating Option ID 12006 in the SYS_OPTION. Please contact support for the exact command if you need assistance.

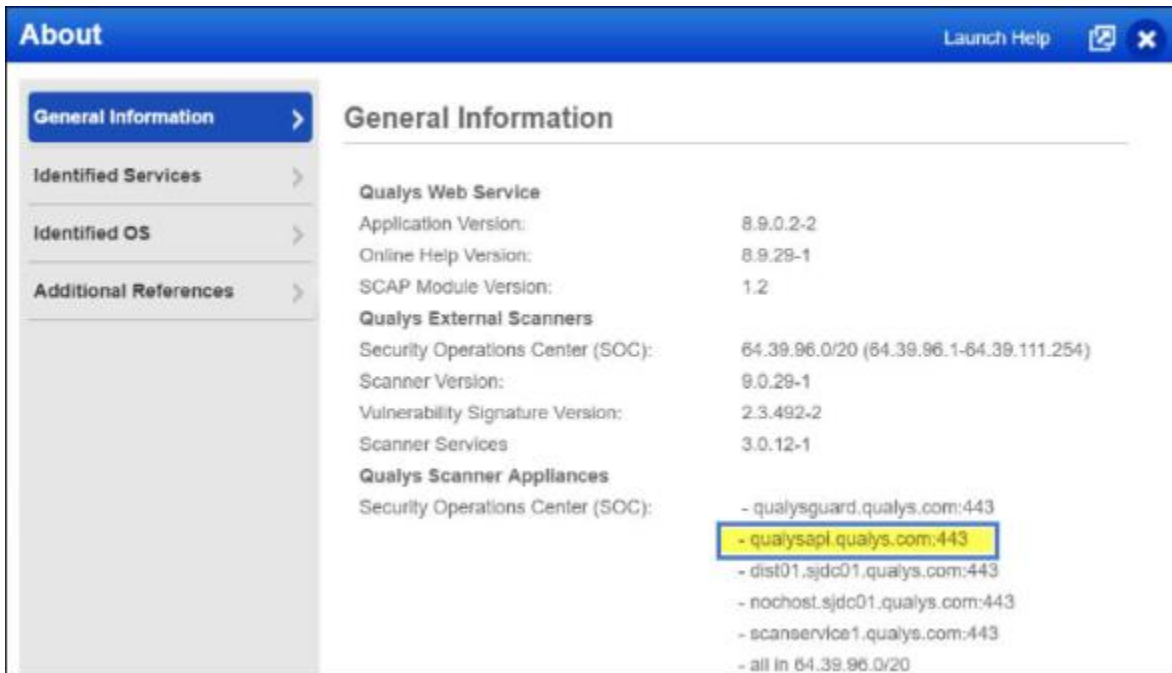
Confirm the platform where your Qualys user account is located matches the default URLs that Rsam uses when making API calls to the Qualys console.

- Qualys Online Report: <https://qualysapi.qualys.com/msp/>

Note: If you are using the Qualys Online Report API option along with a service such as TELUS, you may need to edit this URL. This is done in SQL by updating the Option ID 9020 in the SYS_OPTION table. For exact instructions, please contact Rsam Support.

- Note that Qualys Online Report v2: <https://qualysapi.qualys.com> (Qualys US Platform 1)

The API Server for your user account that is used when accessing Qualys Online Report v2 API option can be found in the Qualys console:



If this is not the platform where your account is located, please enter the correct URL in Rsam Options > Data Import Options. Please ensure "/" is included at the end of your URL. You may need to log out of Rsam and log back in for the change to take effect.

RSAM Options	
Option Categories	
Data Import Options	
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
Nexpose Console URL	https://host:port/api/1.1/xml
Service Now Instance URL	https://instance-name.service-now.com/api/now/v1/table
Delimiter to use for export CSV	,
Qualys V2 API URL	https://qualysapi.qualys.com/

You can validate the user account selected in the import profile and successfully authenticate to the Qualys API by performing the following steps:

1. Open any web browser.
2. Enter a manual API call into the URL field. For examples on API calls, see the [Manually Entered API Calls](#) section.
3. When prompted, enter the credentials for the user account selected in the import profile
4. If account access is successful, you will see the results from the API call displayed in your browser. If the user account is not configured with the correct access, you will get an "Access Denied" message.
5. In this case, confirm the user account has been configured with the required access stated above, as well as, the necessary permissions defined by Qualys mentioned in [Appendix 2: Qualys User Permissions](#). Contact Qualys for the updated list of required permissions.

If access is successful and you still receive authorization errors when trying to import from Rsam, complete the steps above directly from the Rsam web server. This will confirm the network settings that allow Rsam to access the Qualys console.

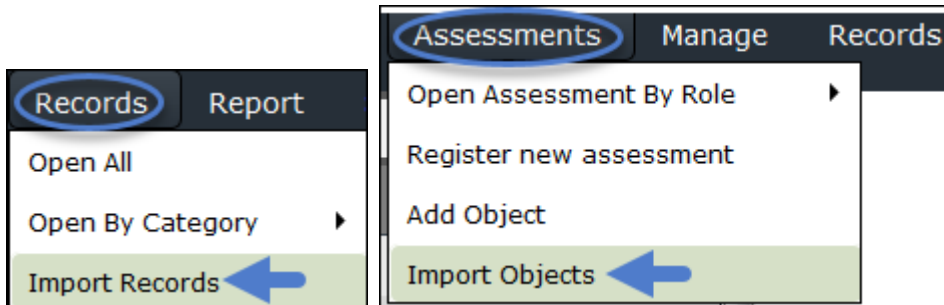
Qualys Limit of Concurrent API Calls

It is important to know that Qualys enforces a limit on the number of concurrent API calls that can be made based on each customer's API tier. Exceeding this limit may prevent import profiles from loading or imports from running. Appendix 3 outlines the number of API calls each import mode makes. Should you have issues when loading profiles or imports successfully completing, please reach out to your Qualys representative to find out what your API limits are.

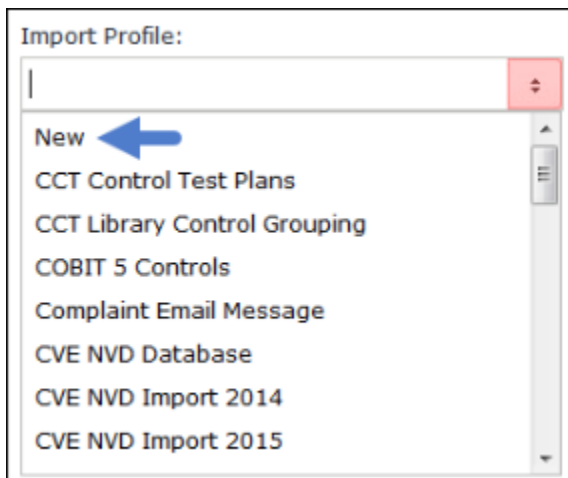
Accessing the Qualys API

To access the Qualys API, perform the following steps:

1. Log into Rsam using an Administrative account or an account that has been granted the privileges to perform imports.
2. To import vulnerabilities, compliance results and Knowledgebase, navigate to **Records** > **Import Records**. To import asset data, navigate to **Assessments** > **Import Objects**.



3. Select **New** from the **Import Profile** drop-down list. Initially a profile will not be configured; however, a profile can be saved to allow for scheduled imports to occur.



Importing Assets

While IT Host objects are created in Rsam during a vulnerability import, customers commonly want to record additional information available in Qualys about these hosts. This may include operating system, DNS or NetBIOS name, date the asset was last scanned or authentication status. Within the Import Objects interface, you can import assets using the following 5 options:

- **Qualys Online Report v2**
 - o Import Host List – Import assets with optional filters based on asset group, IP address and/or last scan date
 - o Import Host List with Tags – Import assets matching selected tag(s)
 - o Import Using Saved Report – Import asset data using a customer’s predefined Qualys saved report
 - o Import Using Custom API Call – Import assets using a user-defined Qualys supported API call
- **Qualys Online Report**
 - o Import Asset Groups - Import assets for a selected Qualys asset group
- **Manually entered API call** – Customer can enter a Qualys API v1 call, such as Asset IP List or Asset Search List

The output available using one option may differ from another option. Rsam’s predefined mappings correspond to the available data returned. Mappings can be found in [Appendix 1: Predefined Import Mappings](#).

Qualys Online Report v2

1. Select **Qualys Online Report v2** from the **Source** drop-down list.
2. Enter user credentials in the **User ID** and **Password** fields.
3. Select any of the following mode from the **Mode** drop-down list.
 - Import Host List
 - Import Host List with Tags

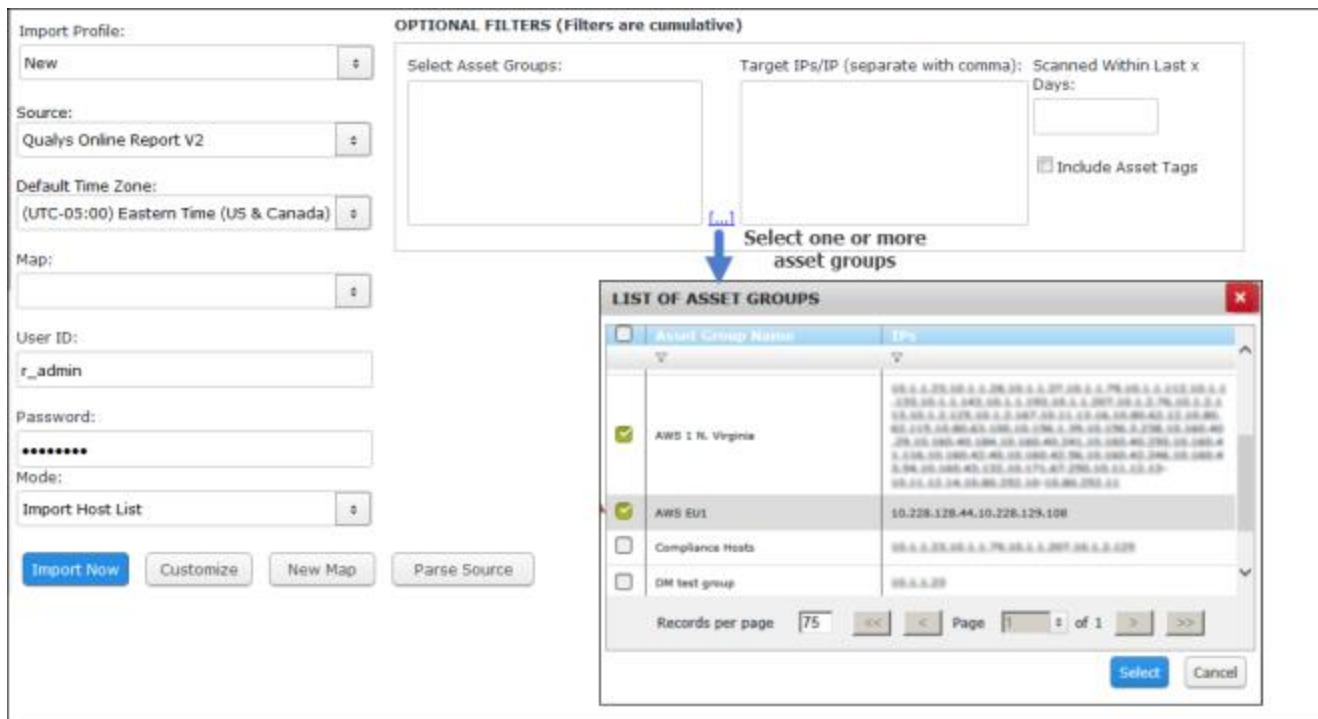
- Import Using Saved Report
- Import Using Custom API Call

After selecting a mode, the screen is updated to provide an interface for entering parameters used in filtering the data returned. Depending on the mode, the user will need to make a required selection and/or choose to select an 'Optional' filter. These screens and filters are described in the sections below.

Import Host List Mode

Rsam will import all assets in Qualys that the user account has permissions to. You can limit the data imported by applying optional filters based on asset group, IP address and days since last scan. All filters are cumulative.

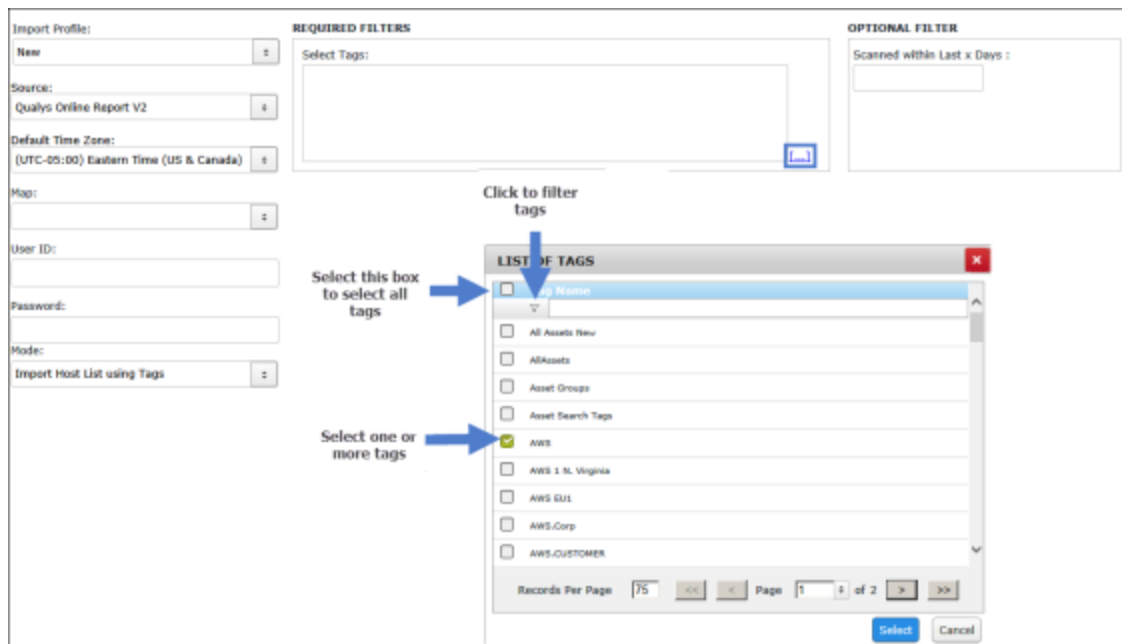
- **Select Asset Groups** – Allows you to import assets within the selected asset group(s).
 - a. Click the [\[...\]](#) select icon on the right side of the **Select Asset Groups** field.
 - b. In the **LIST OF ASSET GROUPS** dialog that opens, select the desired asset group(s) and click **Select**. Selected asset group(s) will be listed in the **Select Asset Group** field.
- **Target IP /Range** – Import assets that match the IP address entered or fall within an entered IP range.
 - a. Enter specific IP addresses or an IP range. Separate values with a comma.
- **Scanned Within Last x Days** – Returns assets that have scanned within the specified number of days selected.
- **Include Asset Tags** – Select the check box to include the tags for each asset.



Import Host List Using Tags Mode

Rsam requires an entry to import assets that match the selected tag(s). Only assets that are tagged with the selected value(s) are returned.

1. Click the [\[...\]](#) select icon on the right side of the **Select Tags** field.
2. In the **LIST OF TAGS** dialog that opens, select the check boxes of the tags you want to import. Selecting the check box next to **Tag Name** will select all tags.
3. Selected tags(s) will be listed in the **Select Tags** field.
4. **Scanned Within Last x Days** – Returns assets that have scanned within the specified number of days selected.



Import Using Saved Report Mode

Rsam will import asset data returned in a Qualys saved report. Rsam will display a list of XML and CVS saved reports defined in your Qualys instance.

1. Click the [...](#) select icon on the right side of the **Select Report** field.
2. In the **LIST OF REPORTS FOR USER TO SELECT** dialog that opens, select the saved report you want to import. The report name will be listed in the **Select Report** field.

Import Profile:

Source:

Default Time Zone:

Map:

User ID:

Password:

Mode:

Select Report:

LIST OF REPORTS FOR USER TO SELECT

Report Type	Report Title	Report Generated By	Date Generated
Scan	Example Report	...	2017-05-12 14:41:54
Authentication	MV Authentication Report	...	2017-05-07 21:00:13

Select the desired report

Records per page: 75 Page 1 of 1

View	Report Title	Type	Launched	Report Template
<input type="checkbox"/>	Example Report			Confirmed Severity 3 - 5
<input type="checkbox"/>	MV Authentication Report			Authentication Report

Note that if saved reports expire or are removed from the Qualys console, subsequent imports may fail.

For more information about Qualys saved reports and templates, see [Qualys Report Template Configuration](#).

Import Using Custom API Call

This mode allows you to import data using a supported Qualys API call available for your Qualys module(s), as defined by the Qualys approved parameters you select. Please refer to Qualys' API documentation for the list of valid API calls and available parameters.

1. Select the API call mode (POST or GET) required by the API call.
2. Enter the API call you wish to use.

Import Profile:

Source:

Default Time Zone:

Map:

User ID:

Password:

Mode:

Select the API call mode:

Enter the API call below. This text will be appended to the base URL set in the Data Import Options section of Rsam Options.

```

/pps/rest/2.0/search/am/hostasset
<ServiceRequest>
<filters>
<Criteria field="tagName" operator="EQUALS">Tag1</Criteria>
</filters>
</ServiceRequest>
    
```

Example API call to asset management and tagging module.
Note that this call requires use of the POST API call mode.

This call will import assets with tag name starting "Tag1"

Import Profile:

Source:

Default Time Zone:

Map:

User ID:

Password:

Mode:

Select the API call mode:

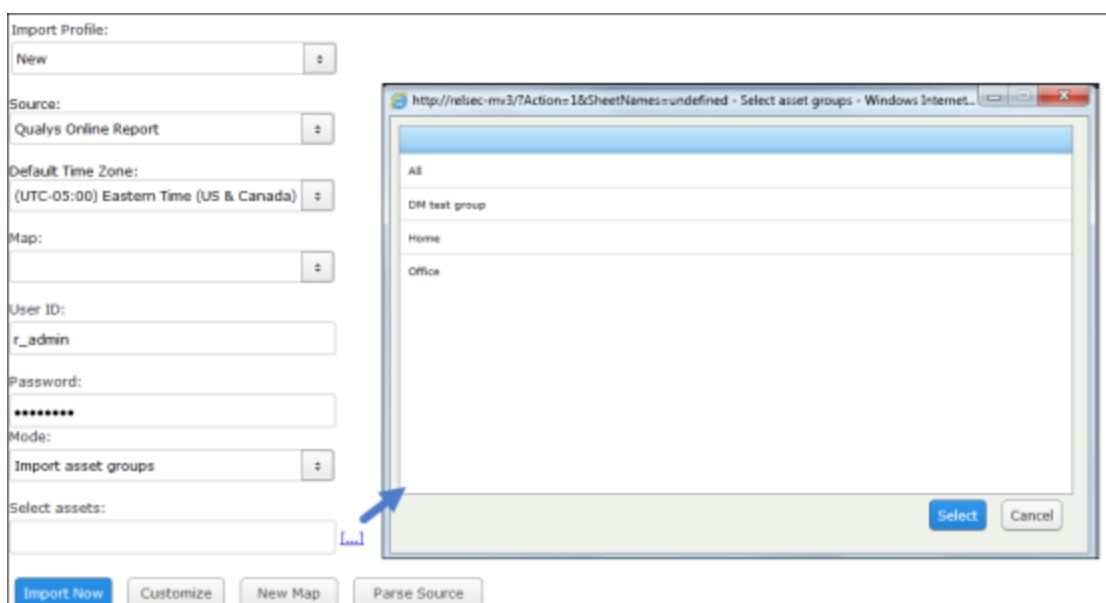
Enter the API call below. This text will be appended to the base URL set in the Data Import Options section of Rsam Options.

```

/api/2.0/fo/asset/host?action=list&truncation_limit=0&details=All&use_tag=1&tag_set_by=name&tag_set_include=tag1,tag2&show_tags=1
    
```

Qualys Online Report

1. Select **Qualys Online Report** from the **Source** drop-down list.
2. Enter user credentials in the **User ID** and **Password** fields.
3. Select the **Import asset groups** mode from the **Mode** drop-down list.
 - a. Click the [\[...\]](#) select icon on the right side of the **Select Assets** field.
 - b. In the pop-up that opens, select the desired asset group and click **Select**.



Manually Entered API Calls

Users can manually enter Qualys V1 API calls to import asset data.

1. Select **XML file** from the **Source** drop-down list.
2. Enter user credentials in the **User ID** and **Password** fields.
3. Change the Source Location to URL and enter a valid API call. For more information on Qualys API calls and parameters, please refer to the *Qualys-api-v1 User Guide*.

Examples of API calls to import asset data:

- Asset IP List – Returns all assets scanned with host details, including asset tags
https://qualysapi.qualys.com/msp/asset_ip_list.php?detailed_results=1
- Asset Search – Returns all assets scanned for one or more asset groups. Includes host details except for asset tags. Adjust this API call to specify individual asset groups or all asset groups.
https://qualysapi.qualys.com/msp/asset_search.php?target_asset_groups=assetgroupname

In the example below, replace assetgroupname with the name(s) of the Qualys asset group(s) you want to import or to return all scanned assets, update the parameter to 'All'. Note that asset group names are case-sensitive and any spaces in the asset group name must be replaced with the + sign. Multiple asset groups can be imported by separating them with a comma.

Importing Assets



Import Profile:

New

Source:

XML file

Default Time Zone:

(UTC-05:00) Eastern Time (US & Canada)

Map:

Source Location:

URL

User ID:

r_admin

Password:

UnCompress Compressed Files

URL https://qualysapi.qualys.com/msp/asset_search.php?target_asset_groups=DM+Test+Group,Home

Importing Vulnerabilities

By using the Import Records interface, you can import vulnerabilities using the following options:

- **Qualys Online Report v2**
 - o Import Current Vulnerabilities – Import vulnerabilities with optional filters based on asset group, IP address and/or last scan date.
 - o Import Using Saved Report – Imports vulnerability data using a customer’s predefined Qualys saved report.
 - o Import Using Custom API Call – Import vulnerabilities using a user-defined Qualys supported API call.

- **Qualys Online Report**
 - o Import vulnerabilities using saved reports - Imports vulnerabilities found using a customer’s predefined Qualys saved report.
 - o Import vulnerabilities using templates - Imports vulnerabilities found using a customer’s predefined Qualys template.
 - o Import vulnerabilities using raw data - Imports all current vulnerabilities for a selected scan of an asset group or IP addresses.
 - o Import Qualys Tickets – Imports vulnerabilities based on Qualys ticketing set up in your instance.

The output available using one option may differ from another option. Rsam’s predefined mappings correspond to the available data returned are available in [Predefined Import Maps](#).

Qualys Online Report v2

1. Select **Qualys Online Report v2** from the **Source** drop-down list.
2. Enter user credentials in the **User ID** and **Password** fields.
3. Select a mode to import from. There are 2 options available:
 - Import Current Vulnerabilities

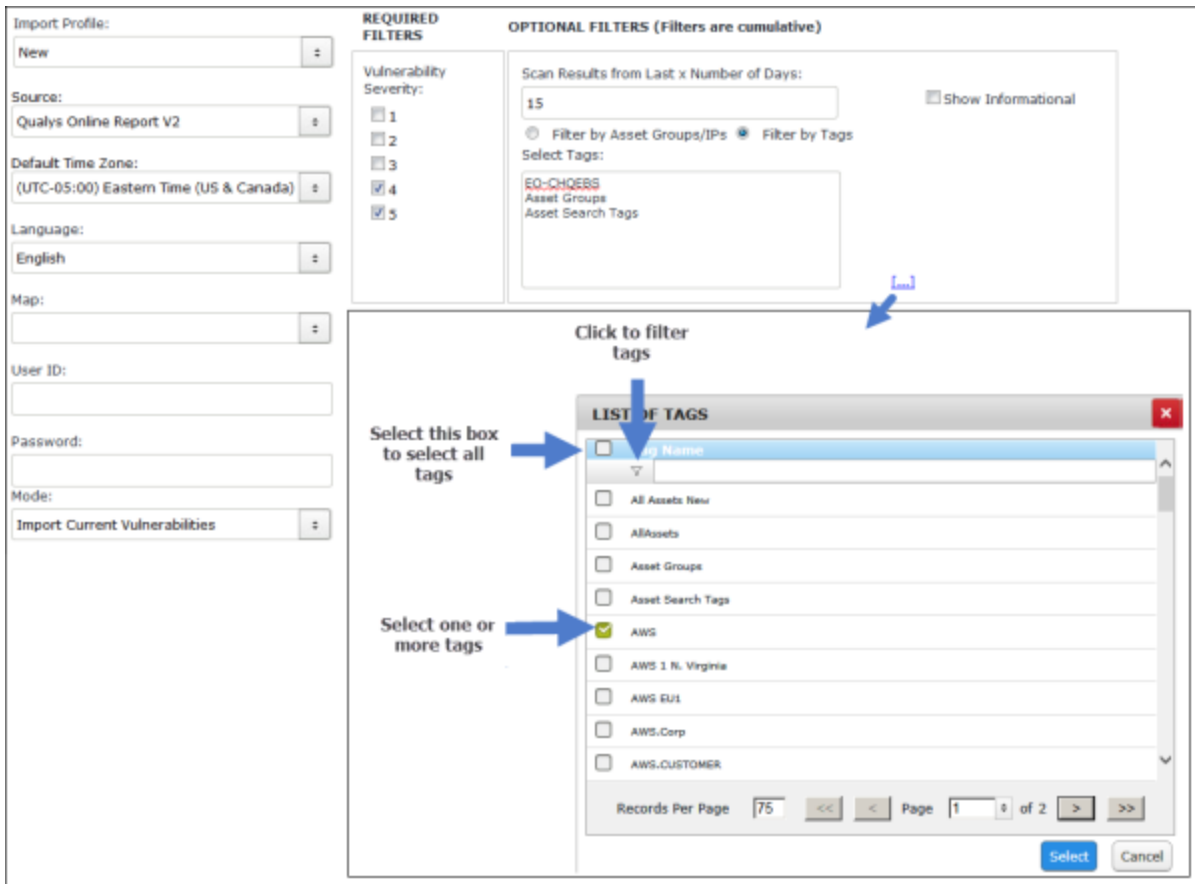
- Import Using Saved Report

After selecting a mode, the screen is updated to provide a graphical interface for entering parameters used in filtering the data returned. Depending on the mode, the user will need to make a required selection and/or choose to select an 'Optional' filter. These screens and filters are described in the sections below.

Import Current Vulnerabilities

Rsam will import all vulnerabilities in Qualys that the user account has permissions to. The severity rating is required and you can further limit the data imported by applying optional filters based on asset group, IP address, tags and days since last scan. All filters are cumulative.

- **Vulnerability Severity** – You are required to select at least one severity rating.
- **Asset group** – Import vulnerabilities for assets within the selected asset group(s)
 - o Select the **Filter by Asset Groups/IPs** radio button.
 - o Click the [\[...\]](#) select icon on the right side of the **Select Asset Groups** field.
 - o In the pop-up that opens, select the desired asset group(s) and click **Select**.
 - o Selected asset group(s) will be listed in the **Select Asset Group** field.
- **Target IP /Range** – Import vulnerabilities that match the IP address entered or fall within an entered IP range
 - o Enter specific IP addresses or an IP range. Separate values with a comma.
- **Tags** – Import vulnerabilities for assets with the selected tag(s).
 - o Select the **Filter by Tags** radio button.
 - o Click the [\[...\]](#) select icon on the right side of the **Select Tags** field.
 - o In the pop-up that appears, select the check boxes of the tags you want to filter your import. Selecting the check box next to **Tag Name** will select all tags.
 - o Selected tags(s) will be listed in the **Select Tags** field.
- **Scan Results from Last x Number of Days** – Returns vulnerabilities for assets that have scanned within the specified number of days selected.
- **Show Informational** – Select this check box to includes vulnerabilities flagged as informational in your import.



The screenshot displays the 'Import Profile' configuration page. On the left, there are fields for 'Import Profile' (set to 'New'), 'Source' (set to 'Qualys Online Report V2'), 'Default Time Zone' (set to '(UTC-05:00) Eastern Time (US & Canada)'), 'Language' (set to 'English'), 'Map', 'User ID', 'Password', and 'Mode' (set to 'Import Current Vulnerabilities').

The 'REQUIRED FILTERS' section shows 'Vulnerability Severity' with checkboxes for levels 1 through 5, where levels 4 and 5 are selected.

The 'OPTIONAL FILTERS (Filters are cumulative)' section includes a 'Scan Results from Last x Number of Days' field set to '15', a 'Show Informational' checkbox, and radio buttons for 'Filter by Asset Groups/IPs' and 'Filter by Tags' (the latter is selected). Below this is a 'Select Tags' list containing 'EO-CHECKS', 'Asset Groups', and 'Asset Search Tags'.

A modal window titled 'LIST OF TAGS' is open, showing a list of tags with checkboxes. Annotations include:

- 'Click to filter tags' pointing to the 'Filter by Tags' radio button.
- 'Select this box to select all tags' pointing to the top checkbox in the tag list.
- 'Select one or more tags' pointing to the 'AWS' checkbox, which is checked.

 The tag list includes: 'All Assets New', 'AllAssets', 'Asset Groups', 'Asset Search Tags', 'AWS', 'AWS 1 N. Virginia', 'AWS EU1', 'AWS.Corp', and 'AWS.CUSTOMER'. The dialog also shows 'Records Per Page' set to 75 and 'Page 1 of 2'.

Import Using Saved Report

Please refer to the [Import Using Saved Report](#) section under Importing Assets.

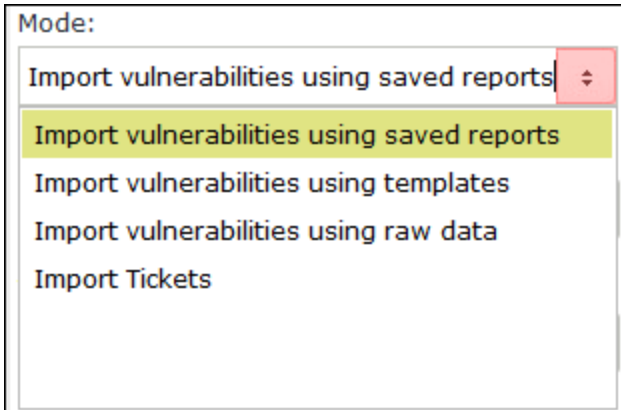
Import Using Custom API Call

Please refer to the [Import Using Custom API Call](#) section under Importing Assets.

Qualys Online Report

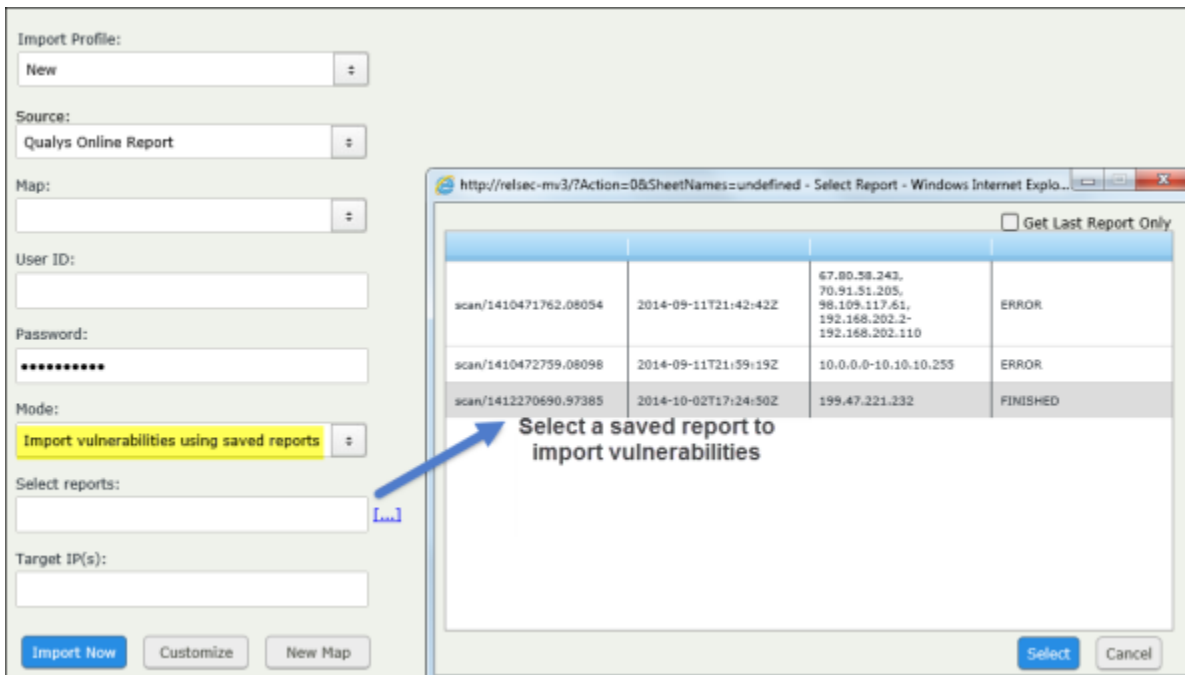
1. Select **Qualys Online Report** from the **Source** drop-down list.
2. Enter user credentials in the **User ID** and **Password** fields.
3. Select any of the following import mode from the **Mode** drop-down list.
 - Import vulnerabilities using saved reports

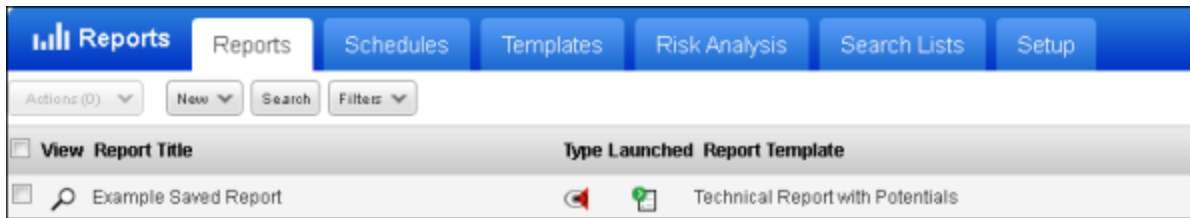
- Import vulnerabilities using templates
- Import vulnerabilities using raw data
- Import tickets



Import Vulnerabilities using Saved Reports

Rsam will display a list of saved reports defined in your Qualys instance.

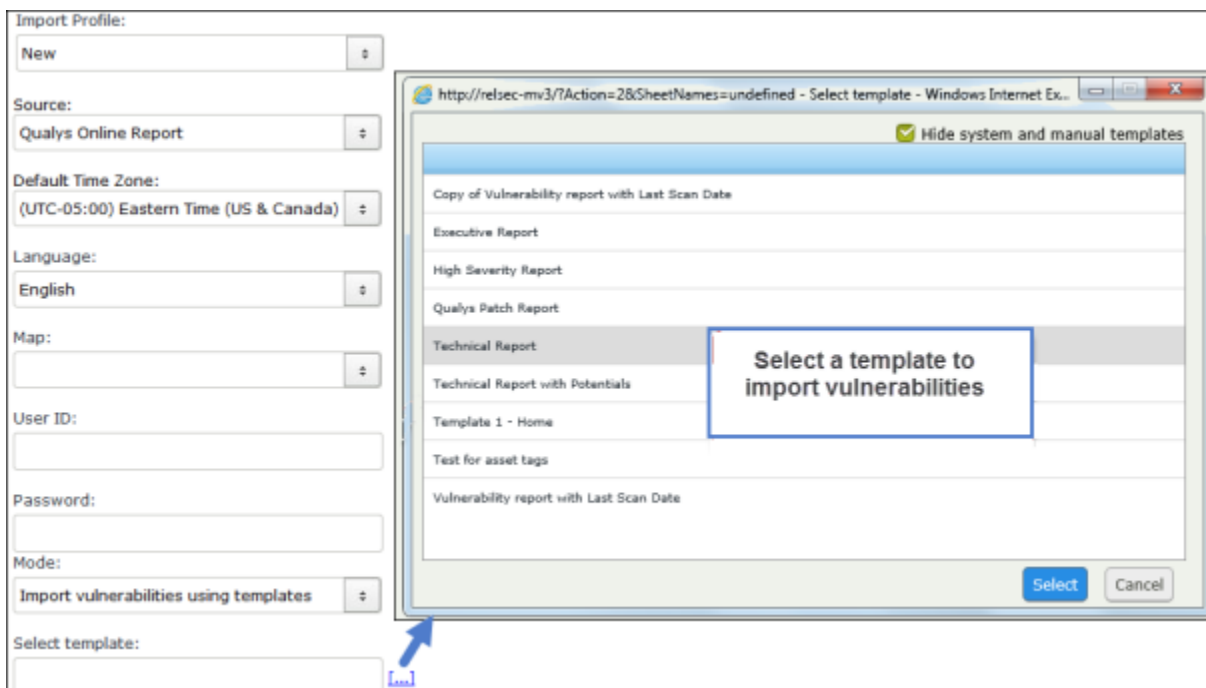


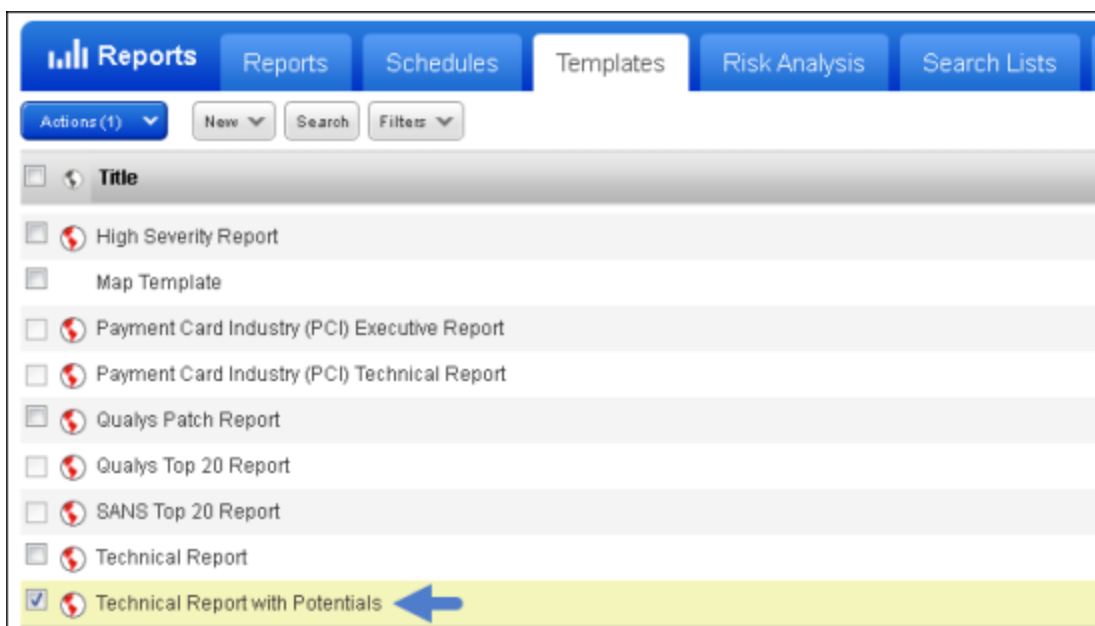


For more information on how to set up Qualys saved reports and templates, see [Qualys Report Template Configuration](#).

Import Vulnerabilities using Templates

Rsam will display a list of templates defined in your Qualys instance.





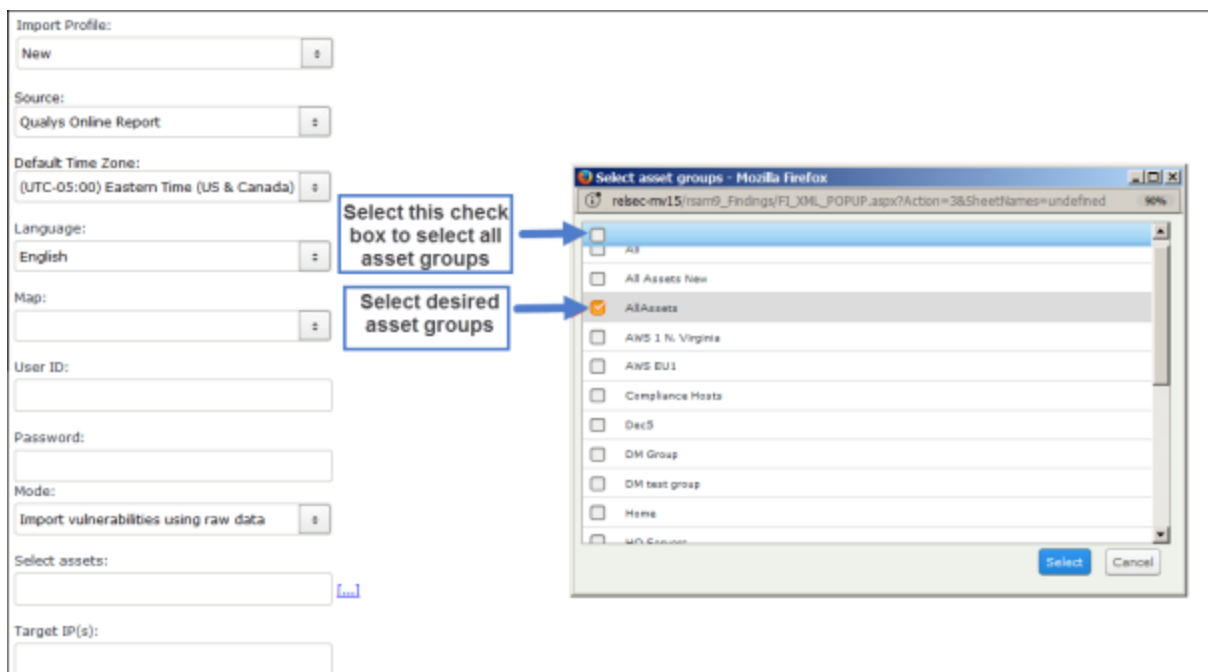
For more information on how to set up Qualys saved reports and templates, see [Qualys Report Template Configuration](#).

Import Vulnerabilities using Raw Data

Rsam will import the last scan results for selected asset groups defined in your Qualys instance. All filters are cumulative.

Rsam will import last scan results for selected asset groups defined in your Qualys instance that the user account has permissions to. An asset group is required and you can further limit the data imported by applying optional filters based IP address. All filters are cumulative.

- **Asset group** – Import vulnerabilities for assets within the selected asset group(s).
 1. Click the [\[...\]](#) select icon on the right side of the **Select Assets** field.
 2. In the pop-up that opens, select the desired asset group(s) and click **Select**.
 3. Selected asset group(s) will be listed in the **Select Asset Group** field.
- **Target IP /Range** – Import vulnerabilities that match the IP address entered or fall within an entered IP range
 - o Enter specific IP addresses or an IP range. Separate values with a comma.



Import Qualys Tickets

Rsam will import existing Qualys tickets based on the filters selected. The ticket status, vulnerability and potential severity rating filters are required. You can further limit the data imported by applying optional filters based on the numbers of days since the ticket was last modified and the ticket assignee. All filters are cumulative.

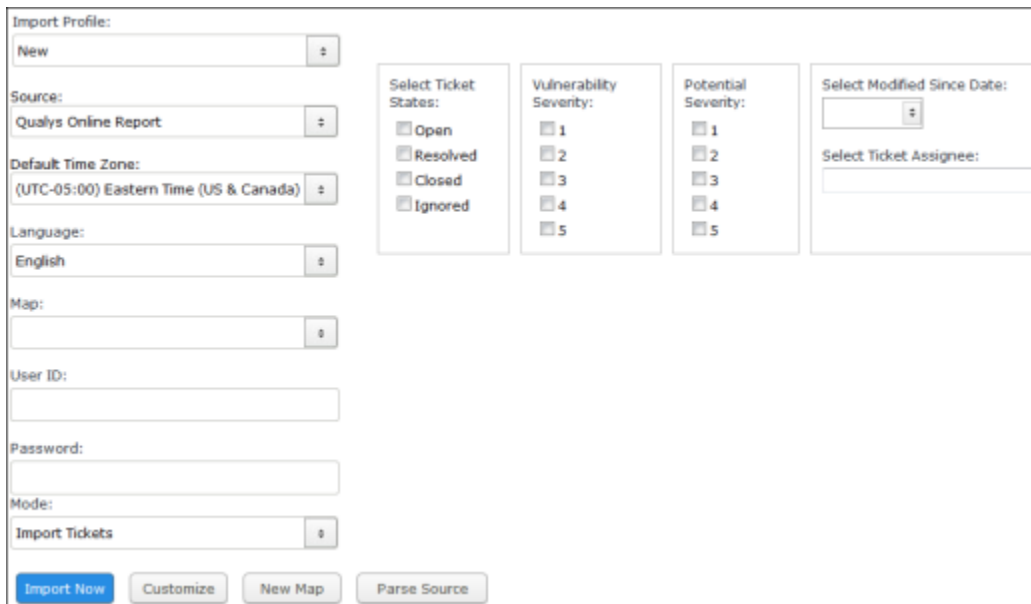
It is recommended to only select 'Open' to take advantage of Rsam's inherent dynamic workflow configuration. This will allow Rsam to automatically change the WF state of tickets that are no longer open. If other states are imported, handlers must be used to check the status and update the workflow state accordingly.

- **Ticket Status**

- o Open – Imports tickets with status of Open
- o Resolved – Imports tickets with status of Resolved
- o Closed – Imports tickets with status of Closed
- o Ignored – Imports tickets with status of Ignored

- **Vulnerability Severity** – Import tickets for Confirmed Vulnerabilities that match the selected severity rating

- **Potential Severity** – Import tickets for Potential Vulnerabilities that match the selected severity rating
- **Select Modified Since Date** – Import tickets that have been modified since the selected date. On subsequent imports, Rsam will automatically use the date of last import as the modified since date.
- **Select Ticket Assignee** – Import tickets specific to a ticket assignee by entering the user’s Qualys user ID



Importing using a Downloaded Qualys Results XML file

1. From the Qualys console, access the report you want to download in XML.
2. In the **Import Records** screen, select **XML file** from the **Source** drop-down list and browse to the downloaded file(s).

Import Profile:

Source:

Default Time Zone:

Language:

Map:

Source Location:

User ID:

Password:

UnCompress Compressed Files

File Path:

Importing Vulnerabilities for High-Volume Devices

Rsam offers the ability to summarize Qualys vulnerability data by QID for high-volume vulnerabilities typically associated with devices such as, workstations or network devices. The summary imports records under a static object and creates one record per vulnerability with a count of how many devices are affected by the vulnerability. It records the IP addresses and machine names of all affected devices to facilitate searches and reporting.

Any of the vulnerability import options discussed above can be used to create your data result set. The pre-defined [Qualys Summary XML \(v.1\)](#) map found in [Predefined Import Maps](#) is based on the Qualys Online Report - Import Vulnerabilities using Saved Reports import option.

As the high-volume vulnerability import map configuration differs slightly from standard vulnerability import maps, please refer to the "High-Volume Vulnerability Imports" supplemental document for more information.

All Objects by Type (nav) ▼

- IT Biomedical Device (1)
- IT Desktops (3)

Object Name ▲

- London Desktops
- New York Desktops
- Paris Desktops

Importing Qualys Knowledgebase

The Qualys Knowledgebase is imported into the Vulnerability KnowledgeBase library in Rsam, one record for each QID. Companies can supplement the imported data by adding custom attributes to this record type, such as modified severity ratings, recommended solutions or mitigating controls. The data will be displayed to the remediation teams when Qualys vulnerabilities are assigned. In addition, a specific QID can be flagged as a false positive that applies to the enterprise. This workflow state will perpetuate to all imported vulnerabilities matching that QID.

Note that you must import the Qualys Knowledgebase if using the Import Current Vulnerabilities import mode described above.

You can limit the data imported by applying optional filters based on patch availability, publication or modification date. You can also include PCI reasons in the output. All filters are cumulative.

- **Limit to Patchable Vulnerabilities** – Returns Knowledgebase entries marked as “Patch Available”
- **Show PCI Reasons** – Show reasons for passing or failing PCI compliance (requires the CVSS Scoring feature to be turned on in your Qualys subscription).
- **Modified Within Last x Days** – Returns Knowledgebase entries that have been modified within the specified number of days selected.
- **Published Within Last x Days** – Returns Knowledgebase entries that have been published within the specified number of days selected.

Import Profile:

Source:

Default Time Zone:

Language:

Map:

User ID:

Password:

Mode:

OPTIONAL FILTERS (Filters are cumulative)

Limit to Patchable Vulnerabilities
 Show PCI Reasons

Modified Within Last x Days:

Published Within Last x Days:

A pre-defined Rsam map can be found in [Predefined Import Maps](#). The map points to the TVM Data library object which will contain all Qualys Knowledgebase records. If you do not have this object in your database, please create an object of the SOAR Data object type and update the map accordingly.

The numeric **Patchable** value returned by Qualys is translated on the **Translate** tab to a checkbox value in the related **Patchable** attribute.

General Map Filter Action Unique ID Definition Translate Management				
XML TYPE	XML ELEMENT	PATH	ORIGINAL_VALUE	NEW VALUE
Element	PATCHABLE	/VULNS/VULN/	1	Yes
Element	PATCHABLE	/VULNS/VULN/	0	No

Importing Policy Compliance Data

Within the Import Records interface, you can import compliance data from the Qualys Online Report v2 source by using the following 2 options:

- **Import Compliance Controls** – Import compliance controls used for policy compliance assessments
- **Import Compliance Scan Results** – Imports compliance result data for the selected policies

Rsam's predefined mappings correspond to the available data returned. Mappings can be found in [Predefined Import Maps](#).

Qualys Online Report v2

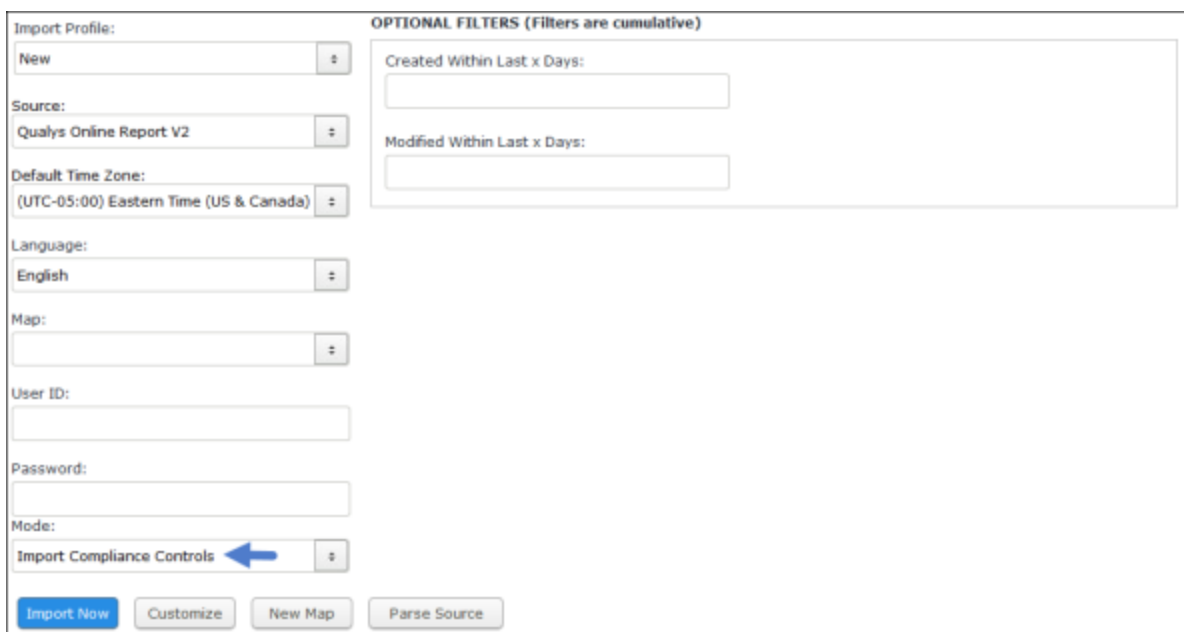
1. Select **Qualys Online Report v2** from the **Source** drop-down list.
2. Enter your user credentials in the **User ID** and **Password** fields.
3. Select any of the following import modes from the **Mode** drop-down list.
 - Import Compliance Controls
 - Import Compliance Scan Results

After selecting a mode, the screen is updated to provide a graphical interface for entering parameters used in filtering the data returned. Depending on the mode, the user will need to make a required selection and/or choose to select an 'Optional' filter. These screens and filters are described in the sections below.

Import Compliance Controls

Rsam will import all compliance controls in Qualys that the user account has permissions to. You can further limit the data imported by applying optional filters based on date the control was created or modified. All filters are cumulative.

- **Created Within Last x Days** – Returns controls that have been created within the specified number of days selected.
- **Modified Within Last x Days** – Returns controls that have been modified within the specified number of days selected.

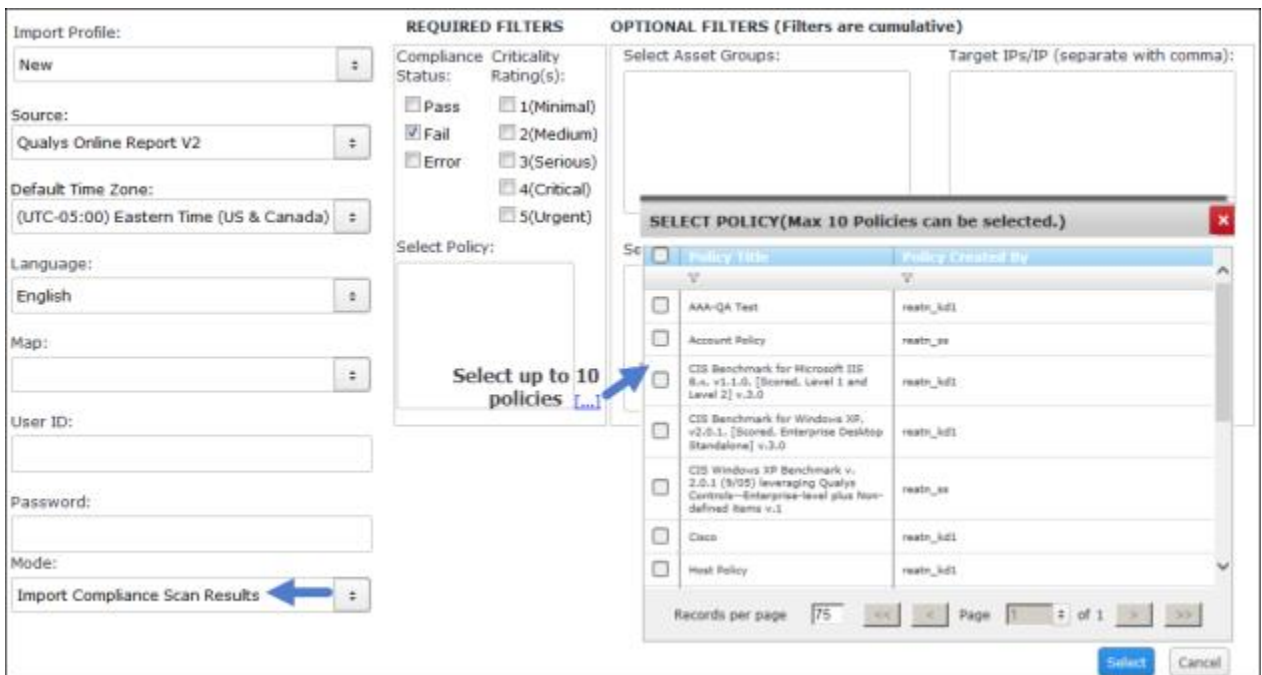


Import Compliance Scan Results

Rsam will import all compliance scan results in Qualys for assets that the user account has permissions to and which are assigned to a policy. The compliance status, criticality rating and policy are required and you can further limit the data imported by applying optional filters based on asset group, IP address, tags and days since compliance status update. All filters are cumulative.

- **Compliance Status** – You are required to select at least one compliance status.
- **Criticality Rating(s)** – You are required to select at least one criticality rating.
- **Select Policy** – Select up to a maximum of 10 policies that you want to import compliance scan results for.
 - a. Click the [\[...\]](#) select icon on the right side of the **Select Policy** field.
 - b. In the pop-up that opens, select the check boxes of the policies you want to filter your import. You can select up to a maximum of 10 policies.
 - c. Selected policies will be listed in the **Select Policy** field.
- **Select Asset groups** – Import compliance scan results for assets within the selected asset group(s). Compliance results will only be imported for these assets assigned to a policy selected above.
 - a. Click the [\[...\]](#) select icon on the right side of the **Select Asset Groups** field.

- b. In the pop-up that opens, select the desired asset group(s) and click **Select**.
- c. Selected asset group(s) will be listed in the **Select Asset Group** field.
- **Target IPs / IP** – Import compliance scan results that match the IP address entered or fall within an entered IP range.
 - o Enter specific IP addresses or an IP range. Separate values with a comma.
- **Select Tags** – Import compliance scan results for assets with the selected tag(s). Compliance results will only be imported for these assets assigned to a policy selected above.
 - a. Click the [\[...\]](#) select icon on the right side of the **Select Tags** field.
 - b. In the pop-up that opens, select the check boxes of the tags you want to filter your import. Selecting the check box next to **Tag Name** will select all tags.
 - c. Selected tags(s) will be listed in the **Select Tags** box.
- **Compliance Status Updated within Last x Days** – Returns compliance scan results for those that have updated within the specified number of days selected.



Managing Maps

Refer to [Appendix 1: Predefined Import Maps](#) for the list of predefined maps available for each import mode listed above.

For more information on reviewing and/or updating the predefined maps, refer to the document titled *Supplemental Integration Guide – Managing TVM Import Mappings*.

Appendix 1: Predefined Import Maps

Asset Import Maps

V: QUALYS_HOST_LIST_API (v.1)

Import Mode: Qualys Online Report v2 – Import Host List AND Import Host List Using Tags

Unique ID: SYS: Scanner Host ID

Rsam Attribute	Path
Object Name	/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/IP
SYS: Asset Group	/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/ASSET_GROUP_IDS
SYS: Asset Tracking Method	/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/TRACKING_METHOD
SYS: Instance ID (for cloud assets)	/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/EC2_INSTANCE_ID
SYS: Last Authenticated Scan Date	/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/LAST_VM_AUTH_SCANNED_DATE
SYS: Last Compliance Scan Date	/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/LAST_COMPLIANCE_SCAN_DATETIME
SYS: Last Scanned Date	/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/LAST_VULN_SCAN_DATETIME
SYS: Qualys GUID	/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/QG_HOSTID
SYS: Scanner Host ID	/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/ID
VM: Asset Tags	/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/TAGS/TAG/NAME
VM: Host IP Address	/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/IP
VM: Host Name - DNS	/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/DNS

Rsam Attribute	Path
VM: Host Name - NetBIOS	/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/NETBIOS
VM: Host OS	/HOST_LIST_OUTPUT/RESPONSE/HOST_LIST/HOST/OS

H: QUALYS_AUTHENTICATION_API (v.1)

Import Mode: Qualys Online Report v2 –Import Using Saved Report (Authentication Report Template)

Unique ID: Name

Rsam Attribute	Path
Object Name	/COMPLIANCE_AUTHENTICATION_REPORT/ASSET_GROUP_LIST/ASSET_GROUP/TECHNOLOGY_LIST/TECHNOLOGY/HOST_LIST/HOST/IP
SYS: Last Authenticated Scan Date	/COMPLIANCE_AUTHENTICATION_REPORT/ASSET_GROUP_LIST/ASSET_GROUP/TECHNOLOGY_LIST/TECHNOLOGY/HOST_LIST/HOST/LAST_SUCCESS
SYS: Failed Authentication Reason	/COMPLIANCE_AUTHENTICATION_REPORT/ASSET_GROUP_LIST/ASSET_GROUP/TECHNOLOGY_LIST/TECHNOLOGY/HOST_LIST/HOST/CAUSE
SYS: Authentication	/COMPLIANCE_AUTHENTICATION_REPORT/ASSET_GROUP_LIST/ASSET_GROUP/TECHNOLOGY_LIST/TECHNOLOGY/HOST_LIST/HOST/STATUS

H: QUALYS_ASSET_GROUP_API (v.1)

Import Mode: Qualys Online Report – Import Asset Groups

Unique ID: Name

Rsam Attribute	Path
Object Name	/ASSET_GROUP_LIST/ASSET_GROUP/SCANIPS/IP/
VM: Host Domain	/ASSET_GROUP_LIST/ASSET_GROUP/MAPDOMAINS/DOMAIN
VM: Host IP Address	/ASSET_GROUP_LIST/ASSET_GROUP/SCANIPS/IP/
SYS: Asset Group	/ASSET_GROUP_LIST/ASSET_GROUP/TITLE

H: QUALYS_ASSET_LIST_API (v.1)

Import Mode: Manually entered API Call - Asset IP List

Unique ID: Name

Rsam Attribute	Path
Object Name	/HOST_LIST/RESULTS/HOST/IP
VM: Host IP Address	/ASSET_SEARCH_REPORT/HOST_LIST/HOST/IP
VM: Host Name - DNS	/HOST_LIST/RESULTS/HOST/DNS
VM: Host Name - NetBIOS	/HOST_LIST/RESULTS/HOST/NETBIOS
SYS: System Description	/HOST_LIST/RESULTS/HOST/COMMENT/VALUE
VM: Host OS	/HOST_LIST/RESULTS/HOST/OPERATING_SYSTEM

H: QUALYS_ASSET_SEARCH_API (v.1)

Import Mode: Manually entered API Call - Asset Search

Unique ID: Name

Rsam Attribute	Path
Object Name	/ASSET_SEARCH_REPORT/HOST_LIST/HOST/IP
VM: Host IP Address	/ASSET_SEARCH_REPORT/HOST_LIST/HOST/IP
SYS: Asset Group	/ASSET_SEARCH_REPORT/HOST_LIST/HOST/ASSET_GROUPS/ASSET_GROUP_TITLE
VM: Host Name - DNS	/ASSET_SEARCH_REPORT/HOST_LIST/HOST/DNS
VM: Host Name - NetBIOS	/ASSET_SEARCH_REPORT/HOST_LIST/HOST/NETBIOS
SYS: Last Scanned Date	/ASSET_SEARCH_REPORT/HOST_LIST/HOST/LAST_SCAN_DATE
VM: Host OS	/ASSET_SEARCH_REPORT/HOST_LIST/HOST/OPERATING_SYSTEM

H: QUALYS_ASSET_IMPORT – Saved Report (v.1)

Import Mode: Downloaded Saved Report (XML)

Unique ID: Name

Rsam Attribute	Path
Object Name	/SCAN/IP/value
VM: Host IP Address	/SCAN/IP/value
VM: Host Name - DNS	/SCAN/IP/name
VM: Host OS	/SCAN/IP/OS
VM: Host Name - NetBIOS	/SCAN/IP/NETBIOS_HOSTNAME

H: QUALYS_ASSET_DATA_REPORT_API (v.1)

Import Mode: Downloaded Template (XML)

Unique ID: Name

Rsam Attribute	Path
Object Name	/ASSET_DATA_REPORT/HOST_LIST/HOST/IP
VM: Host IP Address	/ASSET_ DATA _REPORT/HOST_LIST/HOST/IP
SYS: Asset Group	/ASSET_ DATA _REPORT/HOST_LIST/HOST/ASSET_GROUPS/ASSET_GROUP_TITLE
VM: Host Name - DNS	/ASSET_ DATA _REPORT/HOST_LIST/HOST/DNS
VM: Host Name - NetBIOS	/ASSET_ DATA _REPORT/HOST_LIST/HOST/NETBIOS
VM: Host OS	/ASSET_ DATA _REPORT/HOST_LIST/HOST/OPERATING_SYSTEM
VM: Asset Tags	/ASSET_ DATA _REPORT/HOST_LIST/HOST/ASSET_TAGS/ASSET_TAG

Vulnerability Import Maps

V: QUALYS_CURRENT_VULN_API (v.1)

Import Mode: Qualys Online Report v2 –Import Current Vulnerabilities

Unique ID: Vulnerability ID + Port

Rsam Attribute	Path
Vulnerability - Qualys VM	/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/
VM: Actual Result	/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/RESULTS
VM: Date First Found	/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/FIRST_FOUND_DATETIME
VM: Date Last Found	/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/LAST_FOUND_DATETIME
VM: Lookup Vulnerability KB Entry	/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/QID
VM: Port	/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/PORT
VM: Protocol	/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/PROTOCOL
VM: Qualys Status	/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/STATUS
VM: Severity - Native (numeric)	/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/SEVERITY
VM: SSL	/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/SSL
VM: Vulnerability ID	/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/QID
VM: Vulnerability Type/Family	/HOST_LIST_VM_DETECTION_OUTPUT/RESPONSE/HOST_LIST/HOST/DETECTION_LIST/DETECTION/TYPE

V: Qualys_XML (v.3 – Saved Reports)

Import Mode: Qualys Online Report –Import Vulnerabilities using Saved Reports

Filters: Severity > 1

Unique ID: Vulnerability ID + Port

Rsam Attribute	Path
Vulnerability - Qualys VM	/SCAN/IP/VULNS/CAT/VULN
Vulnerability ID	/SCAN/IP/VULNS/CAT/VULN/number
Vulnerability Name	/SCAN/IP/VULNS/CAT/VULN/TITLE
Description	/SCAN/IP/VULNS/CAT/VULN/DIAGNOSIS
Fix/Resolution	/SCAN/IP/VULNS/CAT/VULN/SOLUTION
Reference - CVE	/SCAN/IP/VULNS/CAT/VULN/CVE_ID_LIST/CVE_ID/ID
Reference - Bugtraq	/SCAN/IP/VULNS/CAT/VULN/BUGTRAQ_ID_LIST/BUGTRAQ_ID/ID
Reference - Bugtraq - URL	/SCAN/IP/VULNS/CAT/VULN/BUGTRAQ_ID_LIST/BUGTRAQ_ID/URL
Reference - CVE URL	/SCAN/IP/VULNS/CAT/VULN/CVE_ID_LIST/CVE_ID/URL
Severity - Native (numeric)	/SCAN/IP/VULNS/CAT/VULN/severity
Risk	/SCAN/IP/VULNS/CAT/VULN/CONSEQUENCE
Actual Result	/SCAN/IP/VULNS/CAT/VULN/RESULT
Category	/SCAN/IP/VULNS/CAT/value
Scan ID	/SCAN/value
Port	/SCAN/IP/VULNS/CAT/port
Protocol	/SCAN/IP/VULNS/CAT/protocol
Exploit Source	/SCAN/IP/VULNS/CAT/VULN/CORRELATION/EXPLOITABILITY/EXPLT_SRC

V: QUALYS_XML (v.4 – Template)

Import Mode: Qualys Online Report –Import Vulnerabilities using Templates

Filters: Severity > 1

Unique ID: Vulnerability ID + Port + Protocol

Rsam Attribute	Path
CVSS: CVSS Base Score	/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CVSS_SCORE/CVSS_BASE
CVSS: CVSS Temporal Score	/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CVSS_SCORE/CVSS_TEMPORAL
VM: Category	/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CATEGORY
VM: Date First Found	/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/FIRST_FOUND
VM: Date Last Found	/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/LAST_FOUND
VM: Description	/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/THREAT
VM: Exploit Source	/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/CORRELATION/EXPLOITABILITY/EXPLT_SRC
VM: Fix/Resolution	/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/SOLUTION
VM: Host IP Address	/ASSET_DATA_REPORT/HOST_LIST/HOST/IP
VM: Host Name - DNS	/ASSET_DATA_REPORT/HOST_LIST/HOST/DNS
VM: Host OS	/ASSET_DATA_REPORT/HOST_LIST/HOST/OPERATING_SYSTEM
VM: Lookup Vulnerability KB Entry	/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/QID
VM: Port	/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/PORT

Rsam Attribute	Path
VM: Protocol	/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/P ROTOCOL
VM: Qualys Final CVSS Score	/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/C VSS_FINAL
VM: Qualys Status	/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/V ULN_STATUS
VM: Reference - Bugtraq	/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/B UGTRAQ_ID_LIST/BUGTRAQ_ID/ID
VM: Reference - Bugtraq - URL	/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/B UGTRAQ_ID_LIST/BUGTRAQ_ID/URL
VM: Related CVE Entries	/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/C VE_ID_LIST/CVE_ID/ID
VM: Risk	/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/I MPACT
VM: Service	/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/S ERVICE
VM: Severity - Native (numeric)	/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/S EVERITY
VM: Severity - PCI	/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/P CI_FLAG
VM: SSL	/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/S SL
VM: Times Found	/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/TI MES_FOUND
VM: Vulnerability ID	/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/Q ID
VM: Vulnerability Name	/ASSET_DATA_REPORT/GLOSSARY/VULN_DETAILS_LIST/VULN_DETAILS/TI TLE
VM: Vulnerability Type/Family	/ASSET_DATA_REPORT/HOST_LIST/HOST/VULN_INFO_LIST/VULN_INFO/T YPE

Qualys Ticket Maps

V: QUALYS _TICKET_XML (v.2)

Import Mode: Qualys Online Report –Import Tickets

Unique ID: Ticket Number

Rsam Attribute	Path
Vulnerability - Qualys Tickets	/REMIATION_TICKETS/TICKET_LIST/TICKET
Ticket Number	/REMIATION_TICKETS/TICKET_LIST/TICKET/NUMBER
Ticket Creation Date	/REMIATION_TICKETS/TICKET_LIST/TICKET/CREATION_DATETIME
Ticket Status	/REMIATION_TICKETS/TICKET_LIST/TICKET/CURRENT_STATE
Host IP Address	/REMIATION_TICKETS/TICKET_LIST/TICKET/DETECTION/IP
Host Name - DNS	/REMIATION_TICKETS/TICKET_LIST/TICKET/DETECTION/DNSNAME
Date Discovered	/REMIATION_TICKETS/TICKET_LIST/TICKET/STATS/FIRST_FOUND_DATETIME
Date Last Found	/REMIATION_TICKETS/TICKET_LIST/TICKET/STATS/LAST_FOUND_DATETIME
Last Scan Date	/REMIATION_TICKETS/TICKET_LIST/TICKET/STATS/LAST_SCAN_DATETIME
Vulnerability Name	/REMIATION_TICKETS/TICKET_LIST/TICKET/VULNINFO/TITLE
Vulnerability Type/Family	/REMIATION_TICKETS/TICKET_LIST/TICKET/VULNINFO/TYPE
Vulnerability ID	/REMIATION_TICKETS/TICKET_LIST/TICKET/VULNINFO/QID
Severity - Native (numeric)	/REMIATION_TICKETS/TICKET_LIST/TICKET/VULNINFO/SEVERITY
Reference - CVE	/REMIATION_TICKETS/TICKET_LIST/TICKET/VULNINFO/CVE_ID_LIST/CVE_ID

Qualys High-Volume Import Maps

V: QUALYS_SUMMARY_XML (v.1)

Import Mode: Qualys Online Report –Import Vulnerabilities using Saved Reports

Unique ID: Vulnerability ID + Port

Rsam Attribute	Path
Vulnerability - Qualys VM Summary	/SCAN/IP/VULNS/CAT/VULN
V: Vulnerability ID	/SCAN/IP/VULNS/CAT/VULN/number
V: Severity - Native (numeric)	/SCAN/IP/VULNS/CAT/VULN/severity
V: Vulnerability Name	/SCAN/IP/VULNS/CAT/VULN/TITLE
V: Category	/SCAN/IP/VULNS/CAT/value
V: Port	/SCAN/IP/VULNS/CAT/port
V: Protocol	/SCAN/IP/VULNS/CAT/protocol
V: Description	/SCAN/IP/VULNS/CAT/VULN/DIAGNOSIS
V: Risk	/SCAN/IP/VULNS/CAT/VULN/CONSEQUENCE
V: List of IP Addresses	/SCAN/IP/value
V: List of Machine Names	/SCAN/IP/name
V: Reference - CVE	/SCAN/IP/VULNS/CAT/VULN/CVE_ID_LIST/CVE_ID/ID
V: Reference - CVE URL	/SCAN/IP/VULNS/CAT/VULN/CVE_ID_LIST/CVE_ID/URL
V: Reference - Bugtraq	/SCAN/IP/VULNS/CAT/VULN/BUGTRAQ_ID_LIST/BUGTRAQ_ID/ID
V: Reference - Bugtraq - URL	/SCAN/IP/VULNS/CAT/VULN/BUGTRAQ_ID_LIST/BUGTRAQ_ID/URL
Exploit Source	/SCAN/IP/VULNS/CAT/VULN/VULN/CORRELATION/EXPLOITABILITY/EXPLT_SRC
Fix/Resolution	/SCAN/IP/VULNS/CAT/VULN/SOLUTION

Knowledgebase Import Maps

V: QUALYS_KB_API (v.1)

Import Mode: Qualys Online Report v2 – Import KnowledgeBase

Unique ID: VM: Vulnerability ID

Rsam Attribute	Path
CVSS: CVSS Access Complexity (AC)	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS/ACCESS/COMPLEXITY
CVSS: CVSS Access Vector (AV)	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS/ACCESS/VECTOR
CVSS: CVSS Authentication (AU)	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS/AUTHENTICATION
CVSS: CVSS Availability Impact (A)	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS/IMPACT/AVAILABILITY
CVSS: CVSS Base Score	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS/BASE
CVSS: CVSS Confidentiality Impact (C)	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS/IMPACT/CONFIDENTIALITY
CVSS: CVSS Exploitability (E)	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS/EXPLOITABILITY
CVSS: CVSS Integrity Impact (I)	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS/IMPACT/INTEGRITY
CVSS: CVSS Remediation Level (RL)	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS/REMEDIATION_LEVEL
CVSS: CVSS Report Confidence (RC)	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS/REPORT_CONFIDENCE
CVSS: CVSS Temporal Score	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS/TEMPORAL
CVSS3: Attack Complexity (AC)	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS_V3/ACCESS/COMPLEXITY

Rsam Attribute	Path
CVSS3: Attack Vector (AV)	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS_V3/ACCESS/VECTOR
CVSS3: Availability Impact (A)	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS_V3/IMPACT/AVAILABILITY
CVSS3: Confidentiality Impact (C)	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS_V3/IMPACT/CONFIDENTIALITY
CVSS3: CVSS3 Base Score	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS_V3/BASE
CVSS3: CVSS3 Temporal Score	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS_V3/TEMPORAL
CVSS3: Exploit Code Maturity (E)	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS_V3/EXPLOITABILITY
CVSS3: Integrity Impact (I)	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS_V3/IMPACT/INTEGRITY
CVSS3: Privileges Required (PR)	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS_V3/AUTHENTICATION
CVSS3: Remediation Level (RL)	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS_V3/REMEDIATION_LEVEL
CVSS3: Report Confidence (RC)	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVSS_V3/REPORT_CONFIDENCE
TVM: Vuln Software Name	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/SOFTWARE_LIST/SOFTWARE/PRODUCT
VM: Additional Vulnerability Information	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/DISCOVERY/ADDITIONAL_INFO
VM: Affected Products	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/VENDOR_REFERENCE_LIST/VENDOR_REFERENCE/ID
VM: Authentication Type	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/DISCOVERY/AUTH_TYPE_LIST/AUTH_TYPE

Rsam Attribute	Path
VM: Category	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CATEGORY
VM: Description	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/DIAGNOSIS
VM: Discovery Method	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/DISCOVERY/REMOTE
VM: Exploit Source	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CORRELATION/EXPLOITS/EXPLT_SRC
VM: Fix/Resolution	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/SOLUTION
VM: Malware Source	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CORRELATION/MALWARE/MW_SRC/SRC_NAME
VM: Patch Available?	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/PATCHABLE
VM: PCI Check	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/PCI_FLAG
VM: Reference - Bugtraq	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/BUGTRAQ_LIST/BUGTRAQ/ID
VM: Reference - Bugtraq - URL	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/BUGTRAQ_LIST/BUGTRAQ/URL
VM: Reference - Compliance	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/COMPLIANCE_LIST/COMPLIANCE
VM: Reference - CVE	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVE_LIST/CVE/ID
VM: Reference - CVE URL	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVE_LIST/CVE/URL
VM: Reference - General	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/VENDOR_REFERENCE_LIST/VENDOR_REFERENCE/URL

Rsam Attribute	Path
VM: Related CVE Entries	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CVE_LIST/CVE/ID
VM: Risk	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/CONSEQUENCE
VM: Severity - Native (numeric)	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/SEVERITY_LEVEL
VM: Vulnerability Check Modify Date	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/LAST_SERVICE_MODIFICATION_DATETIME
VM: Vulnerability Check Publish Date	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/PUBLISHED_DATETIME
VM: Vulnerability ID	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/QID
VM: Vulnerability Name	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/TITLE
VM: Vulnerability Type/Family	/KNOWLEDGE_BASE_VULN_LIST_OUTPUT/RESPONSE/VULN_LIST/VULN/VULN_TYPE

Compliance Import Maps

Compliance Results

V: QUALYS_PCM_API (v.1)

Import Mode: Qualys Online Report v2 –Import Compliance Scan Results

Unique ID: Vulnerability ID + Host ID + DP Name

Rsam Attribute	Path
Vulnerability – Qualys PCM	/POSTURE_INFO_LIST_OUTPUT/RESPONSE/POLICY/INFO_LIST/INFO/
VM: Actual Result	/POSTURE_INFO_LIST_OUTPUT/RESPONSE/POLICY/INFO_LIST/INFO/EVIDENCE/DPV_LIST/DPV/V
VM: Date Last Found	/POSTURE_INFO_LIST_OUTPUT/RESPONSE/POLICY/INFO_LIST/INFO/POSTURE_MODIFIED_DATE
VM: DP Description	/POSTURE_INFO_LIST_OUTPUT/RESPONSE/POLICY/GLOSSARY/DPD_LIST/DPD/DESC
VM: DP Name	/POSTURE_INFO_LIST_OUTPUT/RESPONSE/POLICY/INFO_LIST/INFO/EVIDENCE/DPV_LIST/DPV/LABEL
VM: Evaluation	/POSTURE_INFO_LIST_OUTPUT/RESPONSE/POLICY/INFO_LIST/INFO/EVIDENCE/BOOLEAN_EXPR
VM: Host ID	/POSTURE_INFO_LIST_OUTPUT/RESPONSE/POLICY/INFO_LIST/INFO/HOST_ID
VM: Instance	/POSTURE_INFO_LIST_OUTPUT/RESPONSE/POLICY/INFO_LIST/INFO/INSTANCE
VM: Lookup Vulnerability KB Entry	/POSTURE_INFO_LIST_OUTPUT/RESPONSE/POLICY/INFO_LIST/INFO/CONTROL_ID
VM: Qualys Status	/POSTURE_INFO_LIST_OUTPUT/RESPONSE/POLICY/INFO_LIST/INFO/STATUS
VM: Vulnerability ID	/POSTURE_INFO_LIST_OUTPUT/RESPONSE/POLICY/INFO_LIST/INFO/CONTROL_ID

Compliance Controls

V: QUALYS_CONTROLS_API (v.1)

Import Mode: Qualys Online Report v2 –Import Compliance Controls

Unique ID: Vulnerability ID

Rsam Attribute	Path
Vulnerability Knowledgebase	/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL
VM: Affected Products	/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/TECHNOLOGY/NAME
VM: Category	/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/SUB_CATEGORY
VM: Description	/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/STATEMENT
VM: Reference - General	/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/Framework_LIST/Framework
VM: Risk	/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/TECHNOLOGY_LIST/TECHNOLOGY/RATIONALE
VM: Severity - Native (numeric)	/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/CRITICALITY/VALUE
VM: Vulnerability Check Modify Date	/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/UPDATE_DATE
VM: Vulnerability Check Publish Date	/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/CREATED_DATE
VM: Vulnerability ID	/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/ID
VM: Vulnerability Name	/CONTROL_LIST_OUTPUT/RESPONSE/CONTROL_LIST/CONTROL/STATEMENT

Appendix 2: Qualys User Permissions

This section describes the excerpt of user roles and permissions for assets, vulnerabilities, compliance data, and knowledgebase from the Qualys APIv2 guide.

Importing Assets

The following table lists the user roles and their permissions for assets.

User Role	Permissions
Manager	View all scanned hosts in subscription
Auditor	View all scanned compliance hosts in subscription.
Unit Manager	View scanned hosts in user's business unit. To view compliance hosts, the Manage compliance permission must be granted to the user's account.
Scanner	View scanned hosts in user's account. To view compliance hosts, the Manage compliance permission must be granted to the user's account.
Reader	View scanned hosts in user's account. To view compliance hosts, the Manage compliance permission must be granted to the user's account.

Importing Vulnerabilities

The following table lists the user roles and their permissions for vulnerabilities.

User Role	Permissions
Manager	View all VM scanned hosts in subscription. Download all saved reports in subscription
Auditor	No permission to view VM scanned hosts.
Unit Manager	View VM scanned hosts in user's business unit. Download saved reports in user's business unit, including reports launched by the user and reports launched by other users in the same business unit.
Scanner	View VM scanned hosts in user's account. Download saved reports launched by the user.
Reader	View VM scanned hosts in user's account. Download saved reports launched by the user.

Importing Compliance Data

The following table lists the user roles and their permissions for compliance data.

User Role	Permissions
Manager	View all compliance controls. View all reports in subscription. View compliance postures for all hosts (IP address) in asset groups assigned to the selected policy.
Auditor	View all compliance controls. View all policy reports in subscription. View compliance postures for all hosts (IP address) in asset groups assigned to the selected policy.
Unit Manager	View all compliance controls. View reports in user's business unit, including reports launched by the user and reports launched by other users in the same business unit. View compliance postures for all hosts (IP address) in asset groups assigned to the selected policy, when the hosts are included in the user's business unit.
Scanner	View all compliance controls. View reports launched by the user. View compliance postures for all hosts (IP address) in asset groups assigned to the selected policy, when the hosts are included in the user's account.
Reader	View all compliance controls. View reports launched by the user. View compliance postures for all hosts (IP address) in asset groups assigned to the selected policy, when the hosts are included in the user's account.

Importing KnowledgeBase

The following table lists the user roles and their permissions for KnowledgeBase.

User Role	Permissions
Manager, Unit Manager, Scanner, Reader	Download vulnerability data from the KnowledgeBase.

Appendix 3: Qualys API Calls

This section outlines the number of API calls that Rsam makes for each action listed using the Qualys connectors. The total number of API calls made when setting up an import profile or scheduling the import is the sum of each action taken.

Action	Selection	# of API Calls
Selecting an Asset Group or Tag on any Import Profile Screen	Load asset group or tag screen = 1	1
Create New Map or Customize Map	Load data for map = 1	1
Preview Stats within map screen	Simulate import of data = 1	1
Import Hosts	Import data from map screen or scheduler = 1	2
Import Hosts using Tags	Import data from map screen or scheduler = 1	1
Import asset groups	Import data from map screen or scheduler = 1	1
Import Current Vulnerabilities	Import data from map screen or scheduler = 1	1
Import Using Saved Report	Select a saved report = 1 Import data from map screen or scheduler = 1	2
Import KnowledgeBase	Import data from map screen or scheduler = 1	1
Import Compliance Controls	Import data from map screen or scheduler = 1	1
Import Compliance Scan Results	Select a Policy = 1 Import data from map screen or scheduler = 1	2
Import Using Custom API Call	Import data from map screen or scheduler = 1	1
Import vulnerabilities using Templates	Selecting a Template = 1 Import data from map screen or scheduler = 1	2
Import vulnerabilities using Raw Data	Import data from map screen or scheduler = 1	1
Import Qualys Tickets	Import data from map screen or scheduler = 1	1

Appendix 4: Qualys Report Template Configuration

Qualys Saved Report

Saved reports are based on templates and can be configured as shown below:

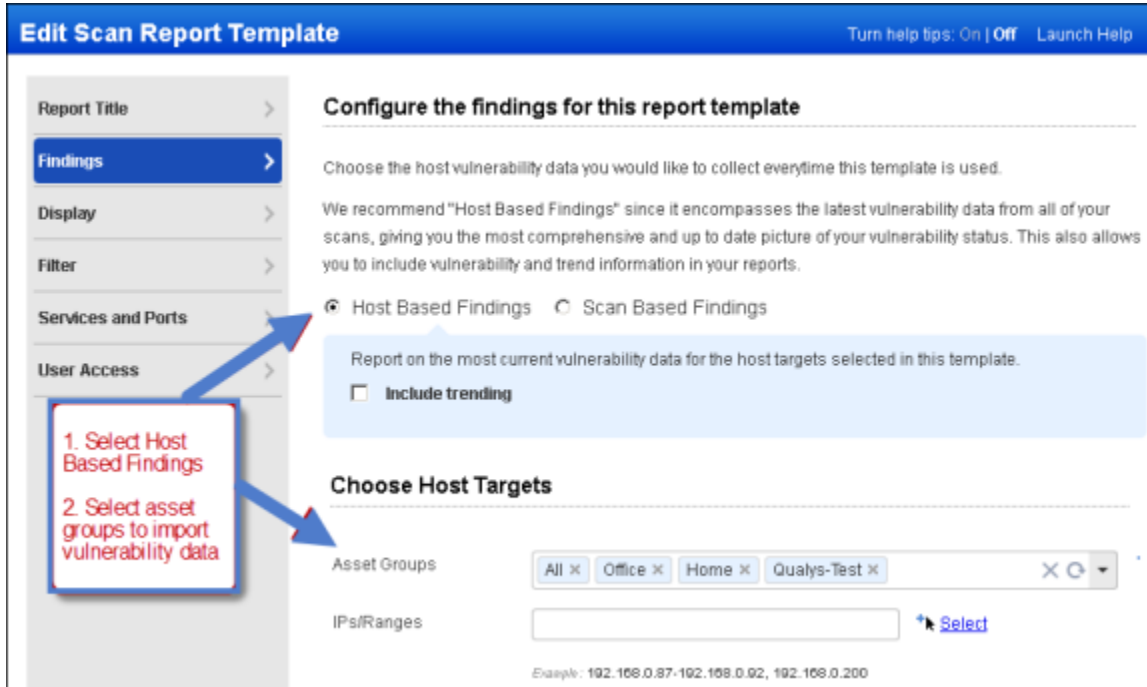
The screenshot shows the 'New Scan Report' configuration interface. It includes a title field with 'Confirmed Severity', a report template dropdown with 'Confirmed Severity 3 - 5', and a report format dropdown with 'Portable Document Format (PDF)'. The 'Report Source' section has 'Asset Groups' and 'IPs/Ranges' fields. A callout box with red text and blue arrows points to these fields, containing the instructions: 'Enter a name', 'Select a template', and 'Select the asset groups or IP addresses'.

After creating the report, you must run it on demand, or schedule it to run.

The 'Report Options' dialog box features a 'Scheduling' checkbox which is currently unchecked. At the bottom of the dialog are two buttons: 'Run' and 'Cancel'.

Qualys Template

The most common approach used for importing vulnerabilities is using Qualys Templates. Templates and can be configured as shown below:



Edit Scan Report Template Turn help tips: On | Off Launch Help

Report Title >

Findings >

Display >

Filter >

Services and Ports >

User Access >

Configure the findings for this report template

Choose the host vulnerability data you would like to collect everytime this template is used.

We recommend "Host Based Findings" since it encompasses the latest vulnerability data from all of your scans, giving you the most comprehensive and up to date picture of your vulnerability status. This also allows you to include vulnerability and trend information in your reports.

Host Based Findings Scan Based Findings

Report on the most current vulnerability data for the host targets selected in this template.

Include trending

Choose Host Targets

Asset Groups: All x Office x Home x Qualys-Test x

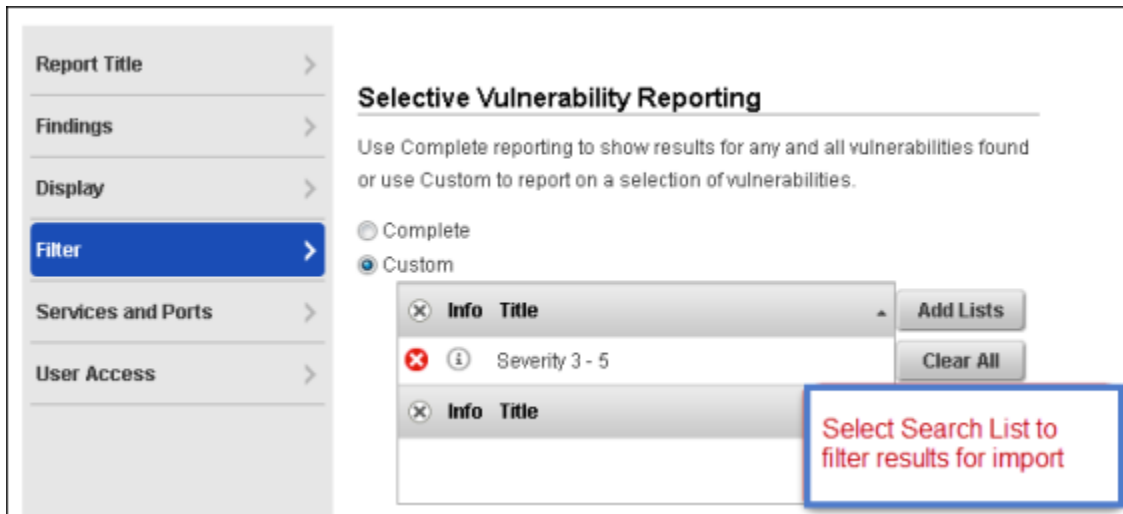
IPs/Ranges: [Select](#)

Example: 192.168.0.97-192.168.0.92, 192.168.0.200

1. Select Host Based Findings

2. Select asset groups to import vulnerability data

To optimize your imports, it is recommended to filter the data returned from Qualys as opposed to filtering the data in Rsam.



Report Title >

Findings >

Display >

Filter >

Services and Ports >

User Access >

Selective Vulnerability Reporting

Use Complete reporting to show results for any and all vulnerabilities found or use Custom to report on a selection of vulnerabilities.

Complete

Custom

Info Title

Severity 3 - 5

Info Title

Select Search List to filter results for import

Using a Search List to Filter on Vulnerabilities Imported

New Dynamic Vulnerability Search List

- General Information >
- List Criteria >
- Comments >

General Information

Title: *

Owner: *

New Dynamic Vulnerability Search List Launch Help

- General Information >
- List Criteria >
- Comments >

User Modified :

Published:

Confirmed Severity: Level 1 Level 2 Level 3 Level 4 Level 5

Potential Severity: Level 1 Level 2 Level 3 Level 4 Level 5

Information Severity: Level 1 Level 2 Level 3 Level 4 Level 5

Edit Scan Report Template Turn help tips: On | Off Launch Help

- Report Title >
- Findings >
- Display >**
- Filter >
- Services and Ports >
- User Access >

Report Summary

Select the components to be included in the report's summary section.

Summary of Vulnerabilities

Text Summary

Graphics

- Business Risk by Asset Group over Time
- Vulnerabilities by Severity over Time
- Vulnerabilities by Status
- Potential Vulnerabilities by Status
- Vulnerabilities by Severity
- Potential Vulnerabilities by Severity
- Information Gathered by Severity
- Top 5 Vulnerable Categories
- 10 Most Prevalent Vulnerabilities
- Operating Systems Detected
- Services Detected
- Ports Detected

Detailed Results

Sorting

Sort by: * Host

Include the following detailed results in the report

- Text Summary
- Vulnerability Details
 - Threat
 - Impact
 - Solution
 - Patches and Workarounds
 - Virtual Patches and Mitigating Controls
 - Compliance
 - Exploitability
 - Associated Malware
 - Results
 - Appendix

None of these options are required

Leave Host as the sorting option

Ensure all Vulnerability Details and Appendix options are selected. This ensures all vulnerability data is included in the Qualys data returned.

Text summary is not required.

Appendix 5: 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.

