

# Qualys Integration Guide

## Synack's Integration with Qualys Vulnerability Management

Last updated: Oct 2025

# Table of Contents

<b>Table of Contents</b>	<b>2</b>
<b>Synack Integration with Qualys</b>	<b>3</b>
Step 1: Get Credentials from Qualys	3
Step 2: Configure Qualys integration in Synack	3
<b>Viewing Vulnerabilities imported from Qualys in Synack</b>	<b>7</b>
Option 1 - Traditional SRT Workflow (default)	7
Option 2 - Sara Triage Workflow (new)	8
<b>Frequently Asked Questions</b>	<b>8</b>

# Synack Integration with Qualys

Synack's integration with Qualys allows customers to easily import vulnerabilities found by their Qualys Vulnerability Management (VM) scanning into their Synack Penetration Testing as a Service (PTaaS) Suspected Vulnerability / Scanner Findings list. Once in the Synack Suspected Vulnerability / Scanner Findings list, connections between the vulnerabilities and the vulnerable assets are made, enabling testing of those assets by the Synack Red Team (SRT) and/or Synack Autonomous Red Agent (Sara). Synack triages which vulnerabilities are truly exploitable, assesses exposure of vulnerable assets, and provides remediation recommendations and patch verification. Synack testing helps you close critical security gaps before bad actors can exploit them.

To get started with the integration configuration installation, follow the steps provided below.

## Step 1: Get Credentials from Qualys

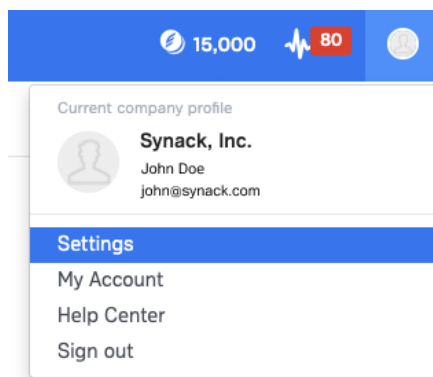
Ask your Qualys administrator to provide information which Synack's integration can use to create a connection between Qualys and Synack. You will need the following information before proceeding to next step;

- Username (note: User Role Manager is recommended, if Scanner or Reader Role is applied then scanned hosts must be assigned to the user using asset group(s). Allow access to API option must be checked for the user.)
- Password
- API URL (this differs from the Qualys Platform URL. The API Server URL can be found by the Qualys administrator in the Help -> About View -> Scanner Appliances section - it will be in format such as [qualysapi.xxx.qualys.com](http://qualysapi.xxx.qualys.com)). For further background about possible API Server URLs please [read here](#).

## Step 2: Configure Qualys integration in Synack

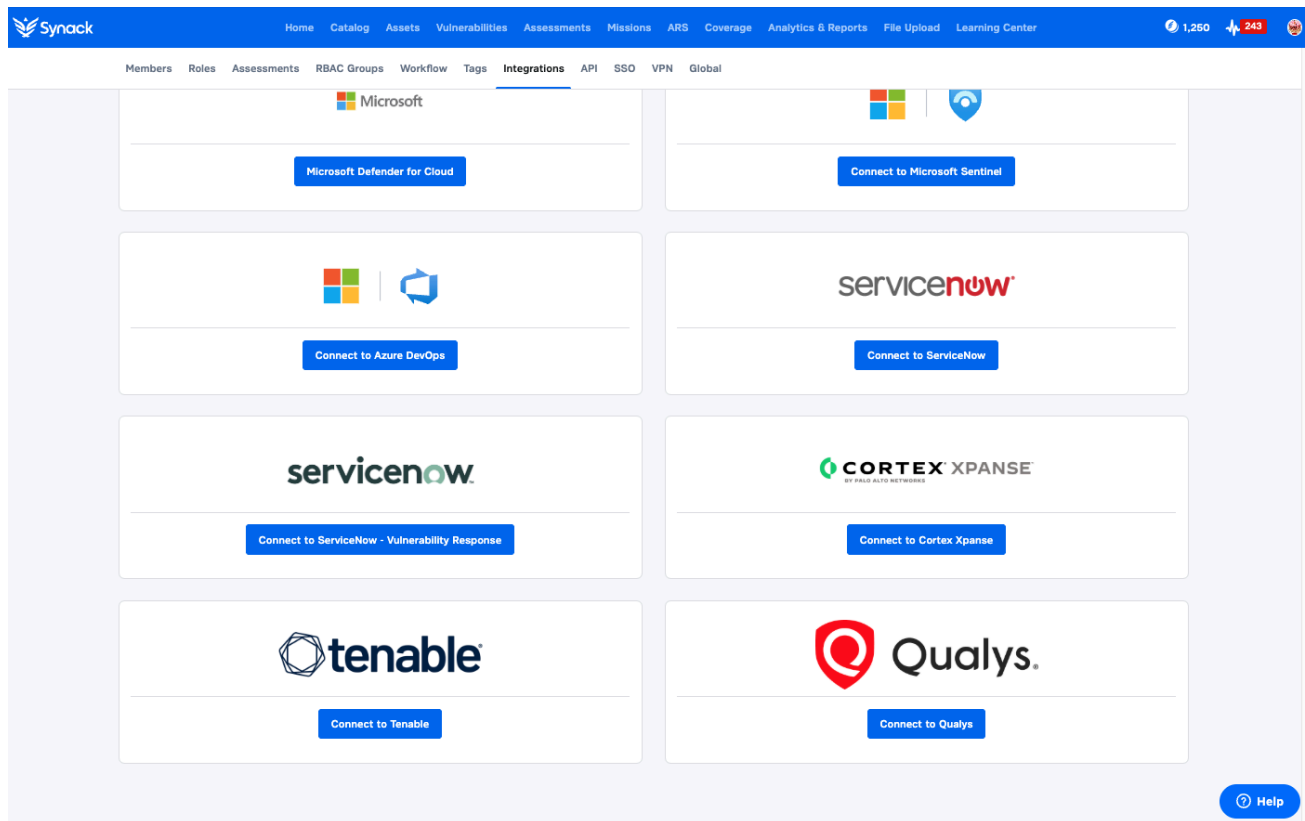
Login to the Synack Portal at <http://login.synack.com>

Click Profile Icon at Top Right corner of the Synack Portal, and then click Settings.



Next, click on the Integrations tab. Then click on the 'Connect to Qualys' button.

Note: your login must have a Synack Admin role in order to be able to configure Integrations.



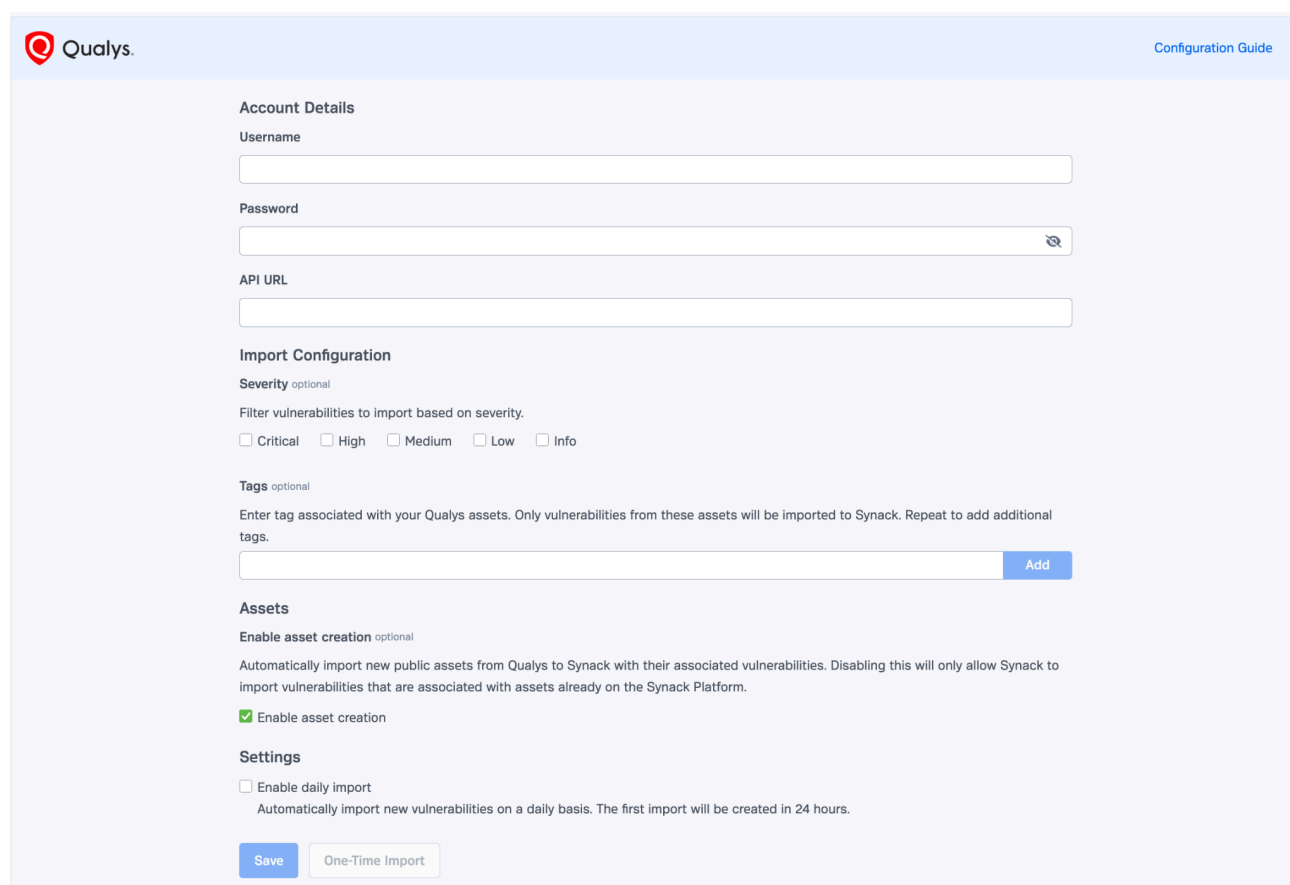
Enter the Username, Password, and API URL information which was provided by your Qualys admin.

*Optionally*, you can specify Asset Tags, and/or Vulnerability Severity from your Qualys implementation. These are used to limit scope of the vulnerability Import to a desired subset of Qualys vulnerabilities.

Note: if you omit these optional settings, Vulnerabilities imported ignore Tag and Severity values.

**Enable asset creation** (selected by default) - If a publicly accessible Host Asset is associated with a Qualys vulnerability scanning result, that Asset will be automatically added to the Synack Asset List (if it isn't already present). Host Assets in the Asset List are available for Synack Sara Triage, or testing by the SRT.

Note: if Enable asset creation is de-selected - Synack will only import Qualys vulnerabilities associated with assets already on the Synack Asset List (i.e. those Assets associated with existing Syntax Testing Assessments, or otherwise previously added to the Asset List.)



The screenshot shows the 'Qualys' configuration page within the Synack interface. The page is divided into several sections: 'Account Details', 'Import Configuration', 'Assets', and 'Settings'. In the 'Account Details' section, there are input fields for 'Username', 'Password' (with a toggle for visibility), and 'API URL'. The 'Import Configuration' section includes a 'Severity' filter (optional) with radio buttons for Critical, High, Medium, Low, and Info, and a 'Tags' section (optional) with a text input and an 'Add' button. The 'Assets' section features the 'Enable asset creation' checkbox, which is checked, and a descriptive text about importing public assets. The 'Settings' section has an 'Enable daily import' checkbox, which is unchecked, with a note about the first import occurring within 24 hours. At the bottom, there are 'Save' and 'One-Time Import' buttons.

You must then click 'Save' and your Qualys Integration configuration will be established.

Next you must initiate the Import of vulnerabilities from Qualys to Synack. From the Synack Platform's Qualys Integration screen where you just Saved your Qualys Account Details, you have 2 options to choose from:

- Option A) Click on the 'One-Time Import'
- Option B) Check 'Enable daily import', then click 'Save'

## Settings

☐ Enable daily import

Automatically import new vulnerabilities on a daily basis.

Save

One-Time Import

After several minutes, table will start to populate with Import History (note: Daily Import, or large One-Time imports may take longer to populate)

### Import History

Created	Activity	Status	Vulnerabilities Imported ⓘ
01/20/2022 10:41 AM	Daily Import	In Progress	--
01/20/2022 10:41 AM	Daily Import	Complete	10
01/19/2022 10:41 AM	Daily Import	Complete	50
01/18/2022 10:41 AM	One-Time Import	Complete	50

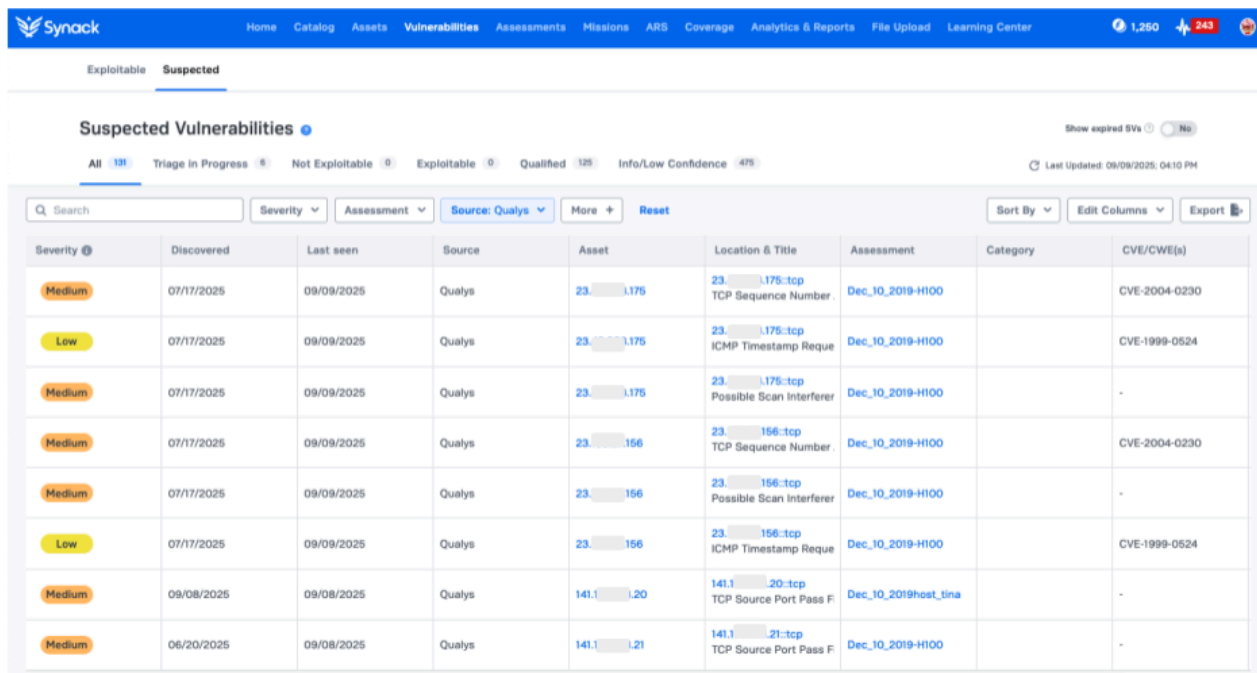
Showing 1-5 of 100

< 1 2 3 4 5 ... 9

# Viewing Vulnerabilities imported from Qualys in Synack

## Option 1 - Traditional SRT Workflow (default)

From the Synack Portal, click the 'Vulnerabilities' tab. Then click 'Suspected Vulnerabilities' (you may Search the Suspected Vulnerability List or filter it by 'Source' in order to see vulnerabilities that were imported by Qualys). Every vulnerability will be connected to an asset that may or may not be already included in an assessment. Assets that aren't in assessments can be added to new assessments. Once in an assessment, Synack can run Synack Penetration Tests, where human-led security testing by the Synack Red Team (SRT) can confirm and assess their exposure.



The screenshot shows the Synack web interface. The top navigation bar includes links for Home, Catalog, Assets, Vulnerabilities, Assessments, Missions, ARS, Coverage, Analytics & Reports, File Upload, and Learning Center. The 'Vulnerabilities' tab is active, and the 'Suspected' sub-tab is selected. The page title is 'Suspected Vulnerabilities'. Below the title, there are filters for 'All' (138), 'Triage in Progress' (5), 'Not Exploitable' (0), 'Exploitable' (0), 'Qualified' (125), and 'Info/Low Confidence' (475). A search bar and dropdown menus for 'Severity', 'Assessment', and 'Source: Qualys' are present. The table below lists the vulnerabilities with columns for Severity, Discovered, Last seen, Source, Asset, Location & Title, Assessment, Category, and CVE/CWE(s).

Severity	Discovered	Last seen	Source	Asset	Location & Title	Assessment	Category	CVE/CWE(s)
Medium	07/17/2025	09/09/2025	Qualys	23.175	23.175:tcp TCP Sequence Number	Dec_10_2019-H100		CVE-2004-0230
Low	07/17/2025	09/09/2025	Qualys	23.175	23.175:tcp ICMP Timestamp Reque	Dec_10_2019-H100		CVE-1999-0524
Medium	07/17/2025	09/09/2025	Qualys	23.175	23.175:tcp Possible Scan Interferer	Dec_10_2019-H100		-
Medium	07/17/2025	09/09/2025	Qualys	23.156	23.156:tcp TCP Sequence Number	Dec_10_2019-H100		CVE-2004-0230
Medium	07/17/2025	09/09/2025	Qualys	23.156	23.156:tcp Possible Scan Interferer	Dec_10_2019-H100		-
Low	07/17/2025	09/09/2025	Qualys	23.156	23.156:tcp ICMP Timestamp Reque	Dec_10_2019-H100		CVE-1999-0524
Medium	09/08/2025	09/08/2025	Qualys	141.1.20	141.1.20:tcp TCP Source Port Pass F	Dec_10_2019-H100		-
Medium	06/20/2025	09/08/2025	Qualys	141.1.21	141.1.21:tcp TCP Source Port Pass F	Dec_10_2019-H100		-

## Option 2 - Sara Triage Workflow (new)

Note: to use this Workflow, please request your Synack CSM to have you on-boarded to the Synack Autonomous Red Agent (Sara) program. Using Sara Triage, eligible Qualys sourced Vulns can be autonomously Triaged to confirm exploitability.

The screenshot displays the Synack 'Scanner Findings' page. At the top, a navigation bar includes links for Home, Catalog, Assets, Vulnerabilities, Assessments, Campaigns, ARS, Coverage, Reports, File Upload, and Learning Center. A user profile icon and a notification badge with '21' are also present. Below the navigation bar, the 'Scanner Findings' section is active, showing a summary of 365 findings. A workflow diagram indicates the process: 365 All findings are split into 346 Not Triaged and 15 Ineligible for Triage. The 346 Not Triaged findings move to Agent Review (1), then to Synack Review (1), and finally to a final status of 1 Exploitable, 1 Not Exploitable, and 0 Unreachable. Below the summary, there are tabs for Unique Vulnerabilities, CVE Clusters, and Software Clusters. A search bar and filters for Status and Source are available. A table lists various vulnerabilities with columns for Title & Location, Status, Discovered, Last Seen, Source, Severity, Asset, and CVE/CWE(s). The table shows several entries for Apache OFBiz Forced Browsing Vulnerability and Citrix NetScaler ADC and Gateway Buffer Overflow, with statuses ranging from Agent Review to Not Exploitable. A 'Submit for Sara Triage' button is located at the top right of the table. At the bottom, there is a pagination control showing 'Show rows per page' set to 25, with a total of 1-10 of 10 rows displayed.

Title & Location	Status	Discovered	Last Seen	Source	Severity	Asset	CVE/CWE(s)
Apache OFBiz Forced Browsing Vulnerability 192.168.1.28	Agent Review	06/25/2025	06/25/2025	Qualys	Critical	192.168.1.28	CVE-2011-2483 +7
Apache OFBiz Forced Browsing Vulnerability 192.168.1.28	Not Exploitable	06/25/2025	06/25/2025	Qualys	Critical	192.168.1.28	CVE-2013-3918
Apache OFBiz Forced Browsing Vulnerability 192.168.1.28	Synack Review	06/25/2025	06/25/2025	Qualys	Critical	192.168.1.28	CVE-2012-2688
Citrix NetScaler ADC and Gateway Buffer Overflow 192.168.1.29	Not Triaged	06/25/2025	06/25/2025	Qualys	High	192.168.1.29	CVE-2014-0160
Citrix NetScaler ADC and Gateway Buffer Overflow 192.168.1.42	Not Triaged	06/25/2025	06/25/2025	Qualys	High	192.168.1.42	CVE-2015-1635
PHP Remote Code Execution Vulnerability 192.168.1.67	Exploitable	06/25/2025	06/25/2025	Qualys	High	192.168.1.67	CVE-2016-0800
PHP Remote Code Execution Vulnerability 192.168.1.42	Not Triaged	06/25/2025	06/25/2025	Qualys	High	192.168.1.12	CVE-2017-0144
PHP Remote Code Execution Vulnerability 192.168.1.42	Not Triaged	06/25/2025	06/25/2025	Qualys	High	192.168.1.67	CVE-2018-11776
PHP Multiple Vulnerabilities Windows 192.168.1.67	Not Triaged	06/25/2025	06/25/2025	Qualys	High	192.168.1.42	CVE-2019-0708
PHP Multiple Vulnerabilities Windows 192.168.1.12	Not Triaged	06/25/2025	06/25/2025	Qualys	High	192.168.1.42	CVE-2020-0601

## Frequently Asked Questions

### What Qualys products does Synack integrate with?

The Synack Integration works with Qualys Vulnerability Management (VM), or Qualys Vulnerability Management Detection and Response (VMDR).

*Note: Synack's integration does NOT currently work with other Qualys scanning solutions such as Qualys TotalAppSec or Container Security*

### Why don't I see the Qualys choice in my Integrations page?

You must be a Synack Admin user to see the Integrations page.



## **I am a FedRAMP customer, can i use this integration?**

Yes, assuming you are using Qualys Government Platform. Note: In this case you will login to FedRAMP instance of the Synack Portal at <https://login.synack.us>

## **I followed the instructions in this guide, but I am still not able to see any data. How long should this take?**

If this is the initial configuration of the app, it can take some time for the initial data to be imported. Depending on the scope of vulnerabilities imported during 'One-Time Import' this can take anywhere from a minute to an hour. In the case of scheduled recurring imports, and depending on the time of day you 'Enable Daily Import' it may take up to 24 hours until the next daily import cycle kicks off.

## **Why don't i see some historical Qualys scanning results show up in Synack**

Qualys vulnerabilities that are more than 14 days old will not be imported into Synack. Note: however if a Vulnerable Asset is being scanned by Qualys Daily or Weekly, and an associated Vulnerability has not been successfully patched, then the 'Last Seen' date of that Vulnerability will have been refreshed and it will be imported.

## **I saw a vulnerability in my Synack Suspected Vulnerability list before, but now it's gone, why might that be?**

Once imported, Qualys vulnerabilities remain in Synack, but may not be displayed by default. By default only Suspected Vulnerabilities Last Seen within the last 14 days are displayed. To view current suspected vulnerabilities, as well as those Last Seen more than 14 days ago, enable Show Expired SVs.

## **I see vulnerabilities in Qualys, but I do not see them (or I only see some of them) imported into the Synack Suspected Vulnerability List, why might that be?**

The Synack Qualys Integration will only import vulnerabilities that are associated with assets that are present in the Asset List of the Synack Platform. Assets may be added to the Synack Platform via Synack Attack Surface Discovery, Palo Xpanse ASM Integration, Assessment creation, or manual Add. **Note:** you may also specify 'Enable asset creation' in the configuration of the Qualys integration, in which case publicly accessible assets which are associated with Qualys vulnerability management scanning results will be automatically added to the Synack Asset List, however this method will not add Internal Assets.

## **The number of Vulnerabilities reported in my Qualys VM platform differs from the number of Suspected Vulnerabilities reported in Synack, why?**

The manner in which Qualys and Synack report vulnerabilities may differ. Depending on the view, Qualys may report the vulnerability count as the number of uniquely vulnerable assets impacts, each of which may be impacted by multiple CVEs. Synack on the other hand counts every vulnerability individually, even when associated with the same asset. Thus, even when comparing for the same number of Assets, the count of Vulnerabilities imported into Synack may exceed what is reported in Qualys.

## **I am still having trouble with my Synack Qualys integration, who do I contact?**

Please reach out to [help@synack.com](mailto:help@synack.com)