

Qualys Integration Guide

Synack's Integration with Qualys
Vulnerability Management

Last updated: Nov 2025

Table of Contents

Table of Contents	2
Synack Integration with Qualys	3
Step 1: Get Credentials from Qualys	3
Step 2: Configure Qualys integration in Synack	3
Engaging Vulnerabilities imported from Qualys in Synack	7
Frequently Asked Questions	8

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) Scanner Findings list. Once in the 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).

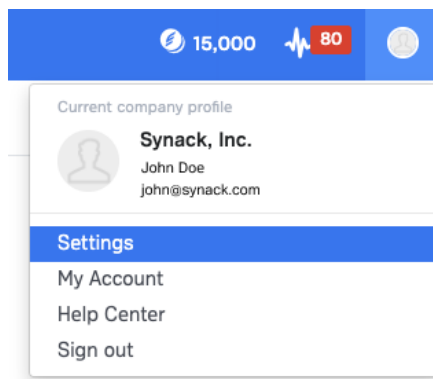
For further background about possible API Server URLs please [read here](#).

Please Note: integration is validated with Qualys Cloud Platforms, if you are using Private Platform please contact help@synack.com to request that your Domain be whitelisted for Synack integration.

Step 2: Configure Qualys integration in Synack

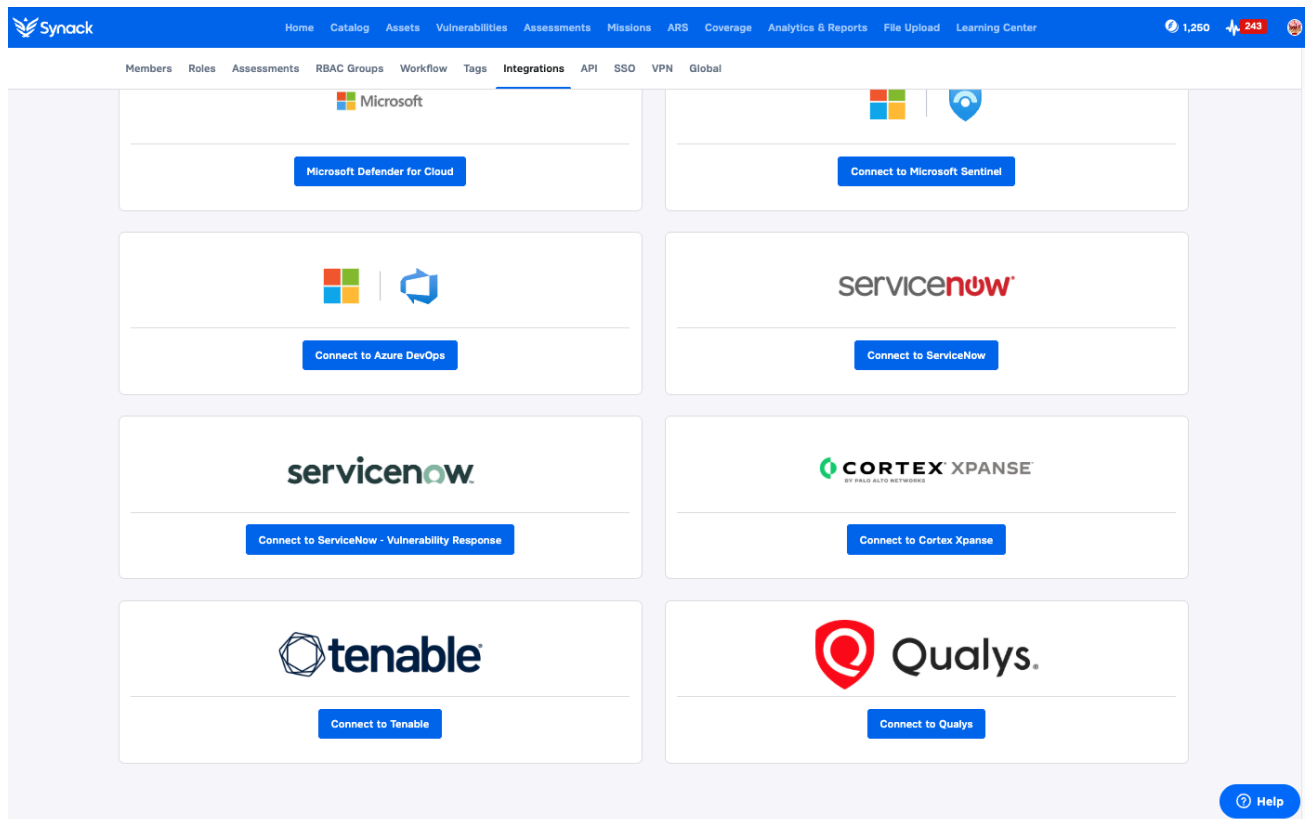
Login to the Synack Portal at <http://login.synack.com>

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' Vulnerability Management button.

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



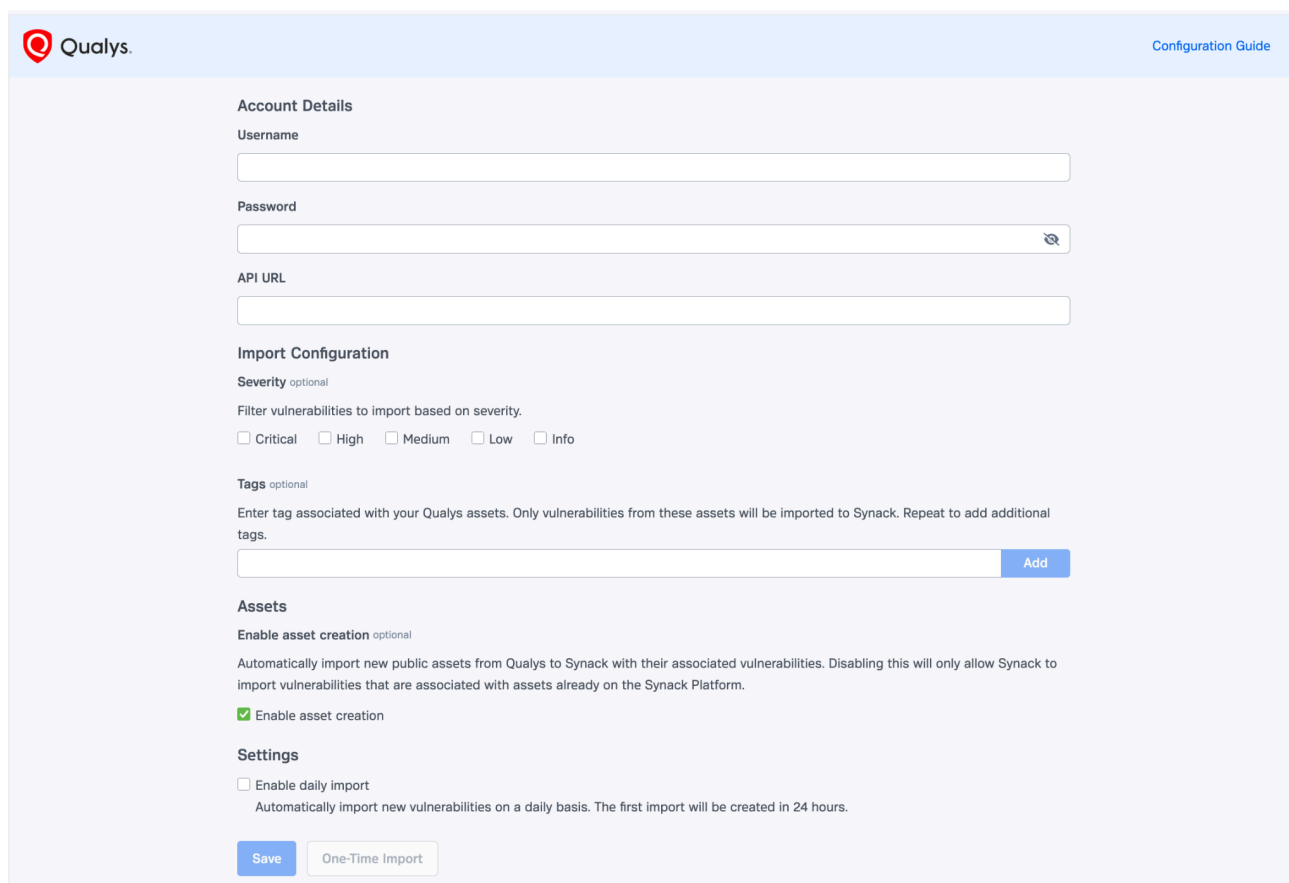
Enter the Username, Password, and API URL information which was provided by your Qualys admin.

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 in the Synack interface. The page is titled 'Qualys' and includes a 'Configuration Guide' link in the top right corner. The configuration is organized into several sections:

- Account Details:** Includes input fields for 'Username', 'Password' (with a visibility toggle), and 'API URL'.
- Import Configuration:**
 - Severity optional:** A section with the instruction 'Filter vulnerabilities to import based on severity.' and radio buttons for 'Critical', 'High', 'Medium', 'Low', and 'Info'.
 - Tags optional:** A section with the instruction 'Enter tag associated with your Qualys assets. Only vulnerabilities from these assets will be imported to Synack. Repeat to add additional tags.' and an input field with an 'Add' button.
- Assets:** Includes the option 'Enable asset creation optional', which is checked. Below it, a note states: 'Automatically import new public assets from Qualys to Synack with their associated vulnerabilities. Disabling this will only allow Synack to import vulnerabilities that are associated with assets already on the Synack Platform.'
- Settings:** Includes the option 'Enable daily import', which is unchecked. Below it, a note states: 'Automatically import new vulnerabilities on a daily basis. The first import will be created in 24 hours.'

At the bottom of the form, there are two buttons: 'Save' and 'One-Time Import'.

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

Engaging Vulnerabilities imported from Qualys in Synack

From the Synack Portal, click the 'Vulnerabilities' tab. Then click 'Scanner Findings'. You may Search the Scanner Findings List or apply filters such as Asset, Category. Every vulnerability will be associated with 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 test the associated assets to confirm and assess their security exposure. Test offerings include human-led testing by the Synack Red Team, or AI supported testing and triage by Synack Autonomous Red Agent (Sara). Please consult with your Synack team if you would like guidance on our test offerings.

Scanner Findings Last updated: 01/01/2022, 12:00 PM

Scanner Findings are vulnerabilities that are discovered by scanners. The exploitability of Scanner Findings can be determined by Synack's Autonomous Red Agent (SARA). Select one, or multiple vulnerabilities, to submit for Sara Triage. Sara will test the vulnerabilities for exploitability and the results will be verified by Synack's Vulnerability Operations team.

365
All

346
Not Triaged

15
Ineligible for Triage

1
Agent Review

1
Synack Review

1 Exploitable

1 Not Exploitable

0 Unreachable

Unique Vulnerabilities
CVE Clusters
Software Clusters
Submit for Sara Triage

Status Source More +
Sort By Edit Columns Export

<input type="checkbox"/>	Title & Location	Status	Discovered	Last Seen	Source	Severity	Asset	CVE/CWE(s)
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	Citrix NetScaler ADC and Gateway Buffe... 192.168.1.29	Not Triaged	06/25/2025	06/25/2025	Qualys	High	192.168.1.29	CVE-2014-0160
<input type="checkbox"/>	Citrix NetScaler ADC and Gateway Buffe... 192.168.1.42	Not Triaged	06/25/2025	06/25/2025	Qualys	High	192.168.1.42	CVE-2015-1635
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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

Show rows per page 25 1-10 of 10
< 1 >

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 (VM DR).

Note: there is a separate integration guide documenting Synack integration with Qualys Web Application Scanning (WAS)

Note: Synack's integration does NOT currently work with other Qualys scanning solutions such as Qualys 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.

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