Tenable Integration Guide

Synack’s Integration with Tenable

Last updated: March 2025

Table of Contents

Synack Integration with Tenable

Synack's integration with Tenable allows customers to easily import vulnerabilities found by their Tenable Vulnerability Management (VM) scanning into their Synack Penetration Testing as a Service (PTaaS) Suspected Vulnerability list. Once in the Synack Suspected Vulnerability List, connections between the vulnerabilities and the vulnerable assets are made.

(note: Synack will only import Tenable Vulnerabilities associated with Assets that are already present in the Synack Asset List. Please consult with Synack for details on how to populate your Synack Asset List.)

Assets with Suspected Vulnerabilities can then be included in Synack Penetration Tests, where human-led security testing by the Synack Red Team (SRT) can confirm and assess their exposure, and provide remediation recommendations and patch verification. Synack testing helps you find Exploitable Vulnerabilities before bad-actors do.

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

Step 1: Get Credentials from Tenable

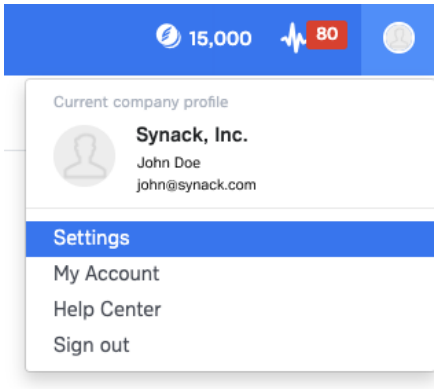
Ask your Tenable administrator to generate / provide you an Access Key and a Secret Key, which Synack's integration can use to create a connection between Tenable and Synack. You will need the following information before proceeding to next step;

- Access Key
- Secret Key

Step 2: Configure Tenable integration in Synack

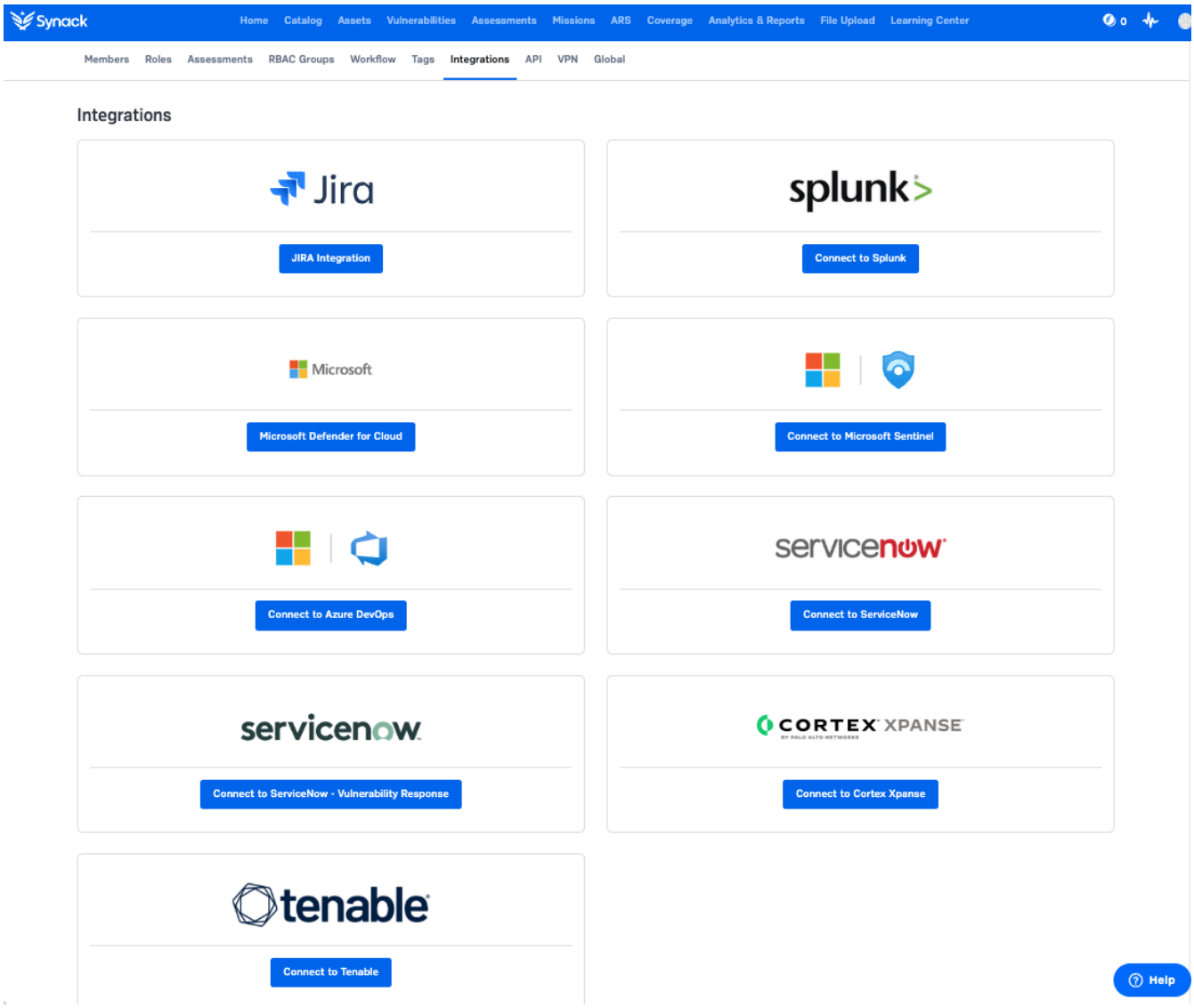
Login to the Synack Portal at http://login.synack.com

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

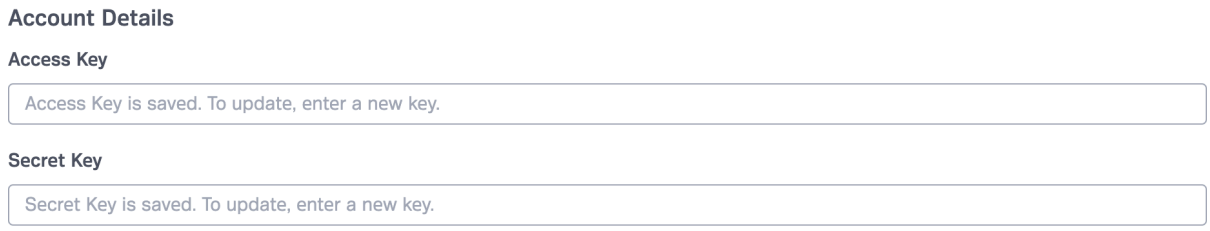


Next, click on the Integrations tab. Then click on the ‘Connect to Tenable’ button.

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



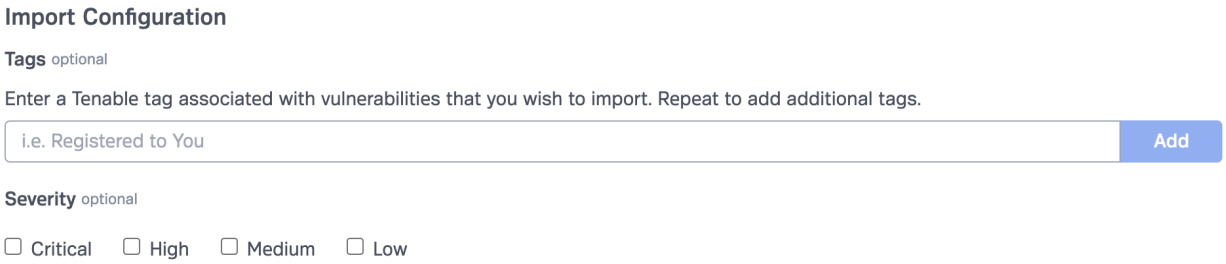
Enter the Access Key and Secret Key information which was provided by your Tenable admin.



You can then click ‘Save’ and your Tenable Integration will be established.

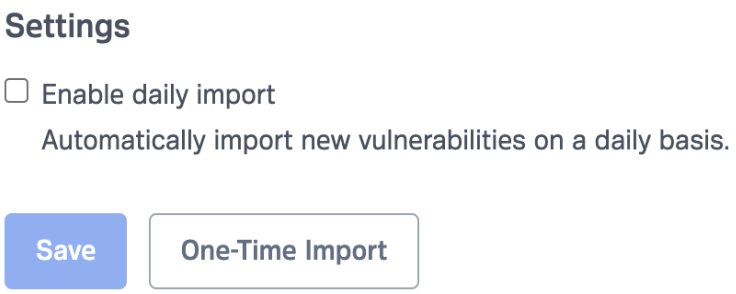
Optionally, you can specify Asset Tags used in your Tenable implementation, or vulnerability severity. These are used to limit scope of the vulnerability Import to a desired subset of Tenable vulnerabilities. If you make changes to these settings click ‘Save’ afterwards.

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

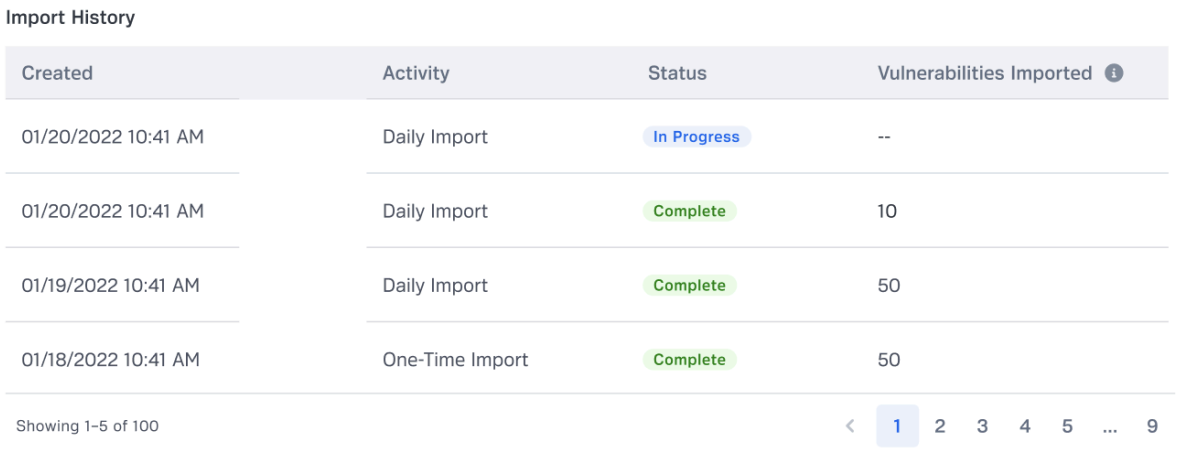


Next you must initiate the Import of vulnerabilities from Tenable to Synack. From the Synack Platform’s Tenable Integration screen where you just Saved your Tenable Account Details, you have 2 options to choose from:

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

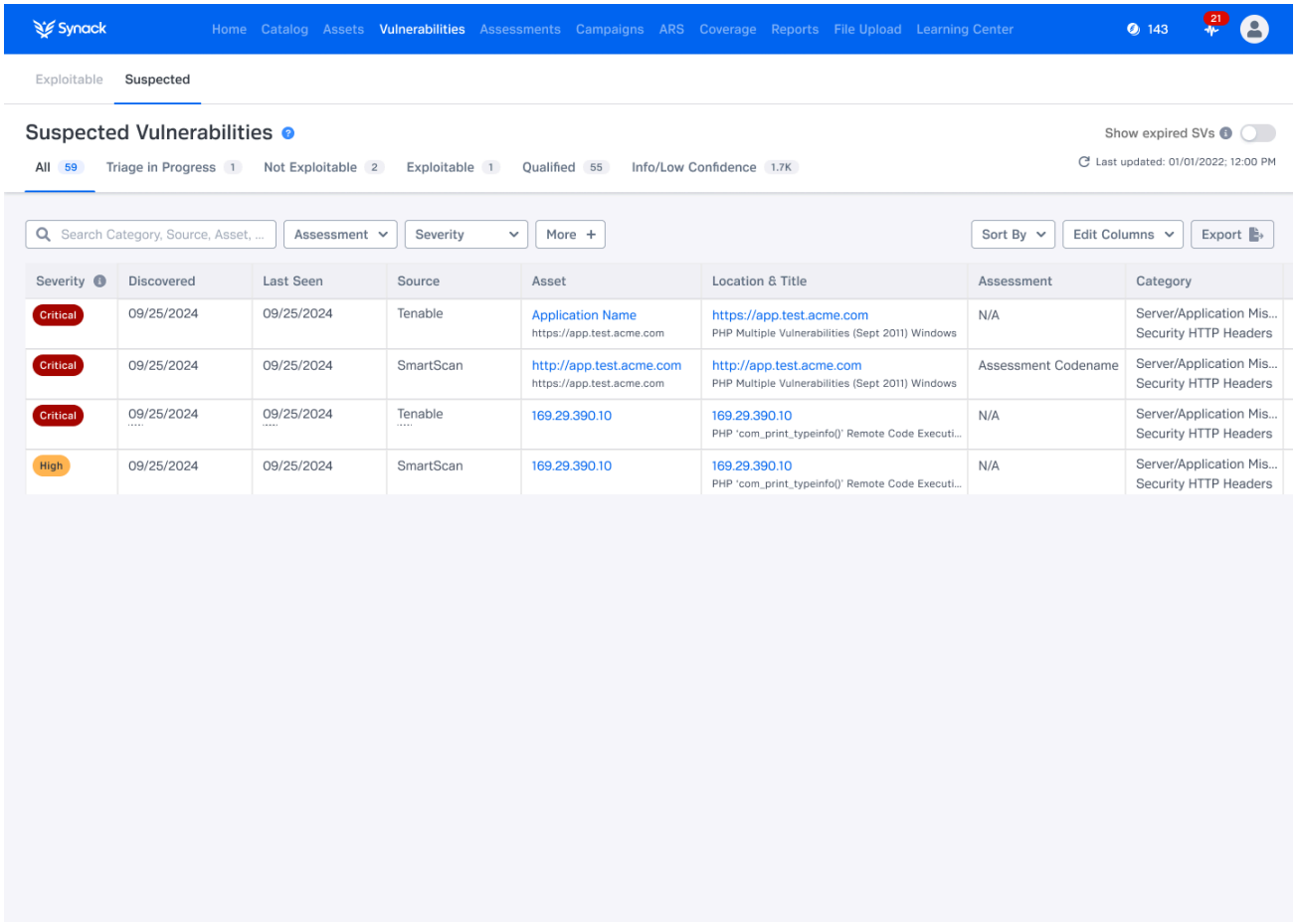


After several minutes, table will start to populate with Import History (note: Daily Import, or large One-Time imports may take significantly longer to populate)



Viewing Vulnerabilities imported from Tenable in Synack

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 Tenable). 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.



Frequently Asked Questions

I'm an Admin user, why don't I see the Tenable choice in my Integrations page?

Tenable is a new integration, and it may not yet have been made visible in your Synack portal. If you are a Synack Admin user and you don't see the Tenable tile in your Integrations page, please contact your Synack CSM or help@synack.com and request access to the Tenable integration.

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

Please contact Synack at help-gov@synack.us for further guidance.

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 several minutes to several hours. 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.

My integration used to work but I am no longer able to import vulnerabilities.

If you see a Failed Import message, this could be because of the API token being expired or being inadvertently deleted. Please check the Tenable platform to verify the API token still exists and is active. (if the token has expired or was deleted, you will need obtain a new token from Tenable, and then re-configure the Synack Integration for Tenable with a valid API Token and Keys)

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

By default only Suspected Vulnerabilities detected within the last 14 days are displayed. To view current suspected vulnerabilities, as well as those that haven't been detected in the last 14 days, enable Show Expired SVs.

Yesterday's Daily Import shows 100 vulnerabilities in the Import History, but today's import only shows 15, why might that be?

Only newly discovered (not previously present) Tenable vulnerabilities get added to the Synack Suspected Vulnerability List and are reflected in the daily Import History counter.

I see vulnerabilities in Tenable, 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 Tenable Integration will only import vulnerabilities that are associated with assets that you have already added to the Synack platform. If Tenable discovers a vulnerability that is associated with an asset that is not in the Synack Asset List, then the Synack Tenable Integration will not import that vulnerability. Note: Please consult with Synack for details on how to populate your Synack Asset List.

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

The manner in which Tenable and Synack report vulnerabilities differ. Tenable reports 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 Tenable.

I am still having trouble with my Synack Tenable integration, who do I contact?

Please reach out to help@synack.com