

JIRA CLOUD INTEGRATION GUIDE

Synack's Integration with
Jira Cloud

May 2024



Index

Synack Integration for Jira	3
Step 1: Synack API Token Generation	3
Step 2: Install the App	4
Step 3: Configure Connection to Synack	4
Step 4: Configure Synchronization	5
Method 1: Security feature workflow	5
Method 2: Traditional workflow	10
Method 3: Combined	12
Project Synchronization Settings	13
Patch Verification Flow	18
Troubleshooting	20
Frequently Asked Questions	21
Which IP address should be used to generate the API token for the Jira Cloud app?	21
Can I use this integration with different projects within Jira?	21
Can I use multiple Jira instances?	21
Can I use Jira and ServiceNow integrations together?	21
Comments are posted to Synack under the name of the user that generated the API token. What can I do to fix this?	22
What is the resolved_at date field?	22

Synack Integration for Jira

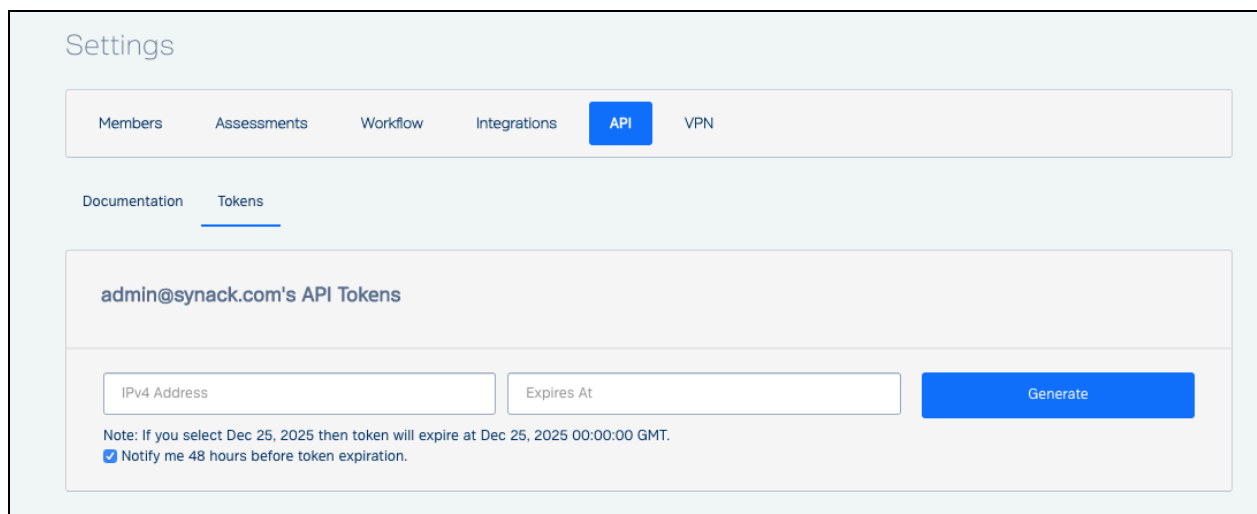
Synack Integration for Jira is used to create and sync Jira issues based on Synack vulnerabilities. This guide has been designed to describe the configuration steps required to configure this add-on on Jira Cloud.

Step 1: Synack API Token Generation

After logging into the Synack Customer Portal as a Super Admin user, navigate to Settings. Click on API and open the Tokens page.

It is important that the token is generated by a user who has write access to Synack assessments and vulnerabilities. The vulnerability information will be fetched from Synack on using that user's permissions. Updates of vulnerability statuses and comments will be posted to Synack on behalf of that user as well.

Note: Rather than using an individual user's account to generate the token, we recommend that you create a new user in the Synack portal specifically to generate the API token with that account. That account must have RBAC access to all relevant assessments.



The screenshot shows the 'Settings' page in the Synack Customer Portal. The 'API' tab is selected under the 'Integrations' section. The 'Tokens' sub-tab is active. The page displays 'admin@synack.com's API Tokens'. There are two input fields: 'IPv4 Address' and 'Expires At'. A blue 'Generate' button is positioned to the right of the 'Expires At' field. Below the fields, a note states: 'Note: If you select Dec 25, 2025 then token will expire at Dec 25, 2025 00:00:00 GMT.' A checkbox labeled 'Notify me 48 hours before token expiration.' is checked.

The IPv4 Address field allows restricting your token to a particular IP address(es). If you use a wildcard * - API requests to Synack from anywhere will be allowed with this token. If you specify an IP address in that field when generating the token - only API requests from this IP will be allowed with this token.

If you are using Jira Cloud, here is the IP address to generate the API token: 34.145.166.47. Wildcards are supported for the IPv4 field. Please also define an expiration date for this token.

Click generate and copy the token. You will be needing this later during the setup process. If you lose the token, you can always come back to this page to copy it again.

Step 2: Install the App

Please follow the [installation steps](#) listed on this Atlassian marketplace listing.

Step 3: Configure Connection to Synack

To access the Configuration Page you need to have administrative permission and access to manage add-ons on your Jira instance. Go to Jira Settings -> Manage Apps -> Configure Synack

After the app is installed, use the following details to configure the connection with the Synack API server.

Configure Integration between Synack and Jira

Connection to Synack

URL

TOKEN

Allow Send Statistics ▼
Allow sending usage statistics

An explanation is provided of each connection setting field below.

Setting	Description
URL	Please enter https://api.synack.com
Token	The Synack API token is used to get and update the vulnerability data. <ul style="list-style-type: none">• Token cannot be empty and must not be expired• Token needs to be generated by a user with write access

	<ul style="list-style-type: none"> If you are using Jira Cloud, please use this IP address to generate the API token: 34.145.166.47 <p>If you need more information on API token generation, please refer to the documentation at help.synack.com (<i>requires logging into the Synack Client Portal to gain access to all help desk articles</i>).</p>
Allow Send Statistics	Enabling this setting will share non-confidential data with Synack, which will help us debug any issues and collect stats such as how many sync jobs were executed, how many patches were requested, etc.
Test Connection	Test if the connection between Jira and the Synack system is working. Any problem with the connection or token will show an error message. You can test the connection settings without saving the configuration.

Don't forget to 'Save Settings' before leaving this page.

Step 4: Configure Synchronization

There are 2 ways to bring Synack vulnerabilities to your Jira.

The first option (Method 1) is to use the [Security](#) feature for Jira Cloud. Synack is one of the vendors supported by Atlassian to provide this feature. With this approach, Synack integration app creates Vulnerability records in Jira for your Synack Vulnerabilities. (Jira Issues may then be created manually as needed via the Security Vulnerabilities list.)

The second option (Method 2) is to create/update Jira issues automatically for your Synack Vulnerabilities. This is the traditional Jira workflow, and does not involve the Security feature in Jira Cloud.

You can use either of the 2 methods, or combine both at the same time. The combined approach creates both Jira Vulnerabilities and Issues, and links them together automatically.

Method 1: Security feature workflow

Synack integration app will create Jira Vulnerabilities in your Jira instance and keep them updated.

First, please enable the Security feature in your desired Jira Project(s). (Note: Jira's Security feature is described [here](#))

1. From your project's sidebar, go to Project settings > Features.
2. Toggle the Security feature on.


In your Jira project, go to Project Settings -> Apps -> Synack integration and select “Vulnerabilities” in the “Create in Jira” field.

Select the list of Assessments that you want to synchronize - vulnerabilities from these assessments will be created as Vulnerabilities in Jira. Make sure you save the settings.


Synack Integration

General Synchronize

Create in Jira



Vulnerabilities 

Sync Mode

Automatic 

every minutes

Synack Assessments

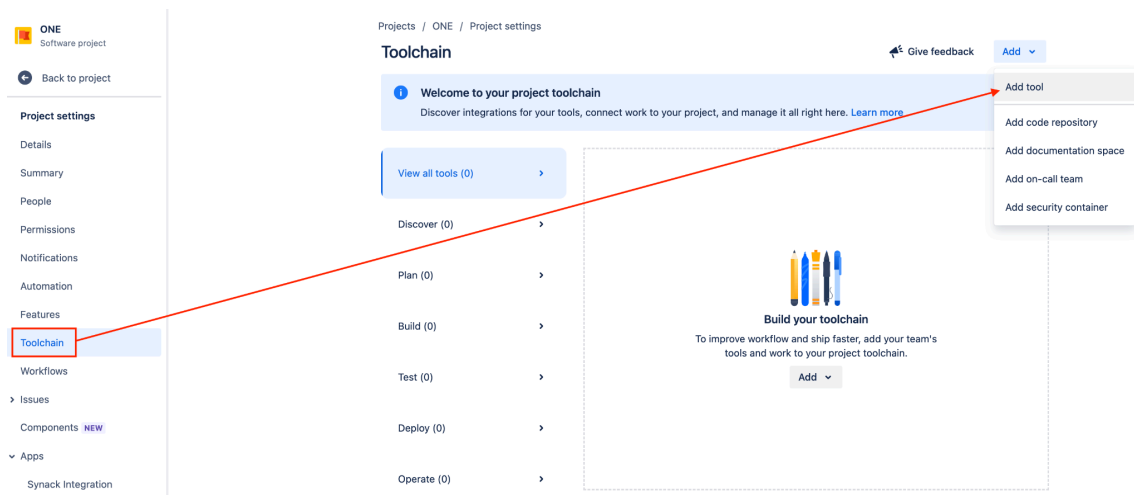
STARSCREAM-Mobile001 
STARSCREAM-Mobile003 
STARSCREAM-Mobile002  

Synack vulns submitted since

Save



You also need to add these Assessments as [Security containers](#). First, you have to add Synack as a tool to your Toolchain.


1. From your project's sidebar, go to Project settings > Toolchain and click “Add tool”

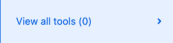


Projects / ONE / Project settings

Toolchain


 Give feedback  Add

 Welcome to your project toolchain
Discover integrations for your tools, connect work to your project, and manage it all right here. [Learn more](#)

 View all tools (0)

- Discover (0)
- Plan (0)
- Build (0)
- Test (0)
- Deploy (0)
- Operate (0)

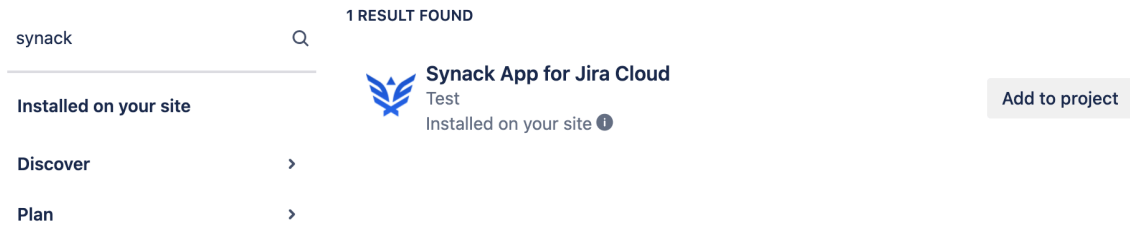
Build your toolchain
To improve workflow and ship faster, add your team's tools and work to your project toolchain.

 Add

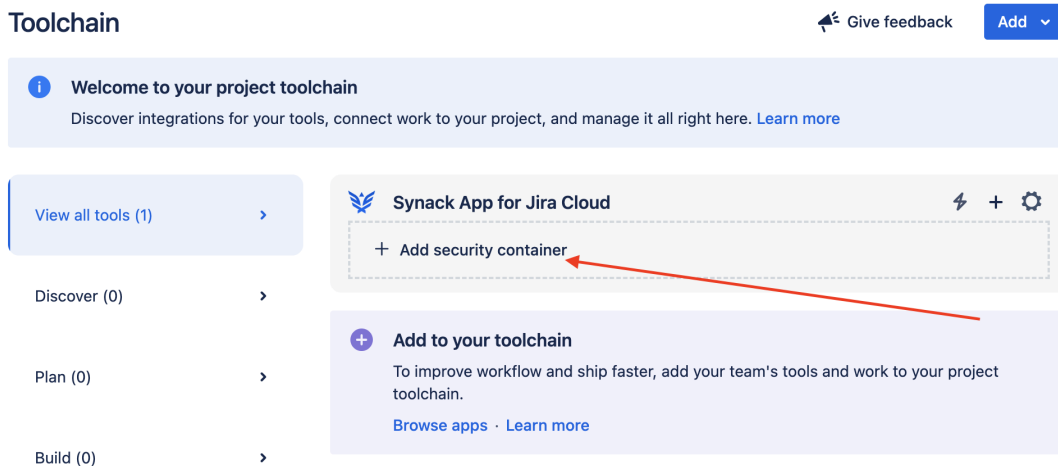
Add tool

- Add code repository
- Add documentation space
- Add on-call team
- Add security container

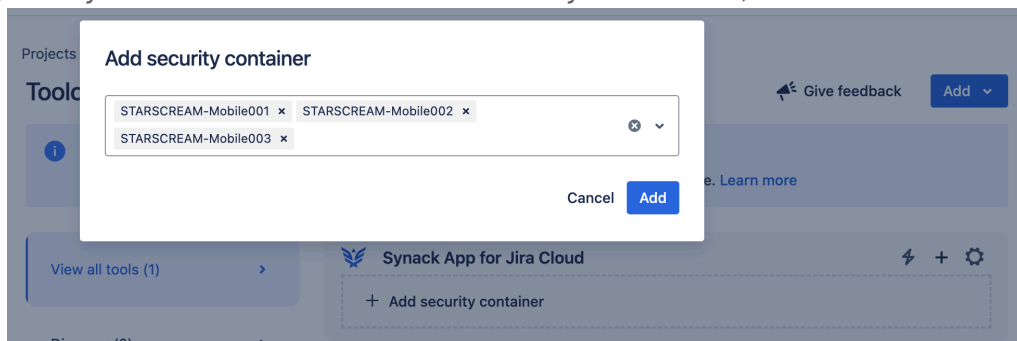
2. Search for Synack then click 'Add to project'



Then, from the Toolchain, click Add security containers, to the Synack App for Jira Cloud tool



Select your Synack assessments as the security containers, then click Add.



As long as your Assessments are listed in the Assessments field of your Project -> Synack Integration settings AND they are added as security containers in the Toolchain - you will see all the Vulnerabilities of these Assessments in the Security tab of the project.

For example, we selected Assessments starscream-mobile001, starscream-mobile002 and starscream-mobile003 here in the Synack Integration settings

Synack Integration

General Synchronize

Create in Jira

Vulnerabilities

Synack Assessments

STARSCREAM-Mobile001 x
STARSCREAM-Mobile003 x
STARSCREAM-Mobile002 x

Sync Mode

Automatic

every 30 minutes

Synack vulns submitted since

08/24/2022

Save

and added them as security containers here in the Toolchain

Toolchain

Give feedback

Add

Welcome to your project toolchain

Discover integrations for your tools, connect work to your project, and manage it all right here. [Learn more](#)

View all tools (1)

Synack App for Jira Cloud

STARSCREAM-Mobile003
STARSCREAM-Mobile001
STARSCREAM-Mobile002

With this setup, all vulnerabilities from these Assessments will be synchronized to Jira. You can work with Jira Vulnerabilities in the Security tab of your project

The screenshot shows the Jira ONE project toolchain interface. On the left, there is a navigation sidebar with options like Board, Reports, List, Goals, Issues, Components, and Security. The main area displays a 'Vulnerabilities' section with a search bar and filters. Below this, a table lists 8 vulnerabilities found, each with a severity level, a description, a status, and an introduction date.

Severity	Vulnerability	Vuln. status	Introduced	Identifiers	Issues	Actions
High	Vulnerability (Accepted) 7c646c Container: STARSCREAM-Mobile002 · starscreamwasp-2	Closed	Over 6 years ago		Create issue	...
Medium	Vulnerability (Accepted) 7554f1 Container: STARSCREAM-Mobile001 · starscreambee-1	Open	Over 6 years ago		Create issue	...
Medium	Vulnerability (Accepted) 27a55d Container: STARSCREAM-Mobile002 · starscreamwasp-1	Closed	Over 6 years ago		Create issue	...
Medium	Vulnerability (Accepted) d5dae0 Container: STARSCREAM-Mobile001 · starscreambee-2	Closed	Over 6 years ago		Create issue	...
Medium	test report Container: STARSCREAM-Mobile001 · starscreambee-3	Closed	Almost 4 years ago		Create issue	...

Jira Vulnerabilities will be updated according to the latest changes in Synack on each synchronization run. Jira Vulnerabilities are read-only, you cannot edit them. From the Vulnerabilities list, you can 'Create Issue' in Jira manually and link them to your Jira Vulnerabilities to track related work.

NOTE: In case you choose to create both Jira Issues (Method 2) and Jira Vulnerabilities (Method 1), you can then combine the workflows - see section **Method 3: Combined** - created Jira issues will be linked to created Jira Vulns automatically, by the Synack integration app.

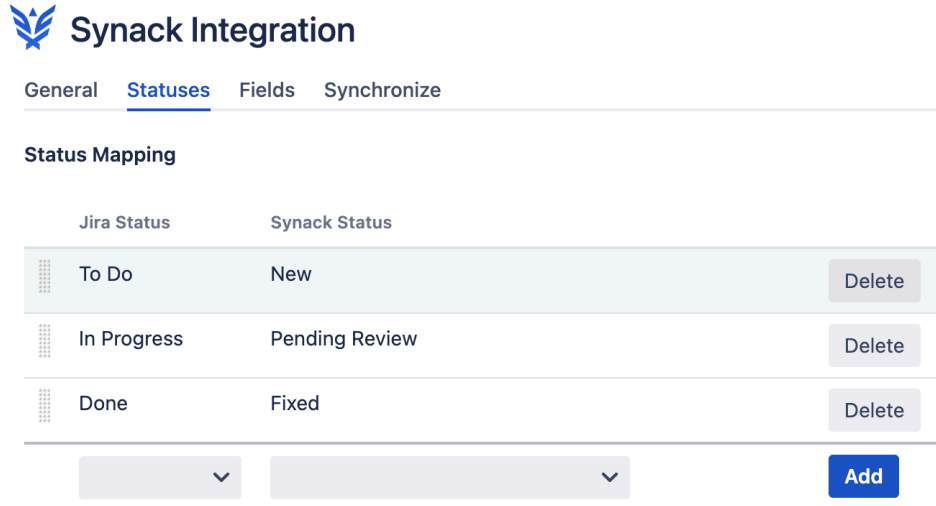
Method 2: Traditional workflow

Synack integration app will automatically create Jira Issues, based off of Synack Vulnerabilities, in your Jira instance.

To use this method, in your Jira project, go to Project Settings -> Apps -> Synack integration and select "Issues" in the "Create in Jira" field.

Note: Set other parameters of the integration and save the settings. Please refer to the section **Project Synchronization Settings** for details of all the parameters.

On the **Statuses** tab please define how you want to map Synack Vuln statuses to Jira Issue statuses. Based on that mapping, the integration app will change statuses of Jira Issues or statuses of Synack Vulns. The direction of changes depends on the parameter "Source of Truth".



The screenshot shows the 'Synack Integration' settings page, specifically the 'Statuses' tab. The page has a header with the Synack logo and the title 'Synack Integration'. Below the header are four tabs: 'General', 'Statuses' (which is selected and underlined), 'Fields', and 'Synchronize'. The main content area is titled 'Status Mapping' and contains a table with three rows. Each row has a 'Jira Status' column, a 'Synack Status' column, and a 'Delete' button. The first row maps 'To Do' to 'New', the second maps 'In Progress' to 'Pending Review', and the third maps 'Done' to 'Fixed'. Below the table are two dropdown menus and an 'Add' button.

Jira Status	Synack Status	
To Do	New	Delete
In Progress	Pending Review	Delete
Done	Fixed	Delete

Below the table, there are two dropdown menus and an 'Add' button.

On the **Fields** tab you can map Synack Vuln fields to Jira Issue fields. You can skip this and the default mapping will be applied automatically.

Synack Integration







General Statuses Fields Synchronize

Field Mapping

To make setup easier, we support mapping multiple Synack fields with the Jira Description Field.

Note: if you don't map Jira Summary, it will be mapped to Synack Title.

[Apply Defaults](#)

Jira Field	Synack Field	
 Summary	Title	Delete
 Description	Id	Delete
 Description	Link	Delete
 Description	Description	Delete
 Description	Category	Delete
 Description	CVSS Score	Delete

With this approach, the Synack integration app will create a Jira Issue for each of Synack Vulns from the selected Assessments and keep it up-to-date. It will synchronize:

- statuses
- comments
- labels
- Patch Verification requests

Please refer to the section **Project Synchronization Settings** for details of the available synchronization parameters.

Method 3: Combined

You can choose to create both a Jira Issue and a Jira Vulnerability for each of the Synack Vulnerabilities from the selected Assessments.

In your Jira project, go to Project Settings -> Apps -> Synack integration and select “Issues and Vulnerabilities” in the “Create in Jira” field, plus follow all other steps from Method 1 and Method 2.

In this case, you will have both the Jira Issues (see Method 2) and Jira Vulnerabilities (see Method 1) created, and they will be linked together automatically.

Vulnerabilities
Recent vulnerabilities found by scanning security containers linked to this project [Learn more](#)

Search Security container Severity Vuln. status Issue status Reset filters

8 vulnerabilities found

Severity	Vulnerability	Vuln. status	Introduced	Identifiers	Issues
High	Vulnerability (Accepted) 7c646c Container: STARScream-Mobile002 - starscreamwasp-2	Open	Over 6 years ago		<input checked="" type="checkbox"/> ONE-10 TO DO
Medium	test report 3 Container: STARScream-Mobile003 - starscreamnow-1	Open	Almost 4 years ago		<input checked="" type="checkbox"/> ONE-11 TO DO

Project Synchronization Settings

(note: this section is applicable to Method 1 - Traditional workflow)

After the connection settings are configured, you can set up synchronization settings for individual projects in your Jira. For any project in Jira, you can set it up to be synchronized with Synack vulnerabilities from chosen assessments. To avoid conflicts, you can only sync each Synack assessment with only one Jira project.

To open Synack synchronization settings for a project, you have to be an administrator of that project. Go to Project Settings -> Synack Integration Settings.

Within these settings, you can determine how often data is synchronized between Synack and Jira. The connection does not push real time updates, but rather at each sync interval it updates anything that has changed since the prior sync. Synack recommends using the Automatic sync mode with a frequency of 30 minutes, however that time period can be adjusted to your organization's needs.

Project settings

- Summary
- Details
- Re-index project
- Delete project
- Issue types
 - Sub-task
 - Task
- Workflows
- Screens
- Fields
- Priorities
- Versions
- Components
- Users and roles
- Permissions
- Issue Security
- Notifications
- Project links
- Issue collectors
- SYNACK INTEGRATION
 - Synack Integration Settings

Synack Integration

Sync Mode: Automatic every 30 minutes

Source of Truth: Jira

Synchronize comments: Both Ways

Synack Assessments: DEMOERITAE_2 x DEMOERITAE_3 x

Jira Username: JiraBot

Jira Issue Type: Task

Jira Status	Synack Status	
To Do	Pending Review	Delete
Done	Fixed	Delete
In Progress	Not Valid	Add

Fields

Jira Field	Synack Field	
Summary	Title	Delete
Description	Id	Delete

Item	Description
Create in Jira	Choose if you want to create Jira Issues, Jira Vulnerabilities, or both. See sections Method 1 and Method 2 for details.
Sync Mode	<p>Manual mode is available to only sync data on demand. We recommend using it for testing and troubleshooting. Manual mode provides feedback on the created/updated Jira issues and Synack vulnerabilities.</p> <p>Otherwise for production, you will want to use Automatic mode.</p>
Refresh interval for automatic mode	Interval in minutes that the sync process will run. Recommended value is 10 or higher.
Source of Truth	<p>This field is used on issues/vulnerabilities status update, to make sure that the status of the vulnerability is only modified in one place and it is reflected in the other system. It is important to note that changing the status on the system that is not SSoT will be reverted on the Sync process.</p> <p>SSoT also applies to labels/tags.</p>
Synchronize comments	<p>You can enable bi-directional sync of Jira and Synack Team Comments, or choose to only synchronize Synack Team Comments to Jira.</p> <p>Note that attachments to Team Comments in Synack will not be posted from Jira comments.</p>
Synack Assessments	List of Synack assessments. Only vulnerabilities from the selected assessments will be synchronized to Jira issues. To avoid conflicts, you can use each Synack assessment in only one Jira project.
Vulns submitted since date	If empty, all Exploitable Vulnerabilities from the selected Assessments will be synchronized. If the date is set, only Exploitable Vulnerabilities submitted to Synack on or after this date will be synchronized to Jira, with the rest ignored.
Synack Patch Verification Requests	<p>If set to Manual, users must request Patch Verifications manually. This process is described in the Patch Verification Flow section of this guide.</p> <p>If set to Automatic, Patch Verifications will be requested automatically when Jira issues are transitioned to the Jira Status that is mapped to Synack's "Closed:Fixed" status. Note that it doesn't</p>

	<p>happen immediately on the status transition, but on the next synchronization after transition.</p> <p>NOTE: This setting only works if the Source of Truth parameter is set to Jira.</p>
Account ID	<p>Account ID field is required when configuring the Jira Cloud integration. Please, go to your Jira users management and select a user. A URL of the selected user account should be like https://admin.atlassian.com/s/43ebd5af4-7dfdd-4284-123e-af111bbe8b33/users/5bd81f2s2da53528b8f1a17. The 5bd81f2s2da53528b8f1a17 part is an Account ID.</p>
Issue Type	<p>Lists the available Jira Issue Types based on the current Project.</p>
Status Mapping	<p>Inbound issues from Synack contain statuses that will be mapped to Jira statuses. The Jira statuses available are based on Workflow associated with your Project and the Issue Type selected on the previous field. The Synack statuses are based on the status values available on the Synack platform.</p> <p>Please note, as statuses in Synack change, Jira issues will be updated with the new status. However, for this to work the transition from each status must be configured in the appropriate Jira workflow.</p>
Fields Mapping	<p>You can change the default mapping of the Jira fields to their related Synack vulnerability fields. The Jira fields available are based on Field Configuration associated with the Project and issue type selected and on the create screen fields.</p> <p>NOTE: You can map multiple Synack fields with the Jira description field.</p>
Save Settings	<p>Button to save the settings. The sync function only uses the new configuration after saving it.</p>
Sync Now	<p>Button to fire a manual synchronization of the data and check if it succeeds. If it does not succeed, an error message will show on the screen. For more detailed information on the error, please see your Jira logs. This option is only available for manual Sync Mode.</p>

Descriptions of Synack fields available for mapping are as follows.

Note: All fields below can be mapped to Jira's Description field, to avoid having to create custom fields.

Synack Field	Description	Custom Field Type and comments
Title	Title of the Synack vulnerability	System Field - By default mapped to Jira Summary field
Id	Synack Vulnerability ID, the unique field that identifies each vulnerability on the Synack Client Portal	This field is mapped with <code>issue.property[synack].id</code> but you can map this to a custom field - Text Field (single line)
Description	Description of the vulnerability	System Field
Category	Name of the category for the vulnerability	Custom Field - Text Field (single line)
Validation Steps	Step by step instructions on how to reproduce the vulnerability	Custom Field - Text Field (multi-line). Set the Renderer as Wiki Style Renderer on project/issue type Field Configuration to make sure the attachments links will work
Tags	Tags associated with the vulnerability	System Field
Cvss Final	CVSS (Common Vulnerability Scoring System) score of the vulnerability	Custom Field - Text Field (single line)
Link	Link back to the Synack vulnerability page	Custom Field - URL Field
Impact	Provides info on the impact of the vulnerability	Custom Field - Text Field (multi-line)
Recommended Fix	Step by step instructions on how to fix the exploit	Custom Field - Text Field (multi-line)
Exploitable Locations	List of exploitable locations where the exploit has been discovered	Custom Field - Text Field (multi-line)
Listing	Provides details on the assessment such as name and link back to the assessment page on Synack	Custom Field - Text Field (multi-line)

Resolved At	Date/time the vulnerability was approved by Synack	Custom Field - Date Time Picker
Closed At	Date/time the vulnerability was closed	Custom Field - Date Time Picker
Updated At	Last updated timestamp	Custom Field - Date Time Picker





Synack Integration for Jira is a bi-directional integration (in the case of Method 2 only). Once the integration setup is complete, existing data from Synack will start syncing over to your Jira instance and new Jira issues will surface as per the defined refresh interval.

If your organization uses Jira Components to tag tickets, you can create Automation Rules within Jira to automatically apply a Component to new tickets as they are created.

Patch Verification Flow

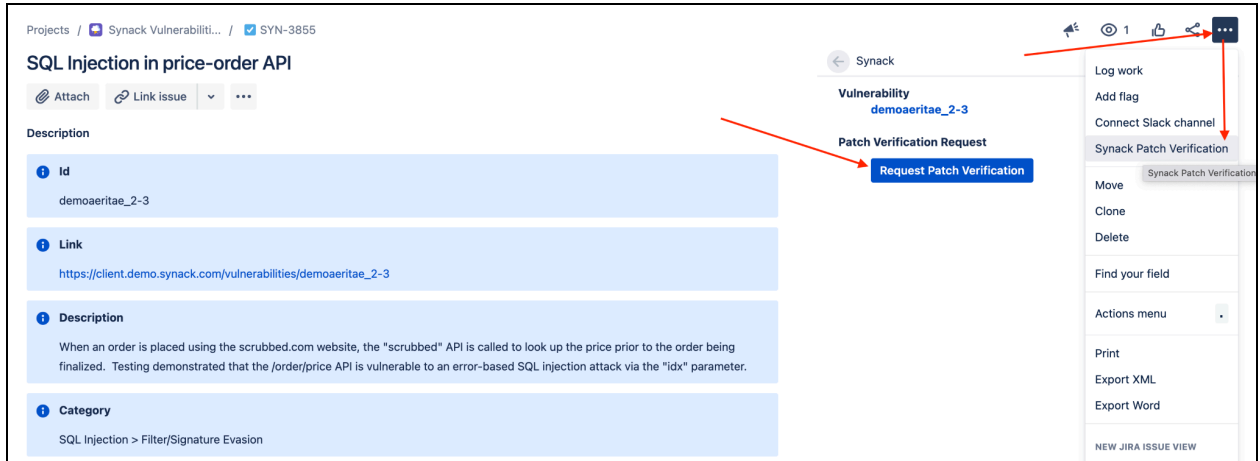
Patch Verification functionality is only available when your integration is configured to create Issues in Jira (i.e. Method 2).

Patch Verification can be requested directly from your Jira instance. It can only be requested for Jira issues that are in the status which is mapped to Synack's Closed:Fixed status. For example, you have this status mapping:

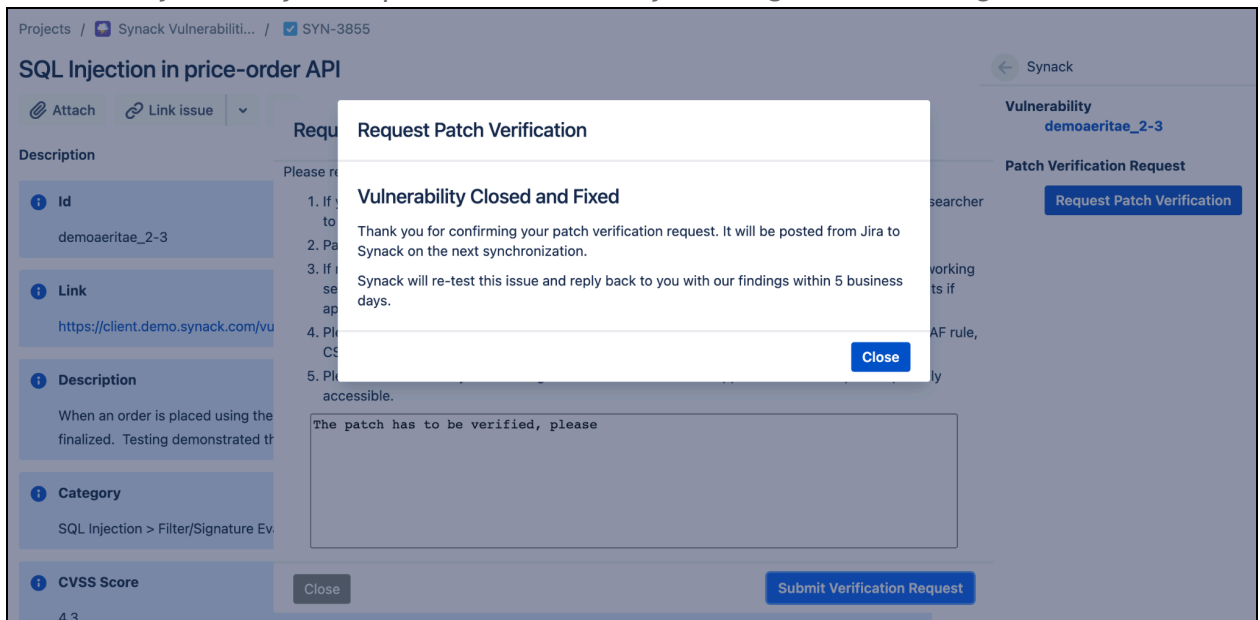
Status Mapping		
Jira Status	Synack Status	
 Open Vuln	Pending Review	Delete
 Won't Fix	Won't Fix	Delete
 Invalid	Not Valid	Delete
 Done	Fixed	Delete

Here the Synack's Closed:Fixed status is mapped to Jira status Done. With this configuration, you will be able to request Patch Verification from Jira only if the issue is currently in status Done. If the issue is in any of other statuses - the Patch Verification menu items won't be available. To request a PV from Jira, use one of the two menu items (see screenshot):

- "Request Patch Verification" button in 'Synack' section
- "Synack Patch Verification" menu item in 'More' menu (on Jira Data Center - 'More', on Jira Cloud it is '..' in the top-right)



Please note that your Patch Verification request may not be submitted to Synack immediately. When you request PV from Jira, you will get this message:



The Patch Verification request will be submitted to Synack at the time of the next synchronization cadence.

The 'Synack' section in Jira issue shows the actual status of the Patch Verification (see screenshot below):

Projects / Synack Vulnerability... / SYN-3855

SQL Injection in price-order API

Attach Link issue

Description

Id
demoeritae_2-3

Link
https://client.demo.synack.com/vulnerabilities/demoeritae_2-3

Synack

Vulnerability
demoeritae_2-3

Patch Verification Request

Created in Jira:
→ Thu Dec 16 11:44:16 GMT 2021

Submitted to Synack:
→ Thu Dec 16 11:56:32 GMT 2021

Status:
Requested

Troubleshooting

These are the ways to troubleshoot a failing synchronization:

- change Sync Mode to Manual. Run synchronization manually and see if there are any errors reported.
- contact Synack support if you need further assistance.

Frequently Asked Questions

Which IP address should be used to generate the API token for the Jira Cloud app?

Please use 34.145.166.47. This is the IP address of the Jira Cloud agent that communicates with the Synack API server to get and update vulnerability data.

Can I use this integration with different projects within Jira?

Yes, this setup is supported with the latest Jira Cloud versions.

Can I use multiple Jira instances?

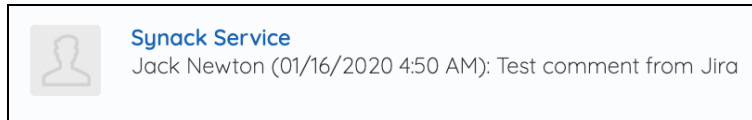
Yes, however this setup requires a few manual steps. Please contact your SPM or SA if you want to use multiple Jira instances.

Can I use Jira and ServiceNow integrations together?

No, as there can be conflicting changes being submitted by Jira and ServiceNow, which can cause data inconsistency.

Comments are posted to Synack under the name of the user that generated the API token. What can I do to fix this?

This is a limitation of the app. Since we don't have a method to map Synack users with Jira users (many times, your Jira users may not even exist within Synack). The way these comments appear on Synack is as follows -



In this screenshot, Synack Service is the user that generated the API and Jack Newton is the user on Jira that posted the comment. Customers can choose to invite a "Service Account" user to Synack Client Portal and generate the API token with that account to not post comments under a personal username.

If you don't care to exchange comments, you can choose to only sync comments from Synack to Jira under the Connection Settings.

What is the resolved_at date field?

Resolved_at field is the timestamp when a vulnerability was approved by the Synack Vuln Ops team. Every exploitable vulnerability is manually triaged by the Vuln Ops team before it is shared with a customer. This is done so customers are not wasting their time filtering through noise.