

JIRA INTEGRATION GUIDE

Synack's Integration with
Jira

September 2023



Index

Synack Integration for Jira	3
Step 1: Synack API Token Generation	3
Step 2: Install the App	4
Step 3: Configure the App	4
Connection Settings	4
Project Synchronization Settings	5
Validation of Configuration	10
Patch Verification Flow	11
Troubleshooting	12
Frequently Asked Questions	14
Which IP address should be used to generate the API token for the Jira Cloud app?	14
Which IP address should be used to generate the API token for the Jira Server / Jira Data Center app?	14
Can I use this integration with different projects within Jira?	14
Can I use multiple Jira instances?	14
Can I use Jira and ServiceNow integrations together?	14
Comments are posted to Synack under the name of the user that generated the API token. What can I do to fix this?	15
What is the resolved_at date field?	15

Synack Integration for Jira

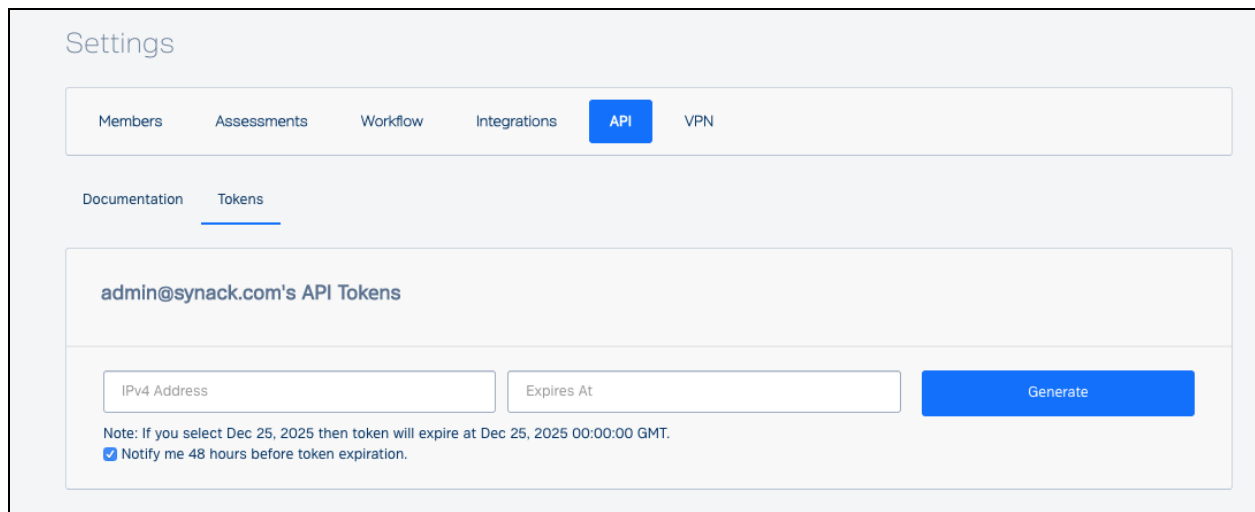
Synack Integration for Jira is used to create and sync Jira issues based on Synack vulnerabilities. This guide has been designed to describe the configuration steps required to configure this add-on for Jira Server, Data Center and Cloud.

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 'Settings' header. Below the header, there are tabs for 'Members', 'Assessments', 'Workflow', 'Integrations', 'API', and 'VPN'. The 'API' tab is active. Under the 'API' tab, there are sub-tabs for 'Documentation' and 'Tokens'. The 'Tokens' sub-tab is active. The main content area is titled 'admin@synack.com's API Tokens'. It contains two input fields: 'IPv4 Address' and 'Expires At'. To the right of these fields is a blue 'Generate' button. Below the input fields, there is a note: 'Note: If you select Dec 25, 2025 then token will expire at Dec 25, 2025 00:00:00 GMT.' and a checked checkbox labeled 'Notify me 48 hours before token expiration.'

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 your Jira instance is installed on-premise, you will need the public IP address of your Jira server. Wildcards are supported for the IPv4 field. Please also define an expiration date for this token. If you are using Jira Cloud, here is the IP address to generate the API token: 34.145.166.47.

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 page to get started.

- For Jira Server & Data Center (DC): <https://marketplace.atlassian.com/1220818>
- For Jira Cloud: <https://marketplace.atlassian.com/1221284>

Step 3: Configure the App

To access the Configuration Page you need to have administrative permission and access to manage add-ons on your Jira instance.

Connection Settings

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

▼

Allow sending usage statistics

Save Settings

Test Connection

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 • If your Jira is installed on-premise, you will need the public IP address of your Jira server • 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.

Project Synchronization Settings

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 a chosen assessment(s). 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

Synchronization mode

Source of Truth

Jira

Primary system definition, used for sync jobs. Setting Source of Truth to Synack will overwrite status and labels values in Jira during sync.

Synchronize comments

Both Ways

Choose how to synchronize comments

Synack Assessments

DEMOAERITAE_2 x DEMOAERITAE_3 x

List of Synack assessments that will be synchronized

Jira Username

JiraBot

Username to create and update issues in Jira

Jira Issue Type

Task

statuses

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

Fields

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

Item	Description
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 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>

Username / Account ID	<p>Jira username that will create/update issues within this project. This user must have permission to create/update issues, transition and to create comments and attachments.</p> <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-af11bbe8b33/users/5bd81f2s2da53528b8f1a17. The 5bd81f2s2da53528b8f1a17 part is an Account ID.</p>
Issue Type	Lists the available Jira Issue Types based on the current Project.
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	Button to save the settings. The sync function only uses the new configuration after saving it.
Sync Now	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.

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 issue.property[synack].id 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. Once the integration setup is complete, existing data from Synack will start syncing over to your Jira instance and new vulnerabilities will surface as per the defined refresh interval.

Aside from setting up a token in the Synack client portal, no configuration is required on Synack.

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.

Validation of Configuration

Synack app allows you to perform a number of checks to make sure the configuration of your Jira project is valid for synchronization. There are multiple aspects of configuration in Jira that could prevent the synchronization from executing successfully. For example, if there are mandatory Jira fields and they are not mapped to one of Synack fields - the app will fail to create an issue in Jira. Missing permissions is another example. If the designated Jira user does not have permissions to create issues or to transition issues - the synchronization will fail.





Synack app allows you to validate your configuration and catch problems at early stages. To run validation, go to the Synack Integration page of your project in Jira and click the button 'Validate Configuration'.

Note that the validation is not able to detect all the problematic cases due to complexity of various possible Jira configurations. If your synchronization doesn't work and the validation does not report any problems please contact Synack support.

NOTE: Validation feature is only available for Jira Server integration at this time.

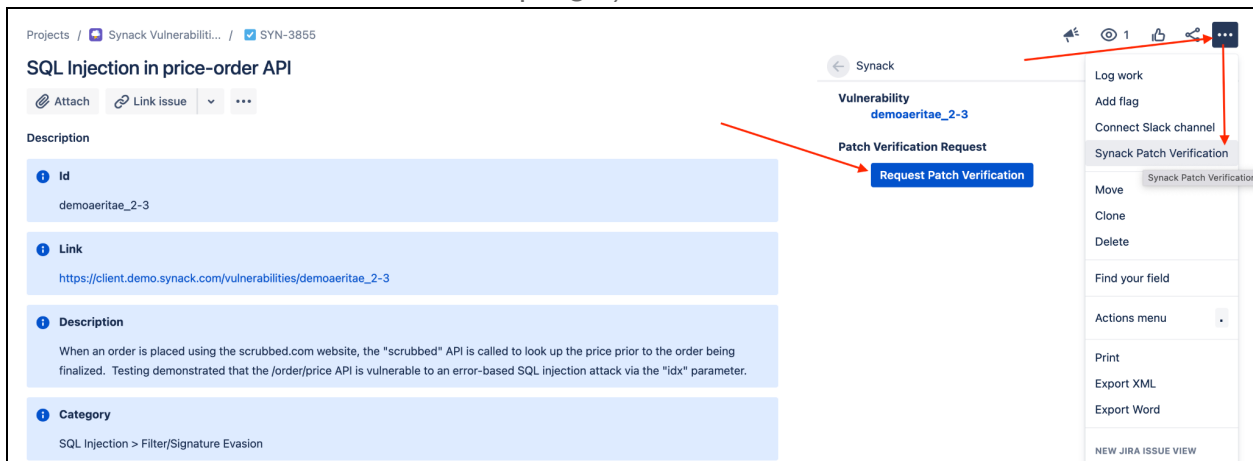
Patch Verification Flow

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	<button>Delete</button>
 Won't Fix		Won't Fix	<button>Delete</button>
 Invalid		Not Valid	<button>Delete</button>
 Done		Fixed	<button>Delete</button>

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 Server - 'More', on Jira Cloud it is '...' in the top-right)



Projects / Synack Vulnerability... / SYN-3855

SQL Injection in price-order API

Attach Link issue

Description

Id
demoaeritae_2-3

Link
https://client.demo.synack.com/vulnerabilities/demoaeritae_2-3

Description
When an order is placed using the scrubbed.com website, the "scrubbed" API is called to look up the price prior to the order being finalized. Testing demonstrated that the /order/price API is vulnerable to an error-based SQL injection attack via the "idx" parameter.

Category
SQL Injection > Filter/Signature Evasion

Synack

Vulnerability
demoaeritae_2-3

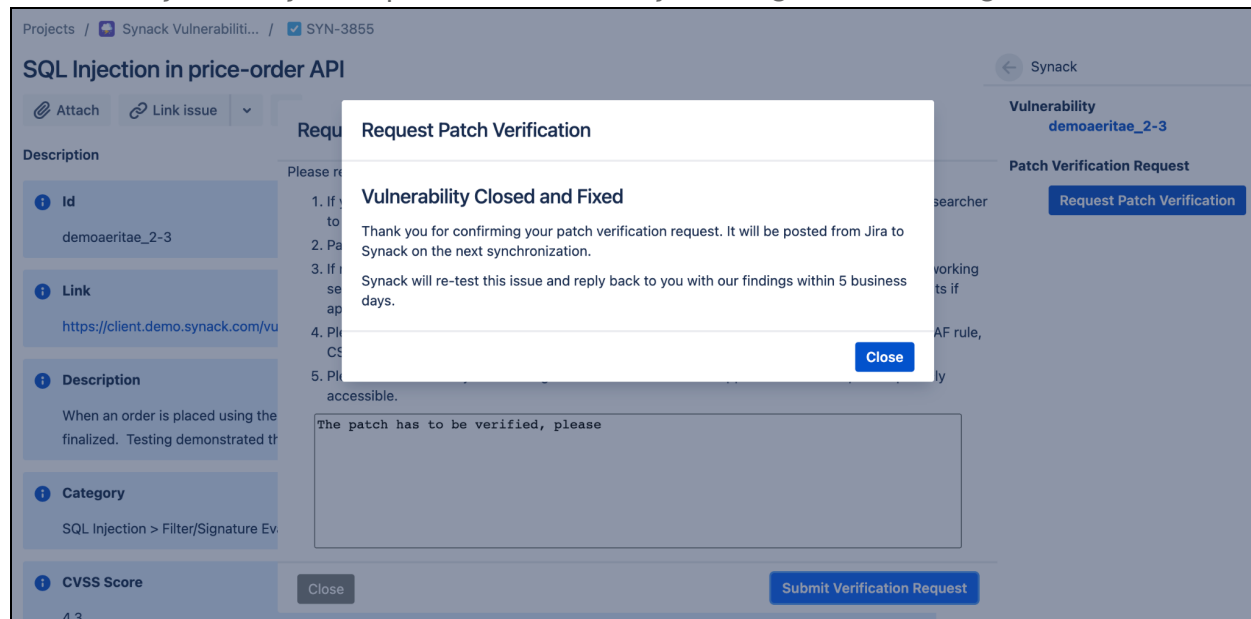
Patch Verification Request

Request Patch Verification

Log work
Add flag
Connect Slack channel
Synack Patch Verification
Move
Clone
Delete
Find your field
Actions menu
Print
Export XML
Export Word
NEW JIRA ISSUE VIEW

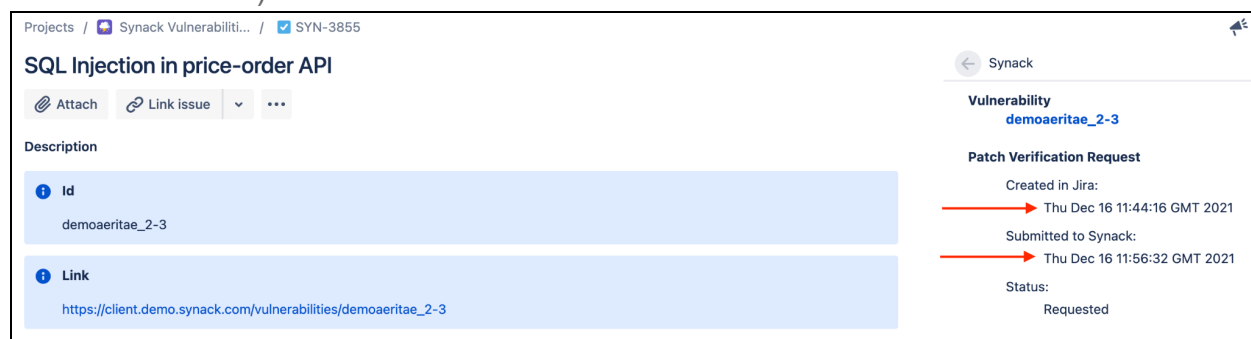
This Jira Cloud screenshot shows both patch verification request options.

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):



Troubleshooting

These are the ways to troubleshoot a failing synchronization:

- validate your configuration. See section [Validation of Configuration](#).
- 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.

Which IP address should be used to generate the API token for the Jira Server / Jira Data Center app?

This should be the IP address of the server where your Jira instance is installed. Please contact your IT admin for details.

Can I use this integration with different projects within Jira?

Yes, this setup is supported with the latest Jira Cloud versions and with Jira Server /Data Center versions 2.0.0 and higher.

Can I use multiple Jira instances?

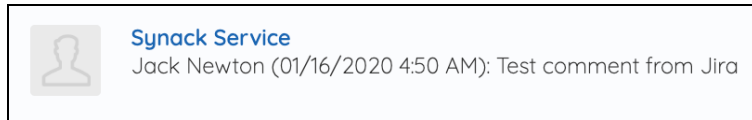
Yes, however this setup requires a few manual steps. Please contact your SPM or SA if you want to use multiple Jira instances.

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.