Tenable and Jira Cloud Integration Guide

Last Revised: April 26, 2024

Table of Contents

Welcome to Tenable for Jira Cloud

The Tenable for Jira Cloud integration provides you with the organizational convenience of managing vulnerabilities detected in Tenable Vulnerability Management from the Tenable platform itself. When you configure the Tenable for Jira Cloud integration, custom fields are created in Tenable for Jira Cloud. The integration uses these custom fields to organize and manage vulnerabilities detected when running vulnerability scans.

- Tenable for Jira Cloud pulls Tenable Vulnerability Management vulnerability data, then generates Jira tasks and linked tasks based on the vulnerability's current state. Tasks are automatically closed once the state of the vulnerability is marked as **Fixed** in Tenable Vulnerability Management.
- Tenable for Jira Cloud creates a **Tenable Vulnerability Task** for each vulnerability and creates each vulnerability instance as a "linked task." For example, if you have five hosts with plugin 151074 on a **Group-by** vulnerability, the integration creates one **Tenable Vulnerability Task** with the details for that specific plugin and creates five linked tasks. Each linked task points to a specific instance of the vulnerability, on a specific host.
- Tenable for Jira Cloud automatically closes **Vulnerability Instances** once the vulnerability is fixed in Tenable Vulnerability Management.
- Vulnerabilities are closed once all linked tasks enter a closed state.
- If a vulnerability is reopened, Tenable Vulnerability Tasks are moved to the **Reopen** status.
- All data imports from Tenable Vulnerability Management are synced with Tenable for Jira Cloud after the scan gets completed. Vulnerabilities are available in Tenable for Jira Cloud after scan completion and some processing time

The Tenable for Jira Cloud integration can pull historic findings as well as new findings as they get discovered by the platform and creates Jira issues for each vulnerability in the project that you specify. The integration creates Jira tickets according to the following scenarios:

Group By Vulnerability

- For every vulnerability plugin, the integration creates a vulnerability issue.
- For every affected asset, the integration creates a vulnerable host issue and a blocking link to the related vulnerability issue. A linked issue is created under the vulnerability task.
- As assets are remediated, vulnerable host tickets are marked as resolved.
- If all vulnerable host issues related to a vulnerability issue are marked as resolved, the vulnerability issue is marked as resolved.
- If an asset is found to have a vulnerability again, but was previously resolved, the integration reopens the vulnerable host issue.
- If a vulnerability issue is marked as resolved and a new vulnerable host issue is linked to it (or a prior vulnerable host issue that was resolved) the vulnerability issue is reopened.
- If a vulnerability issue is marked as resolved and a new vulnerable host issue is linked to it (or a prior vulnerable host issue that was resolved) the vulnerability issue is reopened.
- All historic data imported from Tenable Vulnerability Management uses the `last_found` field. This ensures that all issues are updated whenever new information becomes available.

Group By Asset

- For every host, a vulnerability host issue is created.
- For every reporting plugin, the integration creates a vulnerability issue and a blocking link to the related vulnerability host issue. A linked issue is created under the vulnerability host task.
- As findings are remediated, vulnerability issue tickets are marked as resolved.
- If all vulnerability issues related to a vulnerability host issue are marked as resolved, the vulnerability host issue is marked as resolved.
- If a vulnerability issue is found to have a vulnerability again, but was previously resolved, the integration reopens the vulnerable issue.
- If a vulnerability host issue is marked as resolved and a new vulnerable plugin issue is linked to it (or a prior vulnerable plugin issue that was resolved) the vulnerability issue is reopened.

In Tenable Vulnerability Management, the vulnerability issue and vulnerable host issue titles are automatically generated using the following formula:

- Vulnerability = pluginname + protocol + port + severity
- Vulnerable Host = IPV4 / IPV6 + FQDN

Prerequisites

Meet the following prerequisites before installing and using the Tenable for Jira Cloud integration:

- An admin user in Tenable Vulnerability Management can configure the integration.

  > **Note:** The Tenable for Jira Cloud integration requires a user in Jira Cloud who has admin privileges as the integration has to create various components in Jira Cloud, as described here, After the setup is completed and ticket generation begins, admin privileges can be dropped and you can downgrade the user to these permissions.

- The Tenable for Jira Cloud integration requires a user in Jira cloud with admin privileges.
- Projects cannot have mandatory fields or configured validators.
- Ensure your Tenable for Jira Cloud instance does not have any custom field starting with “Tenable." Delete these.
- Ensure you have no Issue types with the name “Tenable Vulnerability Host” or “Tenable Vulnerability.”
- If you are creating the integration project manually, select the project template as **Business** (Jira Work Management), and the project type as **Company-Managed**. For more information, see the Atlassian documentation.

Roles and Permissions

The Jira Cloud user used to connect to the Tenable for Jira Cloud instance in the integration, should have the following permissions:

- Assignable User
- Assign Issues
- Close Issues
- Create Issues
- Delete Issues
- Edit Issues
- Link Issues
- Modify Reporter
- Move Issues
- Resolve Issues
- Schedule Issues
- Set Issue Security
- Transition Issues

Connect and Configure Tenable for Jira Cloud

Required User Role: Administrator

Before you begin:

- You must have your Tenable Vulnerability Management API keys.

  Note: For your Tenable Vulnerability Management integration:

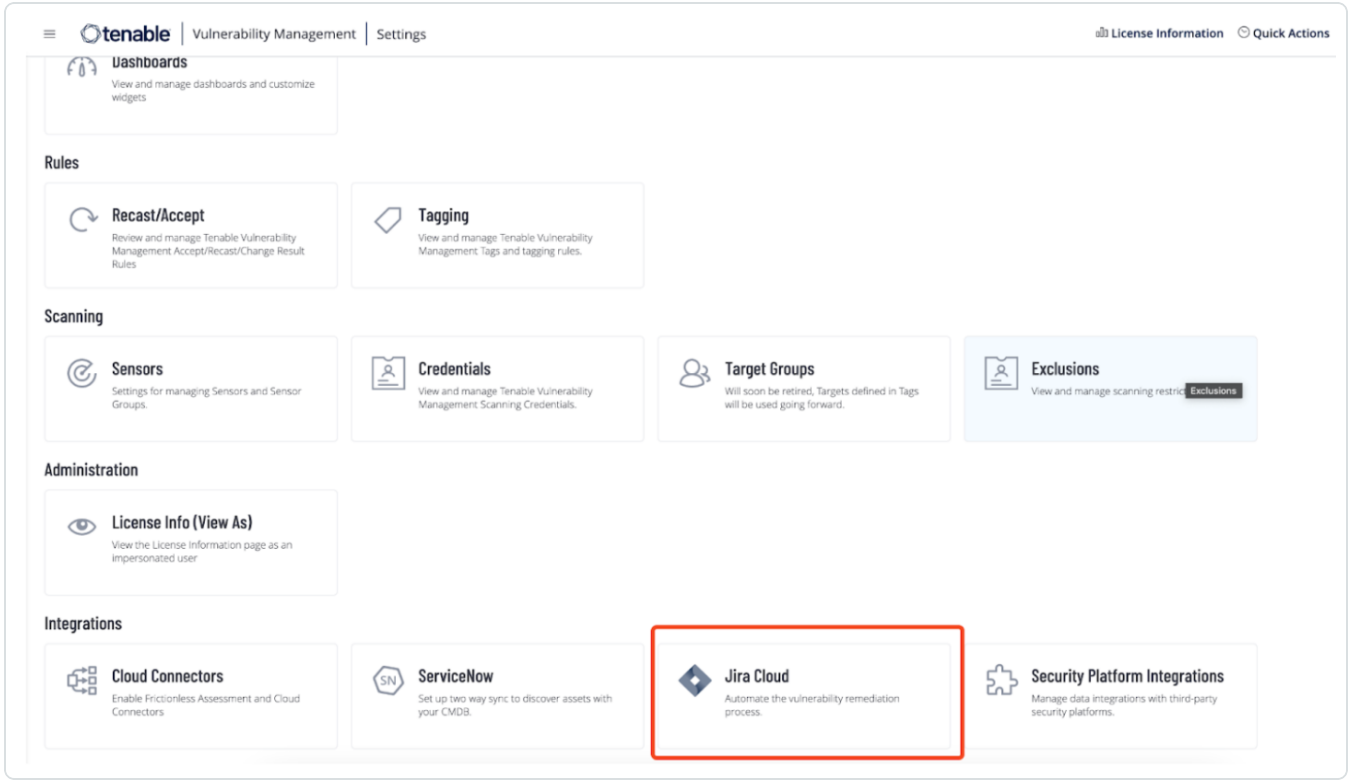
  - Generate an API key in Tenable Vulnerability Management to complete the configuration. See the Tenable Vulnerability Management user guide for instructions on how to generate an API key. (Do not use this API key for any other third party or custom-built application or integration. It must be unique for each installed instance of the integration.)

To configure Tenable Vulnerability Management:

1. Log in to Tenable Vulnerability Management.
2. In the upper-left corner, click the ☰ button.

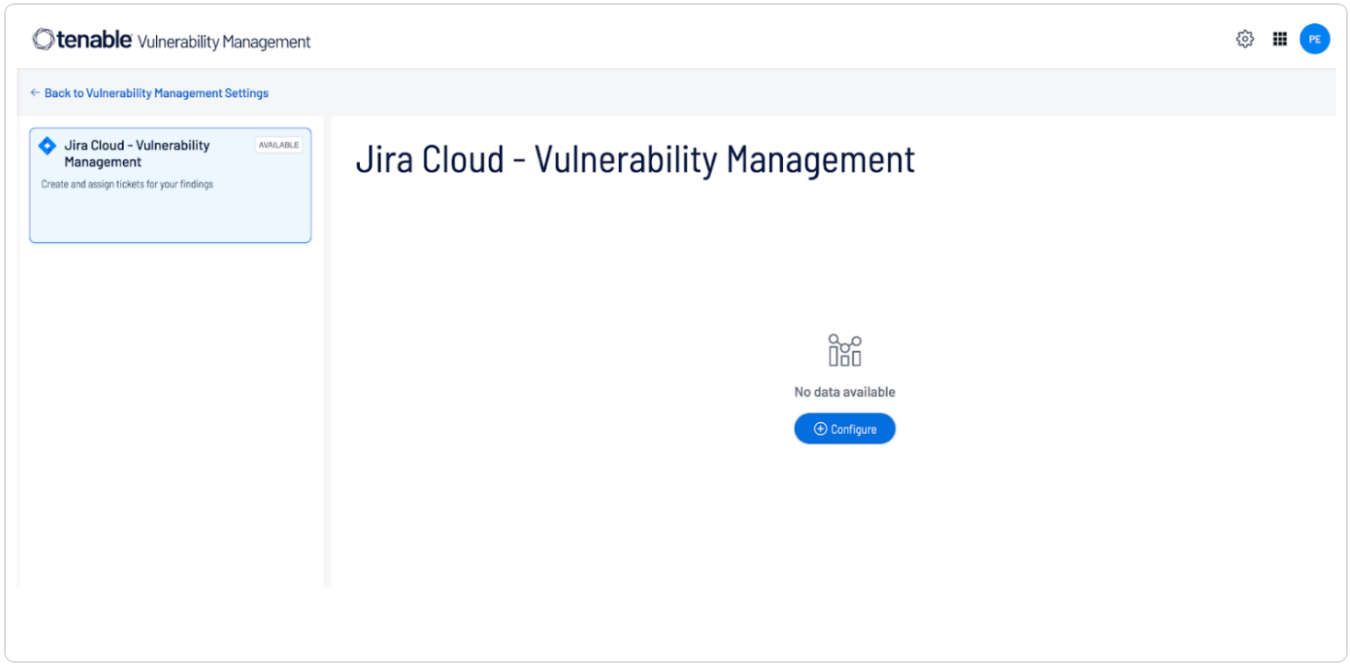
   The left navigation plane appears.
3. In the left navigation plane, click **Settings**.

   The **Settings** page appears:



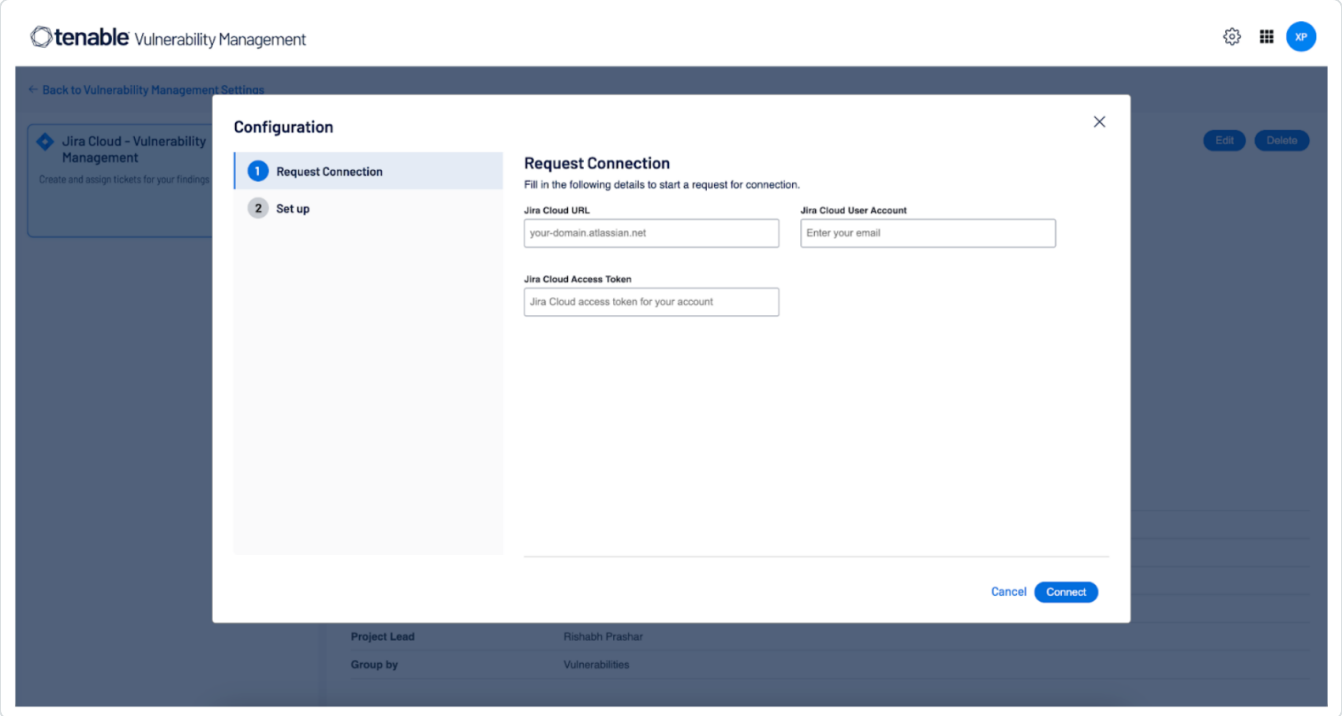
4. In the Integrations section, click the **Jira Cloud** tile.

   The **Jira Cloud - Vulnerability Management** page appears:



5. Click the **Configuration** button.

The **Configuration** pop-up appears. By default, the **Request Connection** tab is active:



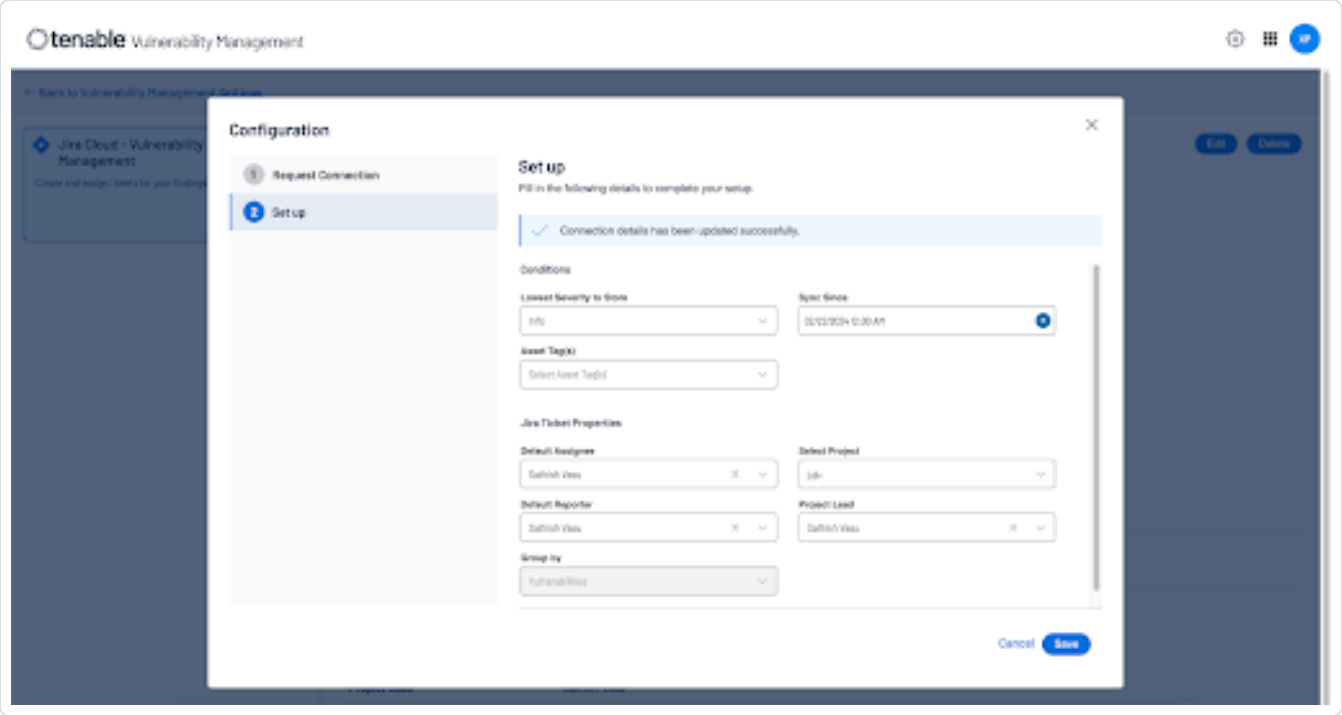
6. Use the following table to fill in the appropriate Tenable for Jira Cloud options in the **Request Connection** tab.

Option Name	Description	Required
Jira Cloud URL	Your Jira cloud instance URL. (For example, yoursite.atlassian.net) **Note:** The integration only supports Jira cloud URLs with a domain ending in `*.atlassian.net`.	yes
Jira Cloud Access Key	The Tenable for Jira Cloud integration requires a Site Admin Access Key to create the project, the custom fields, and link all elements to the correct screens. **Note:** To create an API token, refer to the Atlassian documentation.	yes

Jira User Email Address	The Atlassian user email of the user whose key is provided in the Jira Cloud Access Key field.	yes

7. Click the **Connect** button.

   If your credentials are valid, the **Set Up** section appears to configure the integration:



8. Use the following table to fill in the Tenable for Jira Cloud options in the **Set Up** tab.

Option Name	Description	Required
Set up	Multiple fields to configure Tenable for Jira Cloud, based on your requirements.	yes
Lowest Severity to Store	The lowest severity for which tickets are created. (For example, if you select **Medium** severity, the integration creates a ticket of severity Medium, High, and Critical.	yes
Sync Since	If provided, the integration pulls historic data from that time. The maximum allowed past date is one	yes

	month.	
Asset Tags	(Required if Tags are provided) Tickets are only created for assets which include the provided tag.	yes
Default Assignee	If selected, all the tickets are assigned to the selected user. If not selected, the Tenable for Jira Cloud user who configured the integration is used by default.	yes
Select Project	You can create a project by providing a unique name or by selecting a project already created in Tenable for Jira Cloud, By default, this integration uses the **Business** project in Tenable for Jira Cloud. For more information about project types, see *Product Features and Project Types* in the Atlassian documentation. **Note:** This integration supports classic (Company-managed) Jira projects, You must create a Company-managed project and select that project in this field.	yes
Default Reporter	If selected, the selected user is used as the default reporter on all tickets, If not provided, the Tenable for Jira Cloud user who configured the integration is used by default. **Note:** You must have appropriate permissions to assign the default reporter. If not, the Default Reporter is not assigned.	yes
Project Lead	The lead user for the project.	yes
Group by	You can group tickets by either Asset or Vulnerability.	yes

9. Click **Save** to complete the setup.

What to do next:

Tenable for Jira Cloud creates a "Tenable Vulnerability Workflow" to manage the transition of the Jira tickets. It may take several minutes to setup projects and custom fields in Tenable for Jira Cloud. Details are refreshed on-screen once they are created. As soon as the configuration is saved, Tenable for Jira Cloud starts listening to new findings discovered by the scans, providing near real-time vulnerability data into Tenable for Jira Cloud. When Tenable for Jira Cloud starts creating tickets, the **Waiting for ticket creation on Jira instance** notification banner is removed.

Next, Tenable for Jira Cloud fetches metrics and shows them on the Tenable for Jira Cloud dashboard, as shown in the following image:

Custom Fields and Filters Created in JIRA

Custom fields are created when Tenable for Jira Cloud is installed. Custom field types are either editable **text area** or non-editable **read-only field**. You can also create filters with the custom fields created in Tenable for Jira Cloud.

Note: There may be conflict if a custom field is created manually or as part of another plugin.

Note: While configuring Tenable Vulnerability Management or Tenable Security Center for Jira, if you select **Asset** in the **Group By** drop-down, several fields (Tenable Port, Tenable Protocol, Tenable First Found, Tenable Last Fixed, and Tenable State) are moved from the **Vulnerable Host** issue type to the **Vulnerability** issue type, while the Tenable Severity field is removed from the **Vulnerable Host** issue type.

Note: The Jira Cloud integration does not support pre-configured Custom Fields, Issue Types, or Issue Type Schemes with the prefix `Tenable`. Delete these, then set up the integration again.

Vulnerability

Field Name	Type	Definition
Tenable BID	text area	The Bugtraq ID for the plugin that identified the vulnerability.
Tenable CVE	text area	The Common Vulnerability and Exposure (CVE) ID for the plugin.
Tenable CVSSv3 Base Score	read-only field	The CVSSv3 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).
Tenable CVSSv3 Temporal Score	read-only field	The CVSSv3 temporal score (characteristics of a vulnerability that change over time, but not among user environments).
Tenable CVSSv2 Base Score	read-only field	The CVSSv2 base score (intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments).
Tenable CVSSv2	read-only	The CVSSv2 temporal score (characteristics of a

Temporal Score	field	vulnerability that change over time but not among user environments).
Tenable plugin Family	read-only field	The family of the plugin that identified the vulnerability. For more information about plugin families, see https://www.tenable.com/plugins.
Tenable plugin ID	read-only field	The ID of the plugin that identified the vulnerability.
Tenable MS Bulletin	read-only field	The Microsoft security bulletin that the plugin covers.
Tenable Vulnerability Title	read-only field	The name of the plugin that identified the vulnerability.
Tenable Solution	read-only field	Remediation information for the vulnerability.
Tenable Severity	read-only field	The code for the severity originally assigned to a vulnerability before a user recasts the risk associated with the vulnerability.
Tenable Source	read-only field	Determines if the application is connected to Tenable Vulnerability Management or Tenable Security Center.
Tenable Short Description	read-only field	A short description of the plugin.
Tenable VPR Scores	read-only field	VPR is a dynamic companion to the data provided by the vulnerability's CVSS score. Values range from 0.1 to 10.0, with a higher value representing a higher likelihood of exploit.

Vulnerable Host

Field Name	Type	Definition
Tenable Agent UUID	read-only field	The UUID of the agent that performed the scan where the

		vulnerability was found.
Tenable Device Type	read-only field	The type of asset where the vulnerability was found.
Tenable FQDN	read-only field	The fully qualified domain name of the asset where a scan found the vulnerability.
Tenable Hostname	read-only field	The hostname of the asset where a scan found the vulnerability.
Tenable Asset UUID	read-only field	The UUID of the asset where a scan found the vulnerability.
Tenable IPv4	read-only field	The IPv4 address of the asset where a scan found the vulnerability.
Tenable IPv6	read-only field	The IPv6 address of the asset where a scan found the vulnerability.
Tenable MAC Address	read-only field	The MAC address of the asset where a scan found the vulnerability.
Tenable NetBIOS Name	read-only field	The NETBIOS name of the asset where a scan found the vulnerability.
Tenable Plugin Output	text area	The text output of the Nessus scanner.
Tenable Port	read-only field	The port the scanner used to communicate with the asset.
Tenable Protocol	read-only field	The protocol the scanner used to communicate with the asset.

Tenable Service	read-only field	The service the scanner used to communicate with the asset.
Tenable Severity	read-only field	The severity of the vulnerability as defined using the Common Vulnerability Scoring System (CVSS) base score. Possible values are: • info - The vulnerability has a CVSS score of 0. • low - The vulnerability has a CVSS score between 0.1 and 3.9. • medium - The vulnerability has a CVSS score between 4.0 and 6.9. • high - The vulnerability has a CVSS score between 7.0 and 9.9. • critical - The vulnerability has a CVSS score of 10.0."
Tenable First Found	read-only field	The date on which the vulnerability was first found on the asset.
Tenable Last Fixed	read-only field	The date on which the vulnerability was last fixed on the asset. Tenable Vulnerability Management updates the vulnerability state to fixed when a scan no longer detects

		a previously detected vulnerability on the asset.
Tenable State	read-only field	The state of the vulnerability as determined by the Tenable Vulnerability Management state service. Possible values are: • open - The vulnerability is currently present on an asset. • reopened - The vulnerability was previously marked as fixed on an asset, but detected again by a new scan. • fixed - The vulnerability was present on an asset, but is no longer detected.
Tenable Source	read-only field	Determines if the application is connected to Tenable Vulnerability Management or Tenable Security Center.

Issue Types

- Tenable Vulnerability Host.
- Tenable Vulnerability

Issue Type Scheme

- Tenable Issue Type Scheme

Created Components

Tenable for Jira Cloud creates many component as part of the initial setup. The following list includes many of the actions performed by the integration.

- Search Project Details
- Search User Details
- Create Project
- Check Project Permissions
- Search Tenable Workflow
- Search Tenable Workflow Scheme
- Search Workflow Status
- Get Workflow Status
- Create Tenable Workflow
- Create Tenable Workflow Scheme
- Assign Workflow Scheme to Project
- Search Tenable Issue Types
- Create Tenable Issue Types
- Create Tenable Issue Types Schemes
- Assign Issue Type Scheme to Project
- Search Custom Fields
- Create Custom Fields
- Attach Custom Fields to screens, tabs
- Search/Create/Edit/Link Issues
- Assign User to the Issue
- Transition Issues

- Change Assignee of the Issue
- Change Reporter of the Issue

The Tenable for Jira Cloud workflow uses OPEN, RESOLVED, and REOPENED statuses:

Edit the Configuration

Required User Role: Administrator

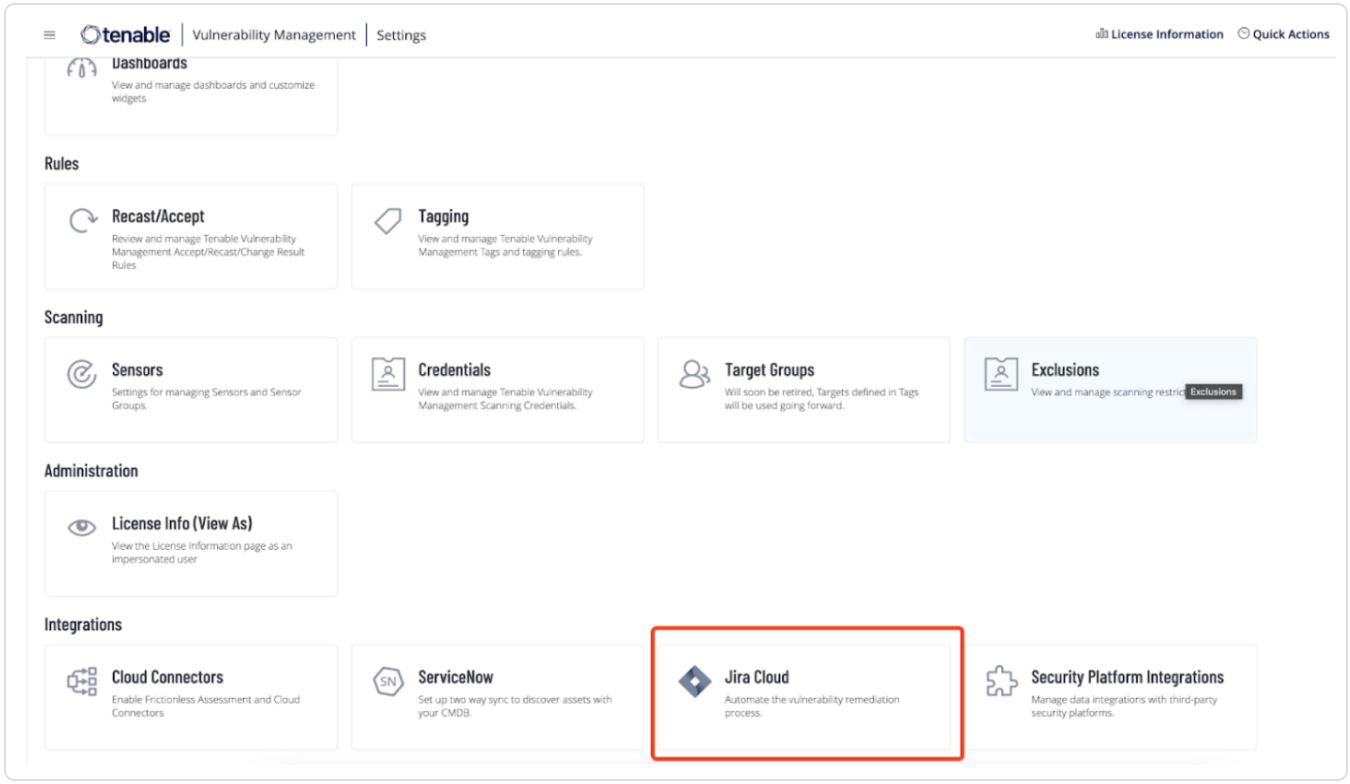
You can re-configure the Tenable for Jira Cloud integration.

To edit the configuration:

1. Log in to Tenable Vulnerability Management.
2. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.
3. In the left navigation plane, click **Settings**.

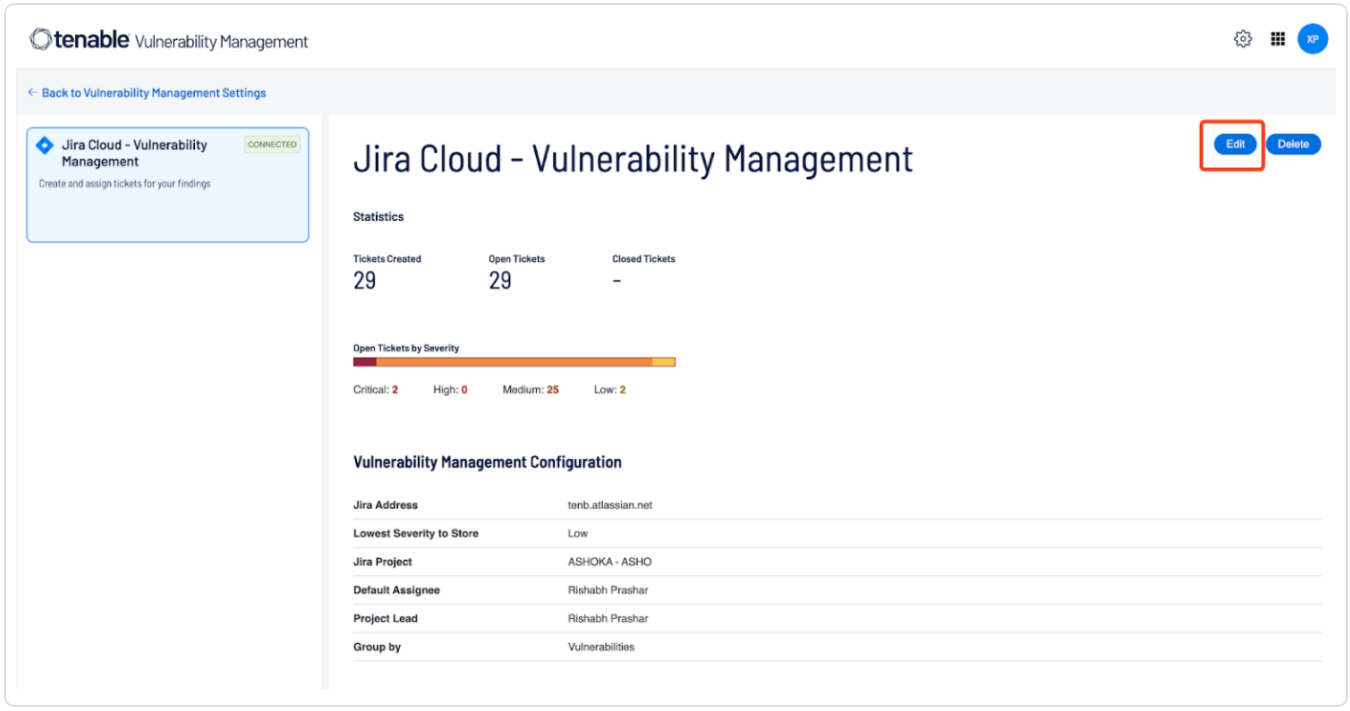
   The **Settings** page appears:



4. In the Integrations section, click the **Jira Cloud** tile.

   The **Jira Cloud - Vulnerability Management** dashboard appears.

5. Click **Edit**.


tenable Vulnerability Management
XP
Back to Vulnerability Management Settings
Jira Cloud - Vulnerability Management
CONNECTED
Create and assign tickets for your findings
Jira Cloud - Vulnerability Management
Edit
Delete
Statistics
Tickets Created
29
Open Tickets
29
Closed Tickets
-
Open Tickets by Severity
Critical: 2
High: 0
Medium: 25
Low: 2
Vulnerability Management Configuration
Jira Address
tenb.atlassian.net
Lowest Severity to Store
Low
Jira Project
ASHOKA - ASHO
Default Assignee
Rishabh Prashar
Project Lead
Rishabh Prashar
Group by
Vulnerabilities

Delete the Configuration

Required User Role: Administrator

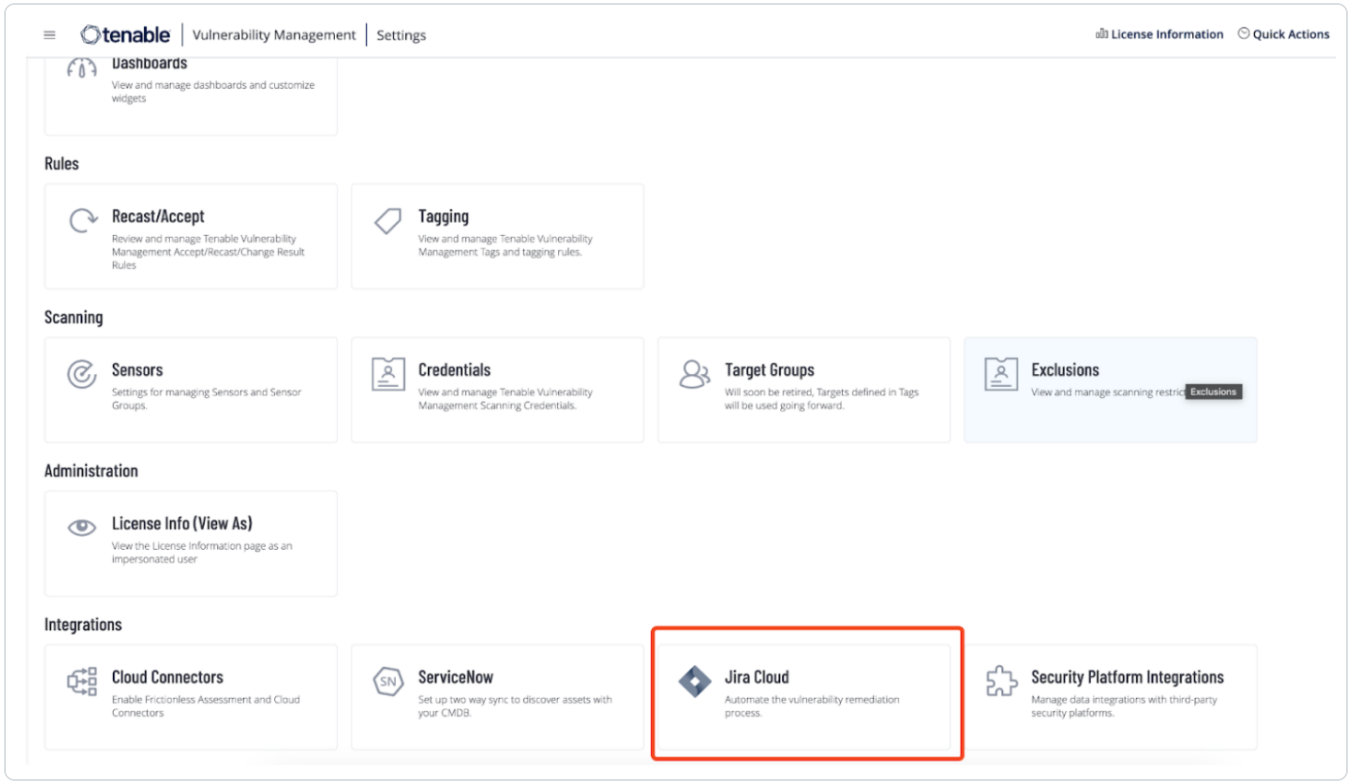
You can re-configure the Tenable for Jira Cloud integration.

To edit the configuration:

1. Log in to Tenable Vulnerability Management.
2. In the upper-left corner, click the ☰ button.

   The left navigation plane appears.
3. In the left navigation plane, click **Settings**.

   The **Settings** page appears:



4. In the Integrations section, click the **Jira Cloud** tile.

   The **Jira Cloud - Vulnerability Management** dashboard appears.

5. Click **Delete**.