How-to Guide: Tenable.io Plugin for JIRA

Last Revised: November 21, 2018

Table of Contents

Welcome to Tenable.io for JIRA

This documentation provides the installation and configuration steps for adding Tenable.io for JIRA. This plugin receives vulnerabilities from Tenable.io on a scheduled basis and creates JIRA issues for each vulnerability in the project that you specify. For every affected host, a sub-task issue is created beneath that vulnerability. As hosts are remediated, the sub-task is automatically marked as resolved.

The Vulnerability Issue and Vulnerable Host Issue have titles automatically generated using the following formula.

- Vulnerability Title = pluginname + protocol + port + severity
- Vulnerable Host Title = Asset_IP + FQDN

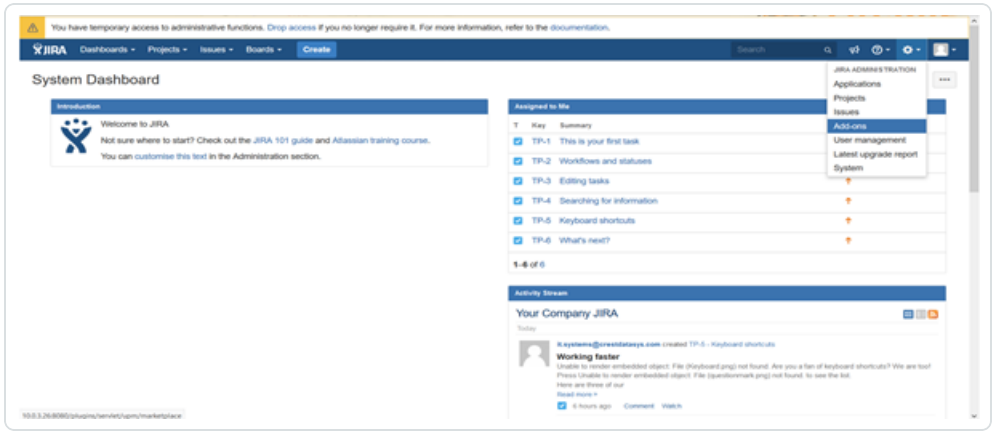
Installation

Before you begin

- You must have administrative access privileges.

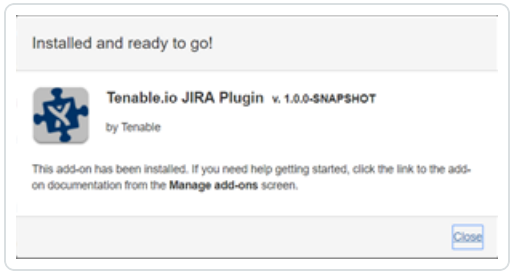
To install Tenable.io for JIRA:

1. Log in to JIRA.
2. Click **Settings** > **Add-ons**.



3. Click **Manage Add-ons**.
4. Click the **Upload Add-on** link.
5. Go to the Tenable Integrations Downloads page.
6. Select the OBR file you want to add.
7. Click **Upload**.

   A confirmation appears.



8. Click **Close**.
9. Refresh the page.

Verify the installation

1. Click **Manage Add-ons** > **User Installed Add-ons**.
2. **Tenable.io for JIRA** appears.

> **Note:** You can also verify the installation by viewing the Tenable.io Configuration in the left panel.

Configuration

Complete the following steps to configure Tenable.io for JIRA.

1. Configure Tenable.io for JIRA
2. Reset the Add-on
3. Add Project to JIRA

Configure Tenable.io for JIRA

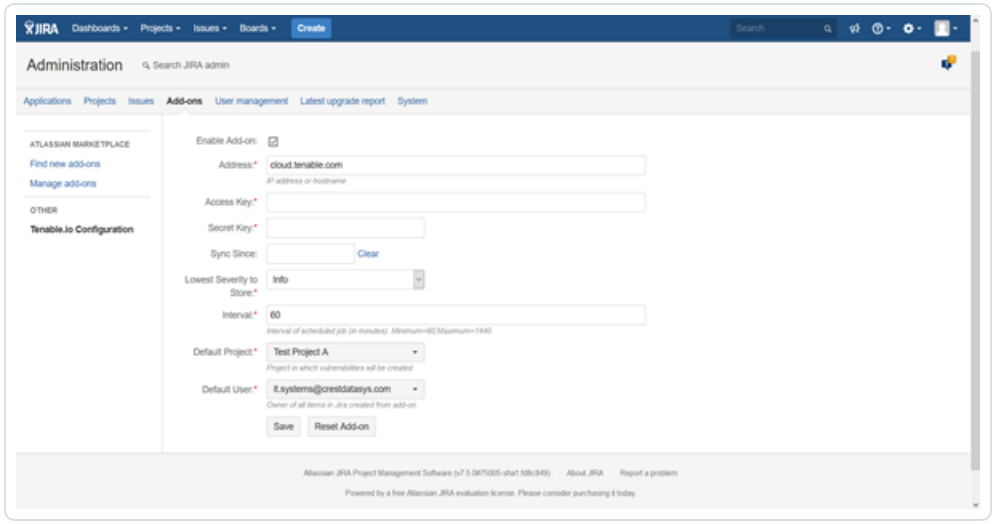
Before you begin

- You must have administrative access privileges.

To configure Tenable.io for JIRA:

1. Log in to JIRA.
2. Click **Settings** > **Add-ons**.
3. Click **Tenable.io Configuration**.

   The **Tenable.io Configuration** page appears.



4. Use the table below to fill in the appropriate JIRA fields.

Field Name	Description	Input
Enable Add-on	(Optional) This allows the system to start data collection. If you want to stop data collection, you must deselect this. If it is selected again, it starts data collection from where it stopped.	Check-box
Address	The data collection source.	IP address / hostname
Access	Ensures user account authentication.	User access key
Secret Key	Ensures user account authentication	User secret key
Sync Since	(Optional) Sets the day to start vulnerability collection. If it is blank, it will collect all.	Date
Lowest Severity to Store	Determines the lowest level of severity that the system stores.	Drop-down selection - info, low, medium, high, or critical.
Interval	Sets the interval of time that the system collects vulnerabilities.	Value in minutes - must be between 60 and 1440 minutes
Default Project	Sets the project in which new Vulnerability issues are automatically created. **Caution:** You cannot change the project once it is saved. You can only change the project if you reset add-on.	Drop-down selection
Default User	Sets the user for the vulnerability host.	Drop-down selection

5. Click **Save**.

Reset Add-on

Changing the JIRA project in which vulnerabilities are created cannot be performed unless you also reset the plugin. This avoids conflicts between vulnerabilities created in previous projects and new projects. When you reset the plugin, it returns to a **Factory New** status and begins the sync from the selected **Sync Since** date.

1. Repeat configuration steps.
2. Click **Reset**.

Add Projects to JIRA

Before you begin

- You must have administrative access privileges.

To add projects to JIRA:

1. Log in to JIRA.
2. Click **Settings** > **Projects**.
3. Click **Create Project**.
4. Select the project you installed in the add-on.

   > **Note:** It can be one of the following types of projects: Scrum software development, Kanban software development, basic software development, project management, task management, or process management.

5. Click **Next**.
6. Click **Select**.
7. Enter a **Name** for the project.
8. (Optional) Modify the automatically generated **Project Key**.
9. (Optional) Update the project lead.
10. Click **Submit**.

Search

See the following sections for steps on how to perform searches in Tenable.io for JIRA.

- Search for Vulnerabilities
- Search for Scheduler Job Information
- Search for System Information

Search for Vulnerabilities

You can use the Tenable.io for JIRA tool to search for specific vulnerabilities. You can perform basic, custom field, and advanced searches.

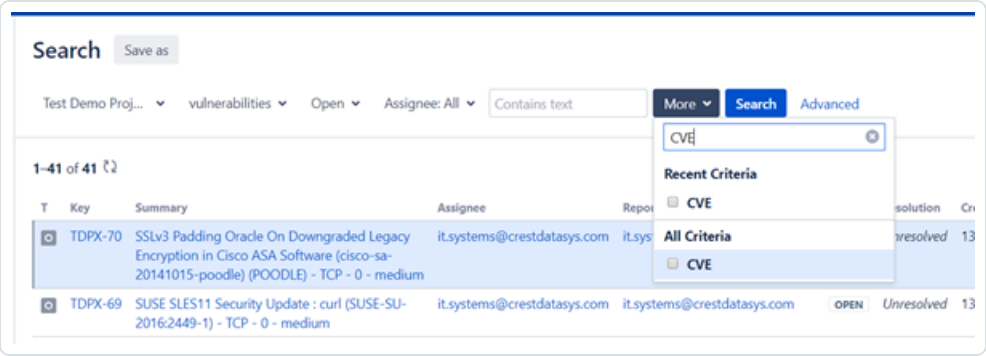
Basic Search

1. In the top navigation bar, click **Issues** > **Search for Issues**.
2. Select the **Project**, **Type**, and **Status**.
3. Click **Search**.

Custom Field Search

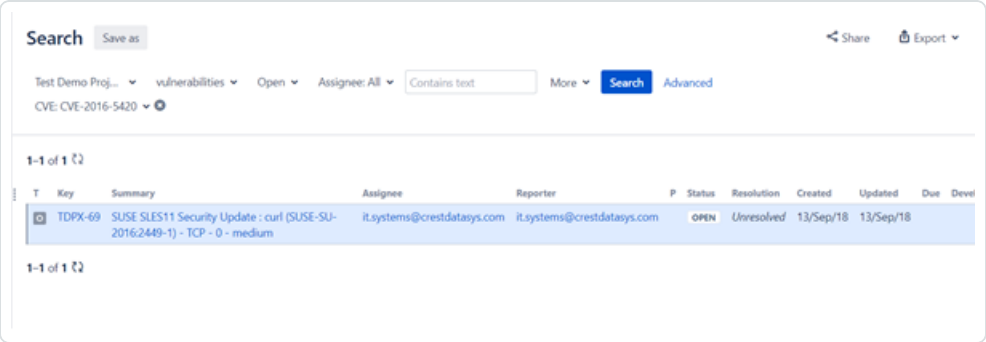
1. In the top navigation bar, click **Issues** > **Search for Issues**.
2. Select the **Project**, **Type**, and **Status**.
3. In the row of **Search** options, click **More** .

   A drop-down appears.



4. In the text box in the drop-down, enter the custom type, i.e., CVE, BDE, etc.

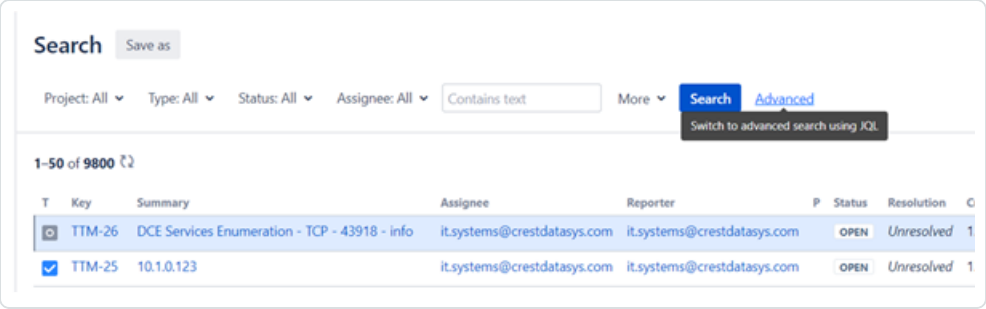
   Results appear below.
5. Select a custom field from the drop-down (such as CVE or hostname).
6. Enter the search value in the text box (for example, enter CVE-2016-5420).



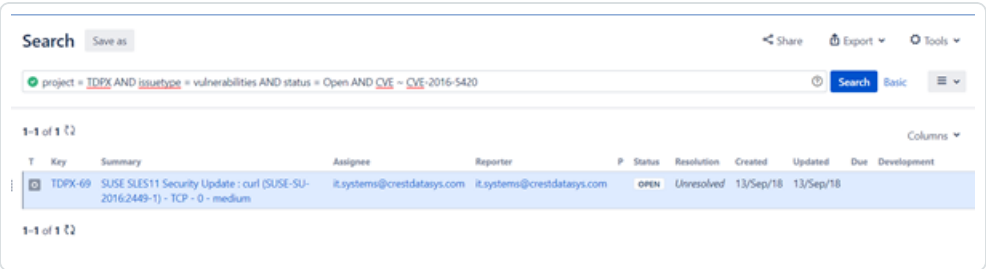
Advanced Search

1. In the top navigation bar, click **Issues** > **Search for Issues**.
2. Select the **Project**, **Type**, and **Status**.
3. In the **Search** options row, click **Advanced**.

   A text box appears.



4. Enter a query or specific vulnerability information in the text box.



5. Click **Search**.

Search for Scheduler Job Information

Before you begin

- You must have administrative access privileges.

To search for scheduler job information:

1. Log in to JIRA.
2. Click **Settings** > **System**.
3. Click **General Configuration** > **Scheduler Details**.
4. Navigate to com.tenable.jira.plugin.scheduler.impl.TenableJobRunnerImpl.
5. Click to view the logs pertaining to the scheduled task.

Search for System Information

Before you begin

- You must have administrative access privileges.

Complete the following steps to add the Tenable.io Add-on to Jira.

1. Log in to Jira.
2. Click **Settings** > **System**.
3. Click **General Configuration** > **System Info**.

   A search box appears.
4. Search for Tenable.

   > **Note:** You can search for all parameters on the configuration page.

Additional Information

See the following sections for additional information.

Troubleshooting

Custom Fields Created in JIRA

Data Collection APIs

You can use the API to submit data to collection servers using standard HTTP techniques. Use the data collection APIs to view the form encoding. This plugin uses the following Tenable.io API endpoints to communicate:

- https://cloud.tenable.com/vulns/export
- https://cloud.tenable.com/vulns/export/{id}/status
- https://cloud.tenable.com/vulns/export/{id}/chunks/{chunk_id}

Troubleshooting

1. **Which JIRA versions are supported?**

   Tenable.io for JIRA is supported for use with JIRA version 7.5+.

2. **Can I create a custom field in the JIRA project used by Tenable.io?**

   No, we strongly advise that you do not create any custom fields in the JIRA project used to sync to Tenable.io vulnerabilities. This is recommended to prevent an override or collide with our custom fields.

3. **Can I create a custom workflow in the JIRA project used by Tenable.io?**

   Yes, you can create a custom workflow for your tickets and have different auto-assign or notification rules.

4. **Will I get updates for manually deleted or moved JIRA tickets?**

   If you manually delete or move a JIRA ticket (Vulnerability or Vulnerable Host), you may not get updates for future events that occur for that same vulnerability.

5. **Where do I look if I encounter an issue?**

   Refer to the tenable.log log file.

Custom Fields Created in JIRA

Issue Type – Vulnerability

- BID - textarea
- CVE - textarea
- CVSSv3 Base Score - readonlyfield
- CVSSv3 Temporal Score - readonlyfield
- CVSSv2 Base Score - readonlyfield
- CVSSv2 Temporal Score - readonlyfield
- Plugin Family - readonlyfield
- Plugin ID - readonlyfield
- MS Bulletin - readonlyfield
- Vulnerability Title - readonlyfield
- Solution - readonlyfield
- Severity Default - readonlyfield

Issue Type – Vulnerable Host

- Agent UUID - readonlyfield
- Device Type - readonlyfield
- FQDN - readonlyfield
- Hostname - readonlyfield
- Asset UUID - readonlyfield
- IPv4 - readonlyfield
- IPv6 - readonlyfield
- MAC Address - readonlyfield
- NetBIOS Name - readonlyfield
- Operating System - readonlyfield
- Output - textarea

- Port - readonlyfield
- Protocol - readonlyfield
- Service - readonlyfield
- Severity - readonlyfield
- First Found - readonlyfield
- Last Fixed - readonlyfield
- State - readonlyfield