# How-to Guide: Tenable Plugin for JIRA

Last Revised: March 09, 2020

# Table of Contents

# Welcome to the Tenable Plugin for JIRA

The Tenable Plugin for JIRA provides users with the organizational convenience of managing vulnerabilities detected in Tenable.io and Tenable.sc. When you install the plugin, custom fields are created in JIRA. The application uses these custom fields to organize and manage vulnerabilities detected when running vulnerability scans.

The Tenable Plugin for JIRA receives vulnerability data from Tenable.io and Tenable.sc on a scheduled basis and creates JIRA issues for each vulnerability in the project that you specify. The application creates JIRA tickets according to the following:

- For every vulnerability plugin, we create a vulnerability issue.
- For every effected asset, we create a vulnerable host issue and blocking link to the related vulnerability issue. A linked issue is created under the vulnerability task.
- As assets are remediated, vulnerable host ticket are marked resolved.
- If all vulnerable host issues related a to a vulnerability issue are marked resolved, the vulnerability issue is marked 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 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 Tenable.io assets are marked as terminated or deleted, the integration resolves all related vulnerable host issues
- All data imports from Tenable.io use the last_found/last_seen fields. This ensures that all issues are updated whenever new information becomes available.
- All data imports from Tenable.sc use the last_found/last_seen fields. This ensures that all issues are updated whenever new information becomes available.

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

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

In Tenable.sc, the vulnerability issue and vulnerable host Issue titles are automatically generated using the following formula:

- Vulnerability = pluginname + protocol + port + severity
- Vulnerable Host = IPV4 + dnsName + repositoryid

# Prerequisites

You must meet the following prerequisites before installing and using the plugin:

- Install the compatible Tenable plugin for your JIRA version. For version compatibility, see the version compatibility table below.
- If integrating with Tenable.sc, use Tenable.sc version 5.7 or later.
- Be a member of one of the following user groups in JIRA - jira-administrators, jira-software-users, jira-core-users, or jira-servicedesk-users.
- Projects cannot have mandatory fields or configured validators.

## Version Compatibility

| Software | JIRA Version | Tenable Plugin Version |
|---|---|---|
| JIRA Software | 7.5 - 7.x | 2.x |
| JIRA Core | 7.5 - 7.x | 2.x |
| JIRA Service Desk | 3.15 - 3.x | 2.x |
| JIRA Software | 8.x | 10.x |
| JIRA Core | 8.x | 10.x |
| JIRA Service Desk | 8.x | 10.x |

# Custom Fields Created in JIRA

Custom fields are created when the Tenable Plugin for JIRA is installed. Custom fields are either text area, which you can modify, or *read only field*, which you cannot modify.

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

## 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 Temporal Score | read only field | The CVSSv2 temporal score (characteristics of a vulnerability that change over time but not among user environments). |
| Tenable Plug-in Family | read only field | The family of the plugin that identified the vulnerability. For more information about plugin families, see https://www.ten- |

| | | |
|---|---|---|
| | | able.com/plugins. |
| Tenable Plug-in 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 recast the risk associated with the vulnerability. |
| Tenable Source | read only field | Determines if the application is connected to Tenable.io or Tenable.sc. |
| Tenable Short Description | read only field | A short description of the plugin. |

## 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 host name 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 Operating System | read only field | The operating system 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:<br>• info - The vulnerability has a CVSS score of 0.<br>• low - The vulnerability has |

| | | |
|---|---|---|
| | | a CVSS score between 0.1 and 3.9.<br>• medium - The vulnerability has a CVSS score between 4.0 and 6.9.<br>• high - The vulnerability has a CVSS score between 7.0 and 9.9.<br>• 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.io 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.io state service. Possible values are:<br>• open - The vulnerability is currently present on an asset.<br>• reopened - The vulnerability was previously marked as fixed on an asset, but has been detected again by a new scan.<br>• 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.io or Tenable.sc. |
| Tenable.sc Repository ID | read only field | The repository identification manager. |
| Tenable.sc Repository Name | read only field | A user friendly name for the repository. |

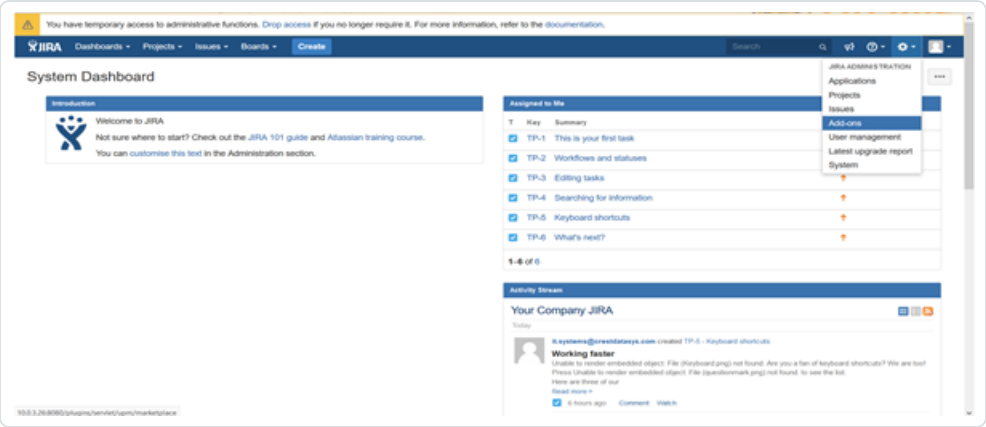
# Install

## Before you begin

- You must meet the requirements on the Prerequisites page.
- You must have administrative access privileges in JIRA.
- Download the Tenable Plugin for JIRA OBR file to your computer from the Tenable Integrations Downloads page.

## To install the Tenable Plugin for JIRA:

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




3. In the left column, click **Manage apps**.

   The **Manage apps** page appears.
4. At the top of the **Manage apps** section page, click **Upload app**.

   The **Upload app** window appears.
5. Select the Tenable Plugin for JIRA OBR file you downloaded.
6. Click **Upload**.

   A new window displays the installation progress.

   After the installation completes, a confirmation appears.

7. Click **Close** to close the confirmation window.
8. To see the installation update, refresh the page.
9. To confirm the installation was successful, click **Manage apps** > **User Installed Add-ons**.

   If the installation was successful, the Tenable Plugin for JIRA appears in the list of add-ons.

**Note:** You can also verify the installation by viewing the **Tenable.io Configuration** section in the left navigation pane of the **Add-ons** page.

# Configure

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

Initial Configuration

1. Add Project to JIRA
2. Configure Tenable.io for JIRA or

   Configure Tenable.sc for JIRA
3. Set Log Level

After Initial Configuration

1. Reset the Add-on

# Configure Tenable.io

## Before you begin

- Install the Tenable Plugin for JIRA.
- In JIRA, identify or ceate the project where you want the plugin to create vulnerability issues.
- You must have the Administrator role in Tenable.io.

  > **Note:** See the Tenable.io User Guide for information about user role configuration.

- You must have administrative access privileges in JIRA.
- You must have your Tenable.io API keys. See the Tenable.io User Guide for instructions on how to generate an API key.

> **Note**: You must use a unique user (API key).

> **Note:** Make sure the unique user (API key) has the correct access group assigned to it.

## To configure Tenable.io:

1. Log in to JIRA.
2. Click ⚙ > **Add-ons**.
3. In the left navigation pane, click **Tenable.io Configuration**.

   The **Tenable.io Configuration** page appears.
4. Use the table below to fill in the appropriate JIRA options.

| Option Name | Description | Input |
|---|---|---|
| Enabled | (Optional) When enabled, Tenable.io starts collecting data. When disabled, Tenable.io stops collecting data.<br><br>**Note:** If you stop data collection, then start it again, Tenable.io provides data from the point where you previously stopped. | Check box |

| | | |
|---|---|---|
| Address | The data collection source. | IP address or hostname |
| Access Key | Ensures user account authentication. | User access key |
| Secret Key | Ensures user account authentication | User secret key |
| Sync Since | (Optional) Specifies the start date of the vulnerability data you want to collect from Tenable.io. If you do not specify a start date, data collection starts from the last date you last enabled data collection.<br><br>**Caution:** If this option is changed, you must click the **Reset Add-on button** to save this change. | Date<br><br>mm/dd/yyyy hh:mm |
| Lowest Severity to Store | Specifies the lowest level of severity of the vulnerabilities you want to collect from Tenable.io.<br><br>Tenable.io severity levels include the following:<br><br>• **info** - The vulnerability has a CVSS score of 0<br>• **low** - The vulnerability has a CVSS score between -.1 and 3.9.<br>• **medium** - The vulnerability has a CVSS score between 4.0 and 6.9.<br>• **high** - The vulnerability has a CVSS score between 7.0 and 9.9<br>• **critical** - The vulnerability has a CVSS score of 10.0 | Drop-down box |
| Interval | Specifies the interval, in minutes, at which JIRA queries Tenable.io for vulnerability data. This interval must be set between 60 and 1,440 minutes. | Minutes |
| Default Project | Specifies the project where JIRA creates new vulnerability issues. | Drop-down box |

| | | |
|---|---|---|
| | **Caution:** If you change this option after initial configuration, you must click **Reset Add-On** to save your change. | |
| Default User | Specifies the user to whom the plugin automatically assigns the vulnerability issues.<br><br>**Note:** The list only displays users that are members of the following groups: jira-administrators, jira-software-users, jira-core-users, and jira-servicedesk-users. | Drop-down box |
| Enable Proxy | (Optional) Enables the plugin to collect Tenable.io data via a proxy server. If you select this option, the plug- in prompts you to enter the following:<br>• **URL** - (Required) The URL of the proxy server.<br>• **Username** - (Optional) The username that JIRA uses to connect to the proxy server.<br>• **Password** - (Optional) The password that JIRA uses to connect to the proxy server.<br><br>**Note:** The username and password are optional if you use a proxy without authentication. | Check box and text boxes |

5. Click **Save**, or if you have changed the **Default Project** or **Sync Since** options, click **Reset Add-on**.
6. Once the configuration is saved, the plugin creates custom fields in JIRA.

# Configure Tenable.sc

## Before you begin

- You must have Tenable.sc 5.7+.
- You must have the Security Manager role in Tenable.sc.

  > **Note:** See the Tenable.sc User Guide for information about user role configuration.

- Install the Tenable Plugin for JIRA.
- In JIRA, identify or ceate the project where you want the plugin to create vulnerability issues.
- You must have administrative access privileges in JIRA.

## To configure Tenable.sc:

1. Log in to JIRA.
2. Click ⚙ > **Add-ons**.
3. In the left navigation pane, click **Tenable.sc Configuration**.

   The **Tenable.sc Configuration** page appears.
4. Use the table below to fill in the appropriate JIRA options.

| Option Name | Description | Input |
|---|---|---|
| Enabled | (Optional) When enabled, Tenable.sc starts collecting data. When disabled, Tenable.sc stops collecting data.<br><br>**Note:** If you stop data collection, then start it again, Tenable.sc provides data from the point where you previously stopped. | Check box |
| Address | The data collection source. | IP address or hostname |
| Username | Ensures user account authentication. | The user-name for Tenable.sc |

| | | |
|---|---|---|
| Password | Ensures user account authentication | The password for Tenable.sc |
| Sync Since | (Optional) Specifies the start date of the vulnerability data you want to collect from Tenable.sc. If you do not specify a start date, data collection starts from the last date you last enabled data collection.<br><br>**Caution:** If this option is changed, you must click the **Reset Add-on button** to save this change. | Date<br><br>mm/dd/yyyy hh:mm |
| Lowest Severity to Store | Specifies the lowest level of severity of the vulnerabilities you want to collect from Tenable.sc.<br><br>Tenable.sc severity levels include the following:<br><br>• **info** - The vulnerability has a CVSS score of 0<br>• **low** - The vulnerability has a CVSS score between -.1 and 3.9.<br>• **medium** - The vulnerability has a CVSS score between 4.0 and 6.9.<br>• **high** - The vulnerability has a CVSS score between 7.0 and 9.9<br>• **critical** - The vulnerability has a CVSS score of 10.0 | Drop-down box |
| Interval | Specifies the interval, in minutes, at which JIRA queries Tenable.sc for vulnerability data. This interval must be set between 60 and 1,440 minutes. | Minutes |
| Default Project | Specifies the project where JIRA creates new vulnerability issues.<br><br>**Caution:** If you change this option after initial configuration, you must click **Reset Add-On** to save your change. | Drop-down box |

| | | |
|---|---|---|
| Default User | Specifies the user to whom the plugin automatically assigns the vulnerability issues.<br><br>**Note:** The list only displays users that are members of the following groups: jira-administrators, jira-software-users, jira-core-users, and jira-servicedesk-users. | Drop-down box |
| Enable Proxy | (Optional) Enables the plugin to collect Tenable.sc data via a proxy server. If you select this option, the plug- in prompts you to enter the following:<br><br>• **URL** - (Required) The URL of the proxy server.<br>• **Username** - (Optional) The username that JIRA uses to connect to the proxy server.<br>• **Password** - (Optional) The password that JIRA uses to connect to the proxy server.<br><br>**Note:** The username and password are optional if you use a proxy without authentication. | Check box and text boxes |

5. Click **Save**, or if you have changed the **Default Project** or **Sync Since** options, click **Reset Add-on**.
6. Once the configuration is saved, the plugin creates custom fields in JIRA.

# Add Projects to JIRA

You can add projects to JIRA to manage Tenable vulnerabilities.

**Note:** Users who manage projects must have the following permissions selected: create issue, edit issue, resolve issue, and link issue. You can set these permissions in the permissions section of the JIRA Plugin for Tenable.io configuration page. For additional information about permissions, see the JIRA documentation.

## Before you begin

- You must have administrative access privileges in JIRA.

## To add projects to JIRA:

1. Log in to JIRA.
2. Click ⚙ > **Projects**.
3. Click the **Create Project** button.
4. Select **Tenable Vulnerability Management** (recommended) or any type that you want.

   **Note:** Do one of the following:

   - If you configured the Tenable Plugin for JIRA, select **Tenable Vulnerability Management**. Tenable recommends you use this project type for managing vulnerability issues in JIRA.
   - If you have not configured the Tenable Plugin for JIRA, select any project type. The plugin automatically adds custom fields, issue types, and workflow when you enable the integration.

5. Click **Next**.
6. Type the information in the corresponding fields.

| Option Name | Description |
|---|---|
| Name | The name of the project. |
| Project Key | (Optional) A unique key identifying the project in JIRA. This value is automatically populated when you type the project name. However, you can manually |

| | |
|---|---|
| | change it. |
| Project Lead | (Optional) The JIRA user who owns the project. |

**Note:** Depending on the project type you select, JIRA may prompt you for additional project configuration. For more information, see the Atlassian JIRA documentation.

7. Click **Submit**.

   The **New Project** window opens.

**Note:** The empty project syncs once you select this project as your **Default Project** on the Tenable.io Configuration or Tenable.sc Configuration page.

# Set Log Level

You can set or modify the log level for the Tenable Plugin for JIRA.

## Before you begin

- You must have administrative access privileges in JIRA.

## To set the log level:

1. Log in to JIRA.
2. Click > **System**.

   The **System** page appears.
3. In the left-hand column, click **Logging and Profiling**.

   The log file page appears.
4. Scroll to the **Default Loggers** section.
5. Click the desired setting for the **Set Logging Level** option.

# Reset Plugin

You must reset the Tenable Plugin for JIRA if you want to change the plugin configuration any time after JIRA has created an issue for a Tenable vulnerability. 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**.

# Manage

See the following sections for steps on managing the Tenable Plugin for JIRA.

- Sync Add-on
- Search for Vulnerabilities
- Search for Scheduler Job Information
- Search for System Information
- Upgrade
- Disable
- Uninstall

# Sync JIRA Issues with the Tenable Plugin for JIRA

Use the **Sync** option to start data collection.

To sync JIRA issues with the plugin:

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

   The selected configuration page appears.
4. Click the **Sync** button.

   A **Warning** appears.
5. Click **Yes** to start the sync.

   **Note:** The data collection starts from last time you enabled data collection.

# Search for Vulnerabilities

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

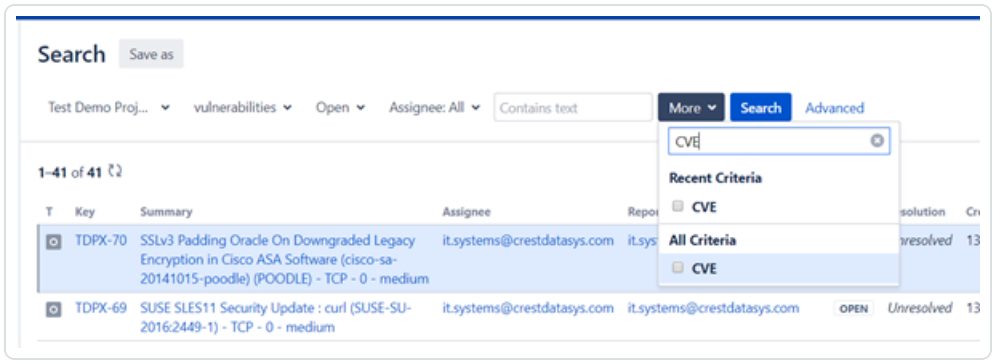
## Basic Search

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

## Custom Field Search

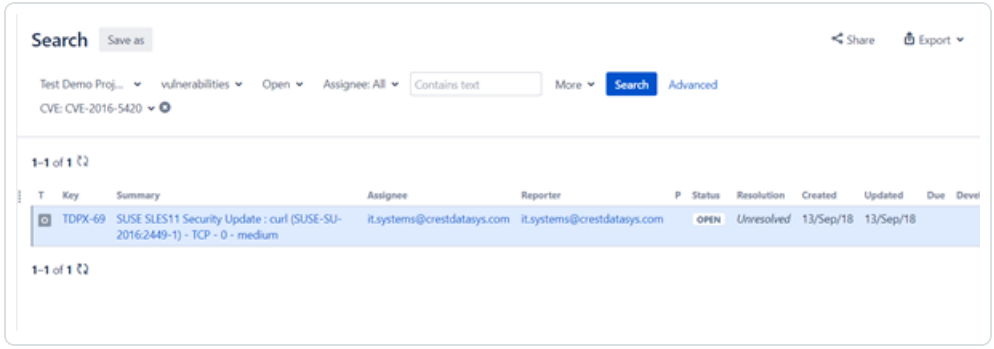
1. In the top navigation bar, click **Issues** > **Search for Issues**.
2. Select the **Project**, **Type**, and **Status**.
3. In the row of **Search** options, click **More** .

   A drop-down box appears.




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

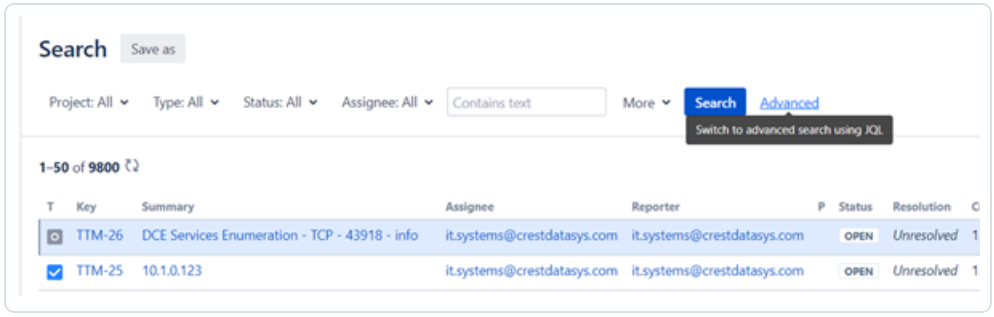
   Results appear below.
5. From the drop-down box, select a custom field.
6. Enter the search value in the text box (for example, enter CVE-2016-5420).



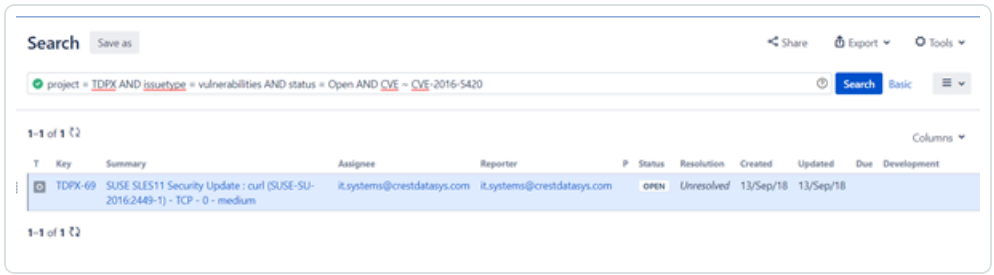

## Advanced Search

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

You can use the Tenable Plugin for JIRA to search for scheduler information.

## Before you begin

- You must have administrative access privileges.

## To search for scheduler job information:

1. Log in to JIRA.
2. Click ⚙ > **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 in JIRA.

## To search for system information:

1. Log in to JIRA.
2. Click ⚙ > **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.

# Upgrade Add-on

To upgrade to the latest version of the Tenable Plugin for JIRA:

1. Follow the installation steps.
2. Verify your credentials.
    - For Tenable.io, re-enter your API keys.
    - For Tenable.sc, re-enter your username and password.
3. Click **Save**.

> **Note:** After the upgrade, and re-entering your credentials, the data collection automatically starts from the last sync.

# Disable the Tenable Plugin for JIRA

## Before you begin

- You must have administrative access privileges.

To uninstall the add-on:

1. Log in to JIRA.
2. Click ⚙ > **Add-ons**.
3. In the left column, click **Manage apps**.

   The **Manage apps** page appears.
4. Scroll to find the **Tenable.io JIRA Plugin** or **Tenable.sc JIRA Plugin** application listing.
5. Click to expand the **Tenable.io JIRA Plugin** or **Tenable.sc JIRA Plugin** application listing.
6. Click the **Disable** button.

   The plugin is disabled and the syncing stops.

**Note:** The scheduler details are removed from the scheduler detail page when the add-on is disabled.

**Note:** If the add-on is uninstalled or disabled, the configuration details remain stored on the **System Info** page.

# Uninstall the Add-on

## Before you begin

- You must have administrative access privileges.

To uninstall the add-on:

1. Log in to Jira.
2. Click ⚙ > **Add-ons**.
3. In the left column, click **Manage apps**.

   The **Manage-apps** page appears.
4. Scroll to find **Tenable.io JIRA Plugin** or **Tenable.sc JIRA Plugin**.
5. Click to expand the **Tenable.io JIRA Plugin** or **Tenable.sc JIRA Plugin** option.
6. Click the **Uninstall** button.

   The **Uninstall app** window appears.
7. Click **Uninstall app**.

**Note:** If the add-on is uninstalled or disabled, the configuration details remain stored on the **System Info** page.

# Troubleshooting

1. **Can I create a custom field in the Tenable Plugin for JIRA?**

   No, Tenable strongly advises that you do not create any custom fields in the JIRA project used to sync to Tenable vulnerabilities. This prevents an override or collide with our custom fields.

2. **Can I create a custom workflow in the Tenable Plugin for JIRA?**

   No, you cannot create a custom workflow because the plugin automatically closes tickets based on the workflow statuses.

3. **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.

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

   Refer to the log file located at `/var/atlassian/application-data/jira/log/Atlassian-jira.log`.

5. **The Plugin page in JIRA states *"This add-on is not compatible with your current Jira version."* How do i correct this?**

   Install the correct Tenable plugin for your JIRA version. The version compatibility for your Tenable plugin and JIRA version is located on the Prerequisites page.

# API Usage

View the links below for information about the APIs used by the JIRA plugin to collect and update vulnerabilities imported from Tenable applications.

## Tenable.io

The JIRA plugin uses the following APIs to collect open, reopen, and fix vulnerabilities:

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

The JIRA plugin uses the following APIs to find assets that were terminated or deleted to close the related vulnerable issues for those assets:

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

## Tenable.sc

The JIRA plugin uses the following APIs to collect open, reopen, and fix vulnerabilities:

- https://docs.tenable.com/tenablesc/api/Analysis.html