Tenable Plugin for JIRA Integration Guide

Last Revised: August 03, 2023

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 Vulnerability Management and Tenable Security Center. 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 Vulnerability Management and Tenable Security Center 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 affected 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 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 Tenable Vulnerability Management assets are marked as terminated or deleted, the integration resolves all related vulnerable host issues.
- All data imports from Tenable Vulnerability Management use the `last_found` or `last_seen` fields. This ensures that all issues are updated whenever new information becomes available.
- All data imports from Tenable Security Center use the `last_found` and `last_seen` fields. This ensures that all issues are updated whenever new information becomes available.

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 + FQDN

In Tenable Security Center, 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

Note: When you have an open Jira ticket and the integration closes it, the Tenable app does not update the **Resolution** field in the integration. The **Resolution** field is one of the fields that the Tenable app does not interact with. When you update your Jira ticket from open to closed/fixed/resolved, etc., the **Resolution** field in the Jira integration stays at "Unresolved."

Prerequisites

Meet the following prerequisites before installing and using the on-premises (locally installed) Jira plugin:

- Install the compatible Tenable plugin for your JIRA version. For version compatibility, see the following version compatibility table.
- If integrating with Tenable Security Center, use Tenable Security Center 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	8.5-9.9.0	10.1.8
JIRA Core	8.5-9.9.0	10.1.8
JIRA Service Desk	8.5-9.9.0	10.1.8
JIRA Data Center	8.5-9.9.0	10.1.8

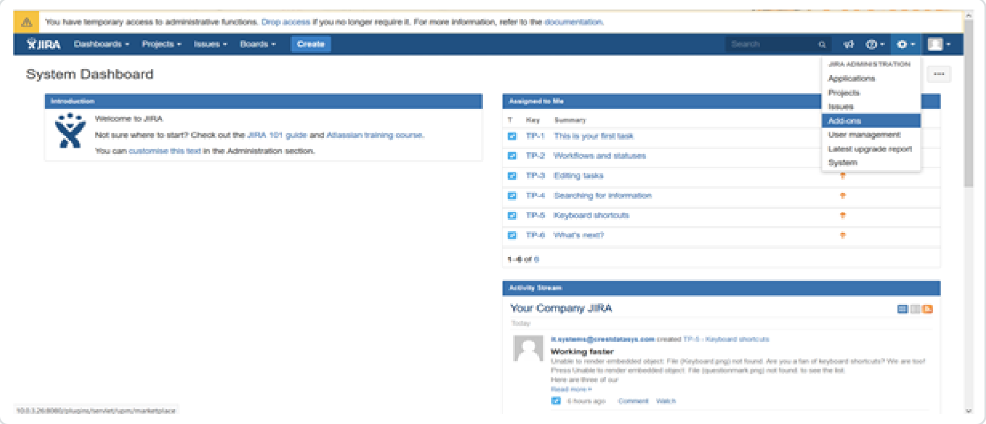
Install

Before you begin:

- 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**.



You have temporary access to administrative functions. Drop access if you no longer require it. For more information, refer to the documentation.

System Dashboard

Welcome to JIRA

Not sure where to start? Check out the JIRA 101 guide and Atlassian training course.

You can customise this text in the Administration section.

T	Key	Summary
☑	TP-1	This is your first task
☑	TP-2	Workflows and statuses
☑	TP-3	Editing tasks
☑	TP-4	Searching for information
☑	TP-5	Keyboard shortcuts
☑	TP-6	What's next?

1–6 of 6

Your Company JIRA

Today

it.systems@crestdatasys.com created TP-5 - Keyboard shortcuts

Working faster

Unable to render embedded object: File (Keyboard.png) not found. Are you a fan of keyboard shortcuts? We are too! Press Unable to render embedded object: File (questionmark.png) not found. to see the list.

Here are three of our

Read more »

6 hours ago Comment Watch

10.0.3.26:8080/plugins/servlet/upm/marketplace

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 Vulnerability Management for JIRA or

   Configure Tenable Security Center for JIRA
3. Set Log Level

After Initial Configuration

1. Reset the Add-on

Configure Tenable Vulnerability Management

Before you begin:

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

> **Note:** While configuring Tenable Vulnerability Management or Tenable Security Center for Jira, if you select **Asset** in the **Group By** drop-down for every vulnerability, the integration creates a vulnerability issue and blocking link to the related vulnerable host. The integration creates a linked issue under the vulnerability host issue.

For Tenable Vulnerability Management:

> **Required User Role:** Administrator

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

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

Option Name	Description	Input

Enabled	(Optional) When enabled, Tenable Vulnerability Management starts collecting data. When disabled, Tenable Vulnerability Management stops collecting data. **Note:** If you stop data collection, then start it again, Tenable Vulnerability Management 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 Vulnerability Management . If you do not specify a start date, data collection starts from the last date you last enabled data collection. **Caution:** If this option is changed, you must click the **Reset Add-on button** to save this change.	Date mm/dd/yyyy hh:mm
Lowest Severity to Store	Specifies the lowest level of severity of the vulnerabilities you want to collect from Tenable Vulnerability Management. Tenable Vulnerability Management severity levels include the following: • **info** - The vulnerability has a CVSS score of 0 • **low** - The vulnerability has a CVSS score	Drop-down box

	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.	
Interval	Specifies the interval, in minutes, at which JIRA queries Tenable Vulnerability Management for vulnerability data. This interval must be set between 60 and 1,440 minutes.	Minutes
Group By	Specifies the grouping mechanism to use when creating JIRA tickets. - **Vulnerability** - Ticket will be group by vulnerability ticket. - **Asset** - Ticket will be group by asset ticket. **Note:** This drop-down will only be enabled if you choose a new project in the **Default Project** drop-down.	Drop-down box
Default Project	Specifies the project where JIRA creates new vulnerability issues. **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.	Drop-down box

	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.	
Default Reporter	Specifies the owner of all items in Jira created from add-on. **Note:** The list only displays users that are members of the following group: jira-administrators.	Drop-down box
Enable Proxy	(Optional) Enables the plugin to collect Tenable Vulnerability Management data via a proxy server. If you select this option, the plug- in prompts you to enter the following: • **URL** - (Required) The URL of the proxy server. • **Username** - (Optional) The username that JIRA uses to connect to the proxy server. • **Password** - (Optional) The password that JIRA uses to connect to the proxy server. **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 Security Center

Before you begin:

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

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

- Install the Tenable Plugin for JIRA.
- In JIRA, identify or create the project where you want the plugin to create vulnerability issues.
- You must have administrative access privileges in JIRA.
- For plugin versions 10.1.0 and later, you must use API keys for authentication.

> **Note:** For more information about API keys, see Enable API Key Authentication and Generate API Keys.

> **Note:** While configuring Tenable Vulnerability Management or Tenable Security Center for Jira, if you select **Asset** in the **Group By** drop-down for every vulnerability, the integration creates a vulnerability issue and blocking link to the related vulnerable host. The integration creates a linked issue under the vulnerability host issue.

To configure Tenable Security Center:

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 following table to fill in the appropriate JIRA options.

Option Name	Description	Input
Enabled	(Optional) When enabled, Tenable Security Center starts collecting data. When disabled, Tenable	Check box

	Security Center stops collecting data. **Note:** If you stop data collection, then start it again, Tenable Security Center provides data from the point where you previously stopped.	
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 Security Center. If you do not specify a start date, data collection starts from the last date you last enabled data collection. **Caution:** If this option is changed, you must click the **Reset Add-on button** to save this change.	Date mm/dd/yyyy hh:mm
Lowest Severity to Store	Specifies the lowest level of severity of the vulnerabilities you want to collect from Tenable Security Center. Tenable Security Center severity levels include the following: • **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.	Drop-down box

	• **high** - The vulnerability has a CVSS score between 7.0 and 9.9 • **critical** - The vulnerability has a CVSS score of 10.0	
Query Name	Specifies the user-created query name. (Case Sensitive) **Note:** Select **Vulnerability Detail List** as the tool to use against the data from the drop-down in the top-left of the page.	Drop-down box
Interval	Specifies the interval, in minutes, at which JIRA queries Tenable Security Center 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. **Caution:** If you change this option after initial configuration, you must click **Reset Add-On** to save your change.	Drop-down box
Default Assignee	Specifies the user to whom the plugin automatically assigns the vulnerability issues. **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
Default Reporter	Specifies the owner of all items in Jira created from add-on. **Note:** The list only displays users that are mem-	Drop-down box

	bers of the following group: jira-administrators.	
Enable Proxy	(Optional) Enables the plugin to collect Tenable Security Center data via a proxy server. If you select this option, the plug- in prompts you to enter the following: • **URL** - (Required) The URL of the proxy server. • **Username** - (Optional) The username that JIRA uses to connect to the proxy server. • **Password** - (Optional) The password that JIRA uses to connect to the proxy server. **Note:** The username and password are optional if you use a proxy without authentication.	Check box and text boxes
Verify SSL	If enabled, JIRA verifies the SSL Certificate in Tenable Security Center.	Check box

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 Vulnerability Management 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.

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 Vulnerability Management Configuration or Tenable Security Center Configuration page.

Custom Fields and Filters 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. You can also create filters with the custom fields created in JIRA.

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.

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 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 vul-

		nerability 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.

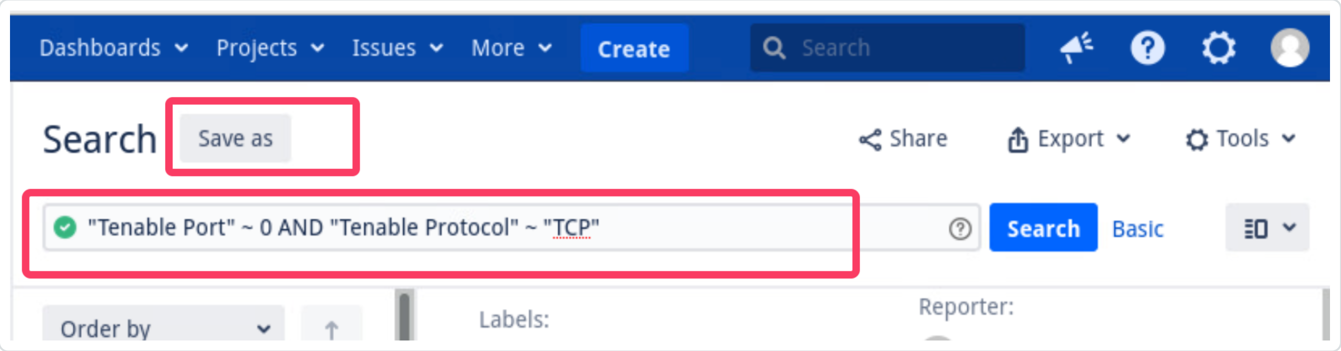
Tenable Severity	read-only field	The severity of the vulnerability as defined using the Common Vulnerability Scoring System (CVSS) base score. Possible values are: • info - The vulnerability has a CVSS score of 0. • low - The vulnerability has a CVSS score between 0.1 and 3.9. • medium - The vulnerability 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.
Tenable Security Center Repository ID	read-only field	The repository identification manager.
Tenable Security Center Repository Name	read-only field	A user-friendly name for the repository.

Create Filters with Custom Fields created in JIRA

To create a filter with custom fields:

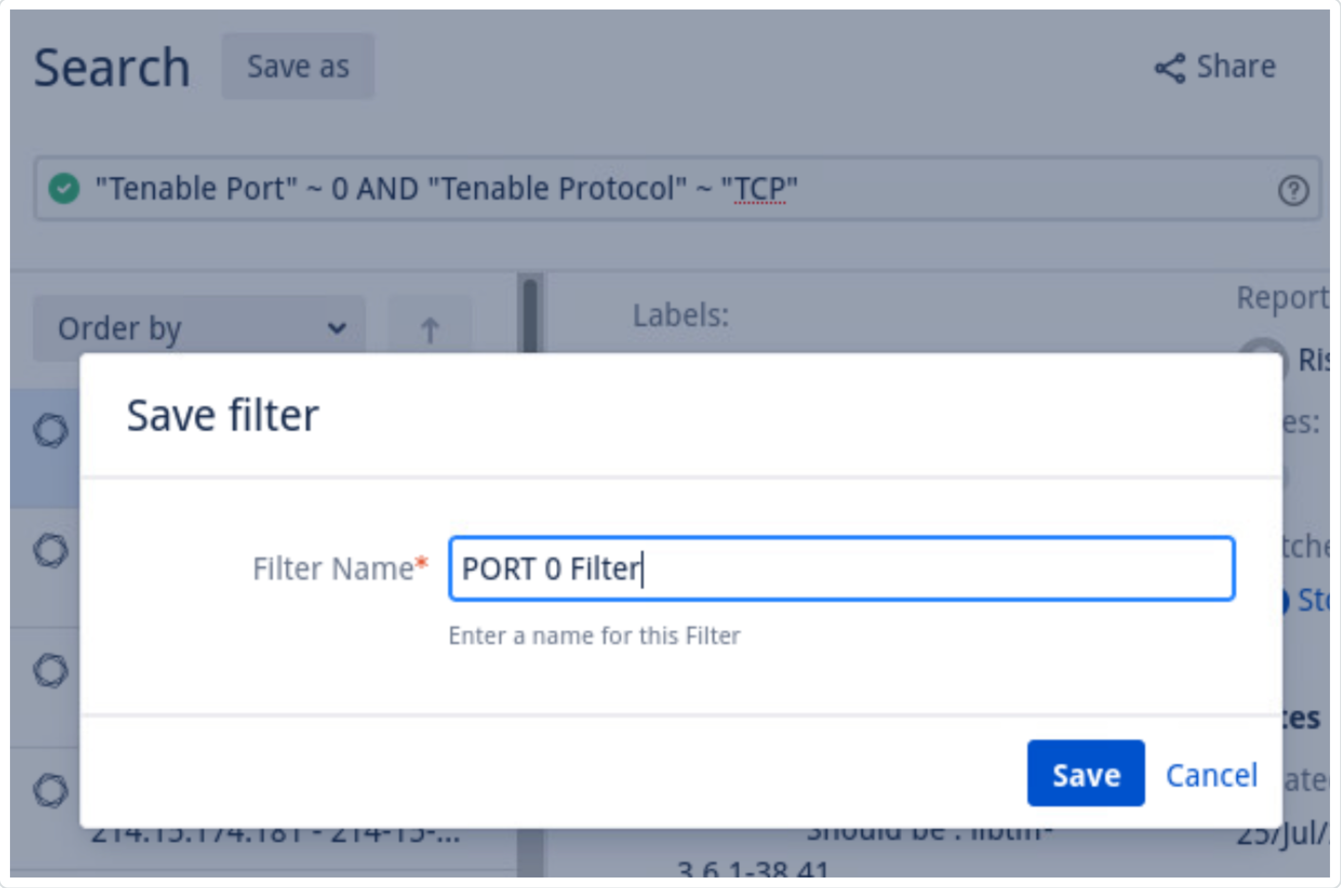
1. Log in to JIRA.
2. In the search bar, enter the custom fields you want to create a filter for.

   "Tenable Port" ~ 0 AND "Tenable Protocol" ~ "TCP"

3. In the upper-left, click **Save as**.

   The **Save filter** pop-up appears.



"Tenable Port" ~ 0 AND "Tenable Protocol" ~ "TCP"

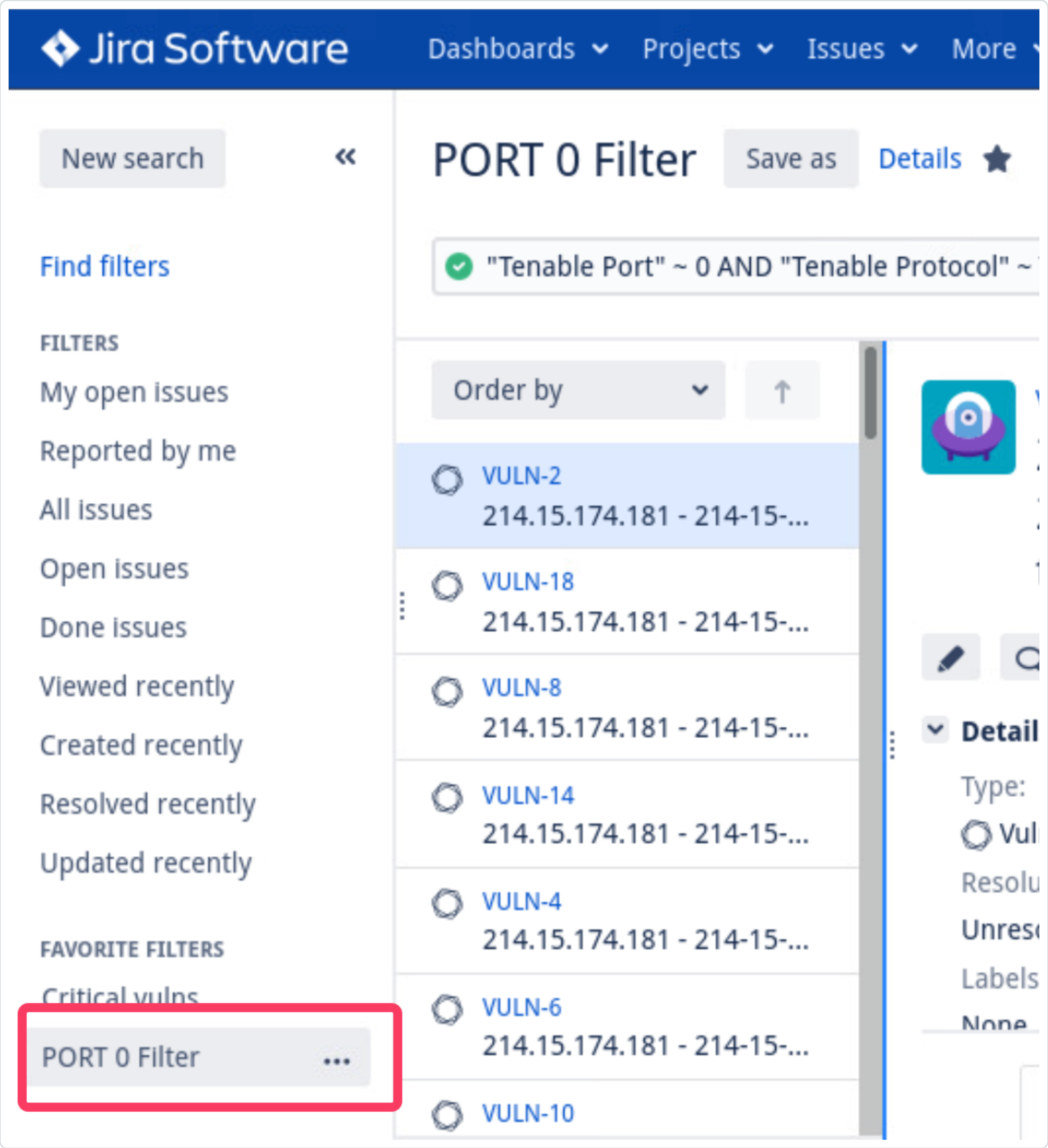
Save filter

Filter Name* PORT 0 Filter

Enter a name for this Filter

4. In the text box, enter a new filter name for your new filter.

   Your new filter appears in your list of filters in the left panel.



PORT 0 Filter

"Tenable Port" ~ 0 AND "Tenable Protocol" ~

VULN-2
214.15.174.181 - 214-15-...

VULN-18
214.15.174.181 - 214-15-...

VULN-8
214.15.174.181 - 214-15-...

VULN-14
214.15.174.181 - 214-15-...

VULN-4
214.15.174.181 - 214-15-...

VULN-6
214.15.174.181 - 214-15-...

VULN-10

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

Reset the Tenable Plugin for JIRA if you want to change the plugin configuration anytime 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.

To reset the plugin:

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.

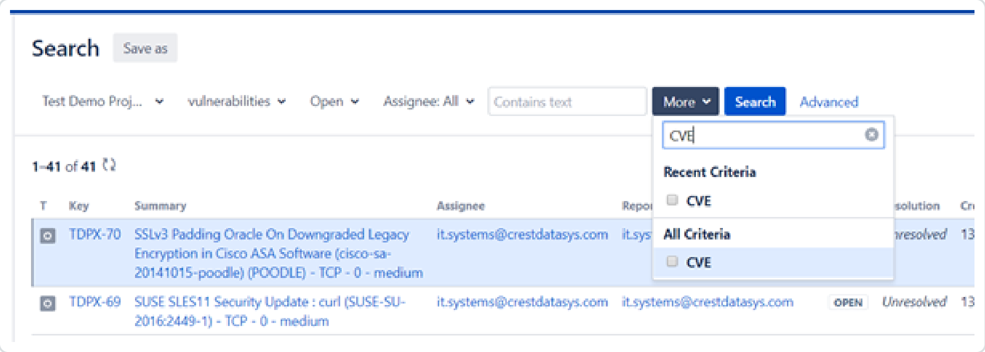
Basic Search

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.

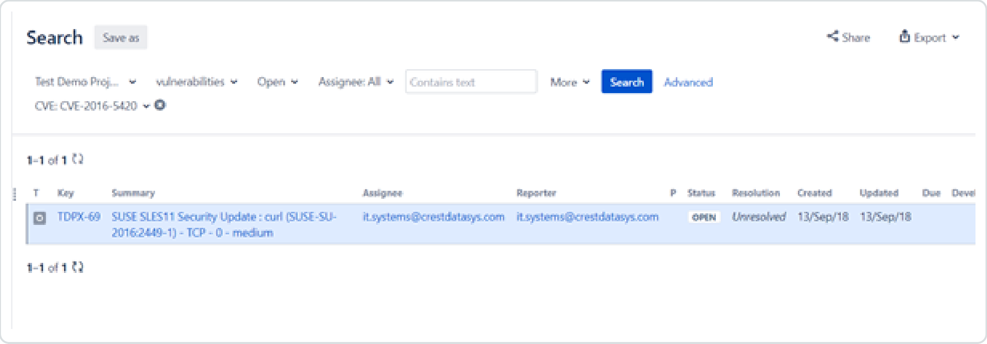
   

T	Key	Summary	Assignee	Repo		solution	Cr
	TDPX-70	SSLv3 Padding Oracle On Downgraded Legacy Encryption in Cisco ASA Software (cisco-sa-20141015-poodle) (POODLE) - TCP - 0 - medium	it.systems@crestdatasys.com	it.sys		nresolved	13
	TDPX-69	SUSE SLES11 Security Update : curl (SUSE-SU-2016:2449-1) - TCP - 0 - medium	it.systems@crestdatasys.com	it.systems@crestdatasys.com	OPEN	Unresolved	13

4. In the drop-down text box, enter the custom type (for example, CVE, BDE, etc.).

   Results appear.

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).



1–1 of 1

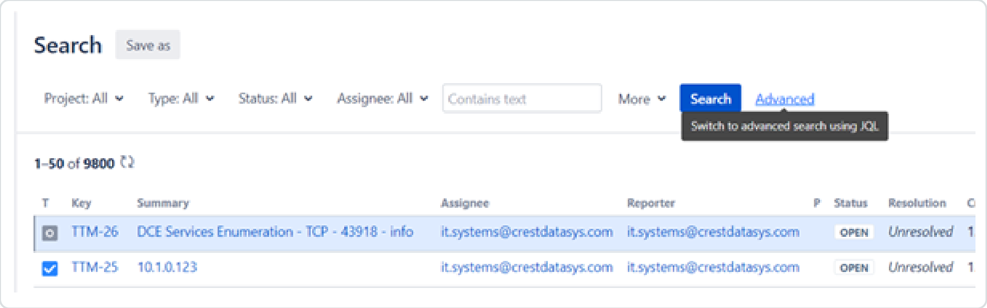
T	Key	Summary	Assignee	Reporter	P	Status	Resolution	Created	Updated	Due	Devel
	TDPX-69	SUSE SLES11 Security Update : curl (SUSE-SU-2016:2449-1) - TCP - 0 - medium	it.systems@crestdatasys.com	it.systems@crestdatasys.com		OPEN	Unresolved	13/Sep/18	13/Sep/18		

1–1 of 1

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**.

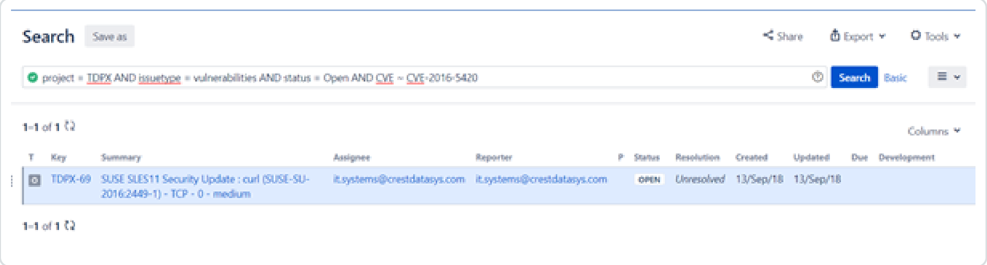
   A text box appears.



1–50 of 9800

T	Key	Summary	Assignee	Reporter	P	Status	Resolution	C
	TTM-26	DCE Services Enumeration - TCP - 43918 - info	it.systems@crestdatasys.com	it.systems@crestdatasys.com		OPEN	Unresolved	1
☑	TTM-25	10.1.0.123	it.systems@crestdatasys.com	it.systems@crestdatasys.com		OPEN	Unresolved	1

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



project = TDPX AND issuetype = vulnerabilities AND status = Open AND CVE ~ CVE-2016-5420

1–1 of 1

T	Key	Summary	Assignee	Reporter	P	Status	Resolution	Created	Updated	Due	Development
	TDPX-69	SUSE SLES11 Security Update : curl (SUSE-SU-2016:2449-1) - TCP - 0 - medium	it.systems@crestdatasys.com	it.systems@crestdatasys.com		OPEN	Unresolved	13/Sep/18	13/Sep/18		

1–1 of 1

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 Vulnerability Management, re-enter your API keys.
    - For Tenable Security Center, re-enter your API keys.
3. Click **Save**.

    After the upgrade, and re-entering your credentials, the data collection automatically starts from the last sync.
4. (Optional) If you want all VPR scores filled out you must click **Reset Add-On**.

Note: If you are a Tenable Security Center user you must use API keys for authentication.

Note: If you upgrade and don't set a default assignee, the integration continues to work as before.

Disable the Tenable Plugin for JIRA

Before you begin:

- You must have administrative access privileges.

To disable 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.

6. **Can I make certain fields required for the tickets the integration creates?**

   No. The Tenable Plugin for JIRA does not fill out every field every time. You must configure tickets the Tenable Plugin for JIRA interacts with to have **no required fields**.

API Usage

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

Note: You can view and try out all of the supported Tenable API endpoints in the Tenable Developer Portal.

Tenable Vulnerability Management

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 Security Center

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

- https://docs.tenable.com/security-center/api/Analysis.html