



Mobilization Quick Reference Guide

Last Revised: December 05, 2025



Table of Contents

| | |
|--|-----------|
| Welcome to the Mobilization Quick Reference Guide | 3 |
| What is Mobilization? | 3 |
| Benefits of Utilizing the Mobilization Workflow | 3 |
| Get Started with Mobilization | 4 |
| Prerequisites | 4 |
| Jira | 4 |
| Automatic Initiatives in Tenable Vulnerability Management | 7 |
| Before you Begin | 8 |
| Jira Initiatives in Tenable Vulnerability Management | 8 |
| Configure Jira | 8 |
| Create a Jira Initiative | 12 |
| What to do Next | 17 |
| View your Initiative Data and Updates | 17 |
| Manage your Initiatives | 18 |
| Ticket Creation in Tenable Exposure Management | 18 |
| Before you Begin | 18 |
| Create a Ticket in Tenable Exposure Management | 19 |
| Jira | 19 |
| What to do Next | 22 |
| Troubleshooting and Frequently Asked Questions | 23 |
| Additional Resources | 24 |
| Tenable User Documentation | 24 |
| Jira Documentation | 24 |



Welcome to the Mobilization Quick Reference Guide

Last updated: December 05, 2025

This guide exists to provide complete instructions on using the mobilization capabilities within Tenable software.

What is Mobilization?

Mobilization is the critical action stage of the exposure management lifecycle. It operationalizes prioritized Continuous Threat Exposure Management (CTEM) findings, transforming your program from a passive system of record into an active system where security intelligence translates directly into measurable business impact. This requires unifying security and remediation teams, establishing clear cross-functional workflows, and securing leadership buy-in to decisively reduce business risk across the modern attack surface.

You can use the mobilization workflow within Tenable Vulnerability Management to create initiatives and link them to tracked action items in your preferred ticketing systems without manual synchronization or complex Security, Orchestration, Automation, and Response (SOAR) solutions. Your vulnerability and exposure status updates automatically between the Tenable platform and your existing workflows, which provides you with a real-time view of your remediation progress.

Tip: For more information about mobilization, see the [Mobilization Quick-Reference Guide](#).

Benefits of Utilizing the Mobilization Workflow

Orchestrate Remediation

Mobilization drives action between your security and remediation teams by creating a direct link between security findings and remediation workflows. This improves collaboration and accelerates response times.

Achieve a Single Source of Truth

End the need for manual data reconciliation. By linking directly to ticketing systems, you ensure your vulnerability status updates in real time as soon as the corresponding ticket is updated.

Unify Your Remediation Workflow



Remove security tool silos and operational complexity with exposure management. Mobilization allows you to identify and resolve critical risks from a single platform across multiple domains and security tools.

Get Started with Mobilization

At this time, you can utilize mobilization capabilities in both Tenable Vulnerability Management or create tickets based on findings directly within Tenable Exposure Management. For more information, see the following topics:

- [Prerequisites](#)
- [Automatic Initiatives in Tenable Vulnerability Management](#)
- [Ticket Creation in Tenable Exposure Management](#)

For further information and troubleshooting, see:

- [Troubleshooting and Frequently Asked Questions](#)
- [Additional Resources](#)

Prerequisites

Before you begin, ensure you have completed the following prerequisites.

Jira

Before you create tickets within Jira via Tenable products, you must have the following:



- A Jira user with the following permissions:

| Jira Permission | Purpose in Exposure Response | Custom Context | Atlassian Documentation |
|-------------------|------------------------------|---|---|
| "ASSIGNABLE_USER" | User Validation | Ensures the dedicated integration user is a valid assignee within the project, which is often a prerequisite for using "ASSIGN_ISSUES". | Assignable User Permissions |
| "ASSIGN_ISSUES" | Work Assignment | Allows the integration to assign the newly created ticket to the designated user or group specified in the Initiative configuration. | Assign Issues Permissions |
| "BROWSE_PROJECTS" | Visibility | Allows the integration to read and confirm the existence of the configured Jira project and its Issue Types. | Browse Projects Permissions |
| "CREATE_ISSUES" | Ticket Creation | Required to | Create Issues |



| Jira Permission | Purpose in Exposure Response | Custom Context | Atlassian Documentation |
|-----------------|------------------------------|--|---|
| | | automatically generate new tickets for findings that match the Initiative's criteria (the "combination"). | Permissions |
| "EDIT_ISSUES" | Status Synchronization | Enables Tenable to update key fields, push risk data (like VPR), and change the ticket status (e.g., from Resolved to Resurfaced). | Edit Issues Permissions |
| "LINK_ISSUES" | Audit Trail | Creates the essential link between the Tenable finding and the corresponding Jira ticket, enabling the Ticket Log functionality. | Link Issues Permissions |

- A Jira project with the following fields enabled for issues:

Important: You must have at least one Jira project for the configuration to function as expected.



- "priority",
- "assignee",
- "labels",
- "summary",
- "description",
- "issuetype",
- "parent",
- "project",
- "reporter" — To use this field, the user must also have the "MODIFY REPORTER" permission enabled.

Tip: In Jira, navigate to **Settings > System > Admin Helper > Permission Helper** to confirm or provision the permission for the user.

For more information about Jira configuration, see the [Tenable for Jira Cloud Integration Guide](#).

Automatic Initiatives in Tenable Vulnerability Management

In the [Exposure Response](#) section of Tenable Vulnerability Management, you can create *initiatives* based off of findings that you can then link directly to your ticketing systems. Tenable calls this process *mobilization*. Initiatives are projects to address vulnerabilities in your environment. You can track specific findings using combinations and apply asset tags to choose the assets in scope. You can then assign initiatives to your team, set SLAs (Service Level Agreements), and measure progress through remediation scan results.

Because these initiatives automatically update when a change is made to the tracked ticket, they are considered *automatic initiatives*.

Example Initiative

To address recently exploited vulnerabilities on your Headquarters network, you might create an initiative as follows:



- **Name** – Recently exploited vulnerabilities at HQ
- **Asset Scope** – Network: HQ
- **Owner** – user@myorganization.com
- **Remediate Within (SLA)** – 7 days
- **Combinations** – Category is equal to Recently Actively Exploited AND VPR is greater than 6

* Query

Saved Filters ▾ Category is equal to Recently Actively Exploited x AND VPR is greater than 6 x

Before you Begin

- Review the [Prerequisites](#) and ensure you have the appropriate permissions and ticketing configurations enabled for initiative creation.
- Create asset tags – Initiatives use [asset tags](#) to define the assets in scope. Create any asset tags you plan to use for your initiative.
- (Optional) Create custom combinations – If you plan to use custom combinations, [create them](#) via the **Manage Combinations** tab.

You can create the following kinds of initiatives within Tenable Vulnerability Management:

Jira Initiatives in Tenable Vulnerability Management

Configure Jira

Before you create an initiative, you must first configure a connection between Jira and Tenable Vulnerability Management.

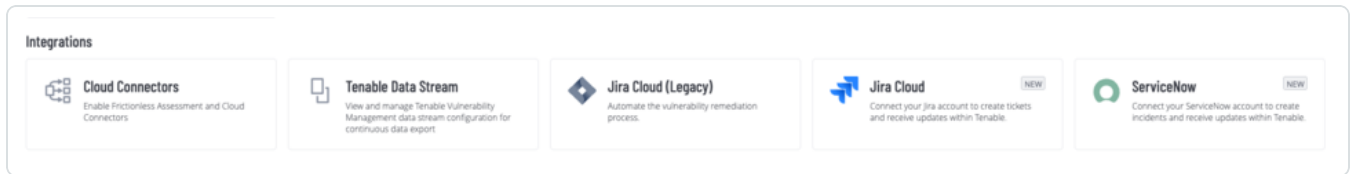
To configure Jira issue creation in Tenable Vulnerability Management:

1. In the left navigation, click  **Settings**.

The **Settings** page appears.



- Click on the  **Jira Cloud** tile.



The Jira Connector page appears.

- Configure the following Jira Cloud Credentials:

Jira Cloud

INTEGRATION NAME

REQUIRED

JIRA CLOUD URL

REQUIRED

JIRA CLOUD USER ACCOUNT

REQUIRED

JIRA CLOUD API TOKEN

REQUIRED

| Option | Description |
|--------------------------------|--|
| Integration Name | Choose your own Jira integration name. |
| Jira Cloud URL | The unique web address for your organization's instance of Jira Cloud, typically formatted as https://[your-company-name].atlassian.net . |
| Jira Cloud User Account | Your individual credentials (email and password) used to authenticate and access your organization's Jira Cloud site. |



Jira Cloud API Token

Your API key or token for authenticated access to the Jira Cloud API.

- To test the connection, click **Connect**.

Connect to Jira Cloud

Validate and link the integration connectivity. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Connect

Delete Connection

Once Tenable validates the integration connectivity, a **Connection was Successful** notification appears.

Connect to Jira Cloud

Validate and link the integration connectivity. Note that successful connectivity testing does not indicate successful integration, as the connector sync might encounter syncing or processing issues.

Connect

✓ Connection was successful.

Delete Connection

- Configure the following default values for each Jira project:



Defaults

Use this section to define default settings per project in Jira

PROJECT

ANGKor (ANGK)

REQUIRED



DEFAULT ASSIGNEE

Select Assignee



DEFAULT REPORTER

Select Reporter



DEFAULT LABEL(S)

Select Label(s)



Sync Jira Priorities

This allows you to align finding severities with corresponding Jira priorities

| Finding Severity | Default Jira Priority |
|------------------|-----------------------|
|------------------|-----------------------|

Critical

Select



High

Select



Medium

Select



Low

Select



Info

Select



[+ Add another project](#)



| Option | Description |
|-----------------------------|--|
| Project | The Jira Project name that these options relate to. |
| Default Assignee | Assign a user as a default assignee from the drop-down list. |
| Default Reporter | Assign a default reporter value from the drop-down list. |
| Default Label(s) | Your organization's Cloud URL. |
| Sync Jira Priorities | Create a mapping of Tenablefindings severities (for example, Critical, High, Medium, Low, Info) to Jira Priorities (for example, Highest, High, Lowest). |


6. To set default values for additional Jira projects, click  **Add Another Project**.


Note: To delete project configurations click the  next to the corresponding project.

7. Click **Save**.

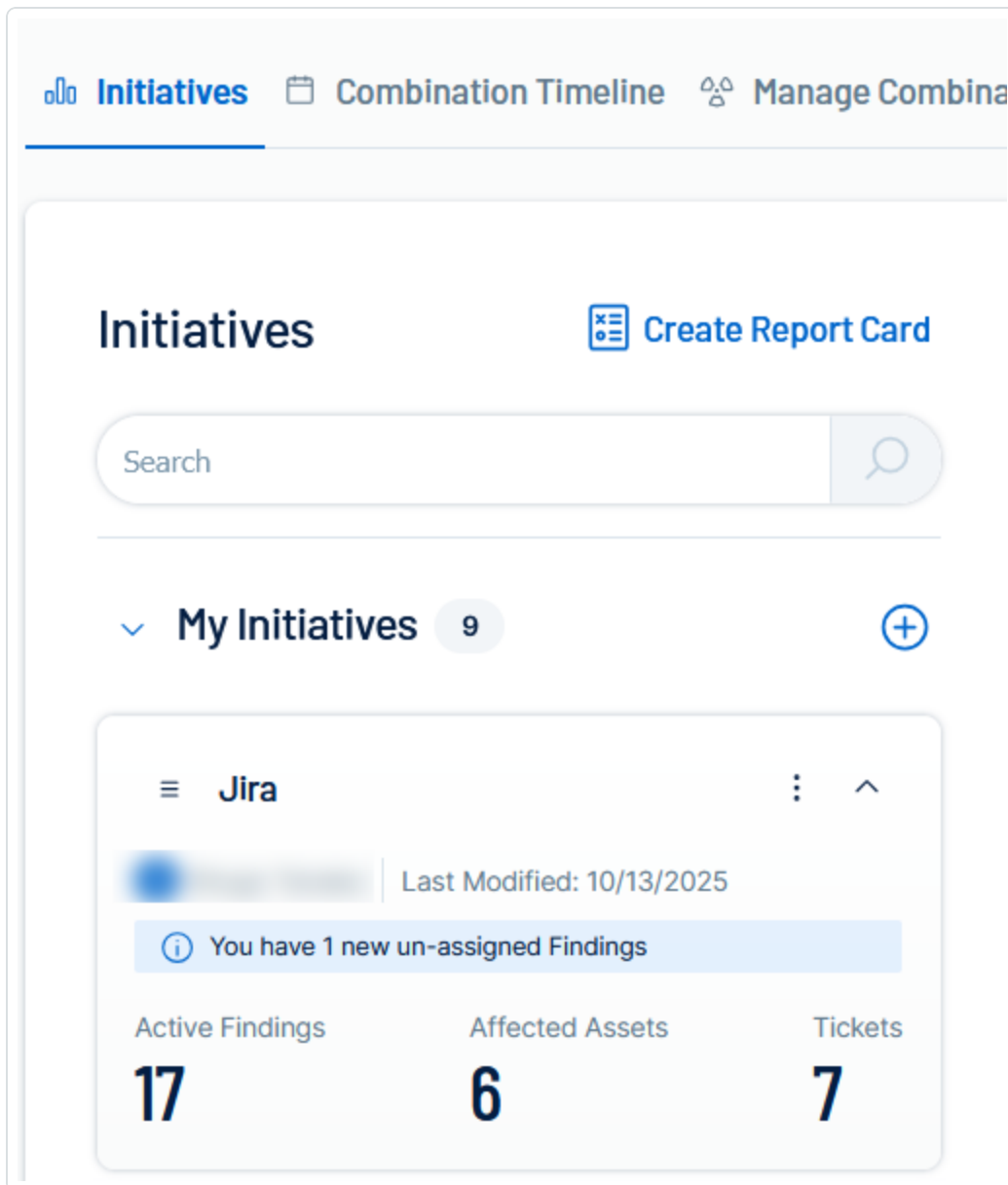
Create a Jira Initiative

To create a Jira mobilization initiative based off of a finding:

1. In Tenable Vulnerability Management, in the left navigation menu, click  **Exposure Response**.

The **Exposure Response** page appears. By default, the  **Initiatives** tab is active.

2. In the **My Initiatives** section, click the  button.



The **Create an Exposure Response Initiative** pane appears.

3. On the **Basic Setup** tab, configure the following options:



Create an Exposure Response Initiative [?](#)



Basic Setup

Configure your initiative, share and assign combinations



Ticketing Automation

Configure automatic ticketing defaults

Basic Setup

General Settings

* Name [?](#)

REQUIRED

Description

* Owner [?](#)



[?](#) Owner cannot be changed once the initiative is saved.

* Asset Scope [?](#)

REQUIRED



* Remediate Within (SLA) [?](#)

REQUIRED

Days

Assign Combinations [?](#)

[?](#) At least one item must be selected.



My Combinations

Shared

Tenable

| Option | Description |
|-------------------------------|--|
| Name (required) | Type a name for the initiative. |
| Description | Type a description for the initiative, for example <i>Reduce my external attack surface</i> . |
| Owner | Select the initiative owner from a list of [MadCap Variable: Tenable.VulnerabilityManagementStandalone] users. You cannot reassign initiatives once you create them. <div>Note: Only administrators and initiative owners can view initiatives.</div> |
| Asset Scope (required) | Choose up to ten tags to define which assets in your environment are in scope. Search for and select tags to assign, for example <i>Priority: High</i> or <i>Software: Oracle</i> . |

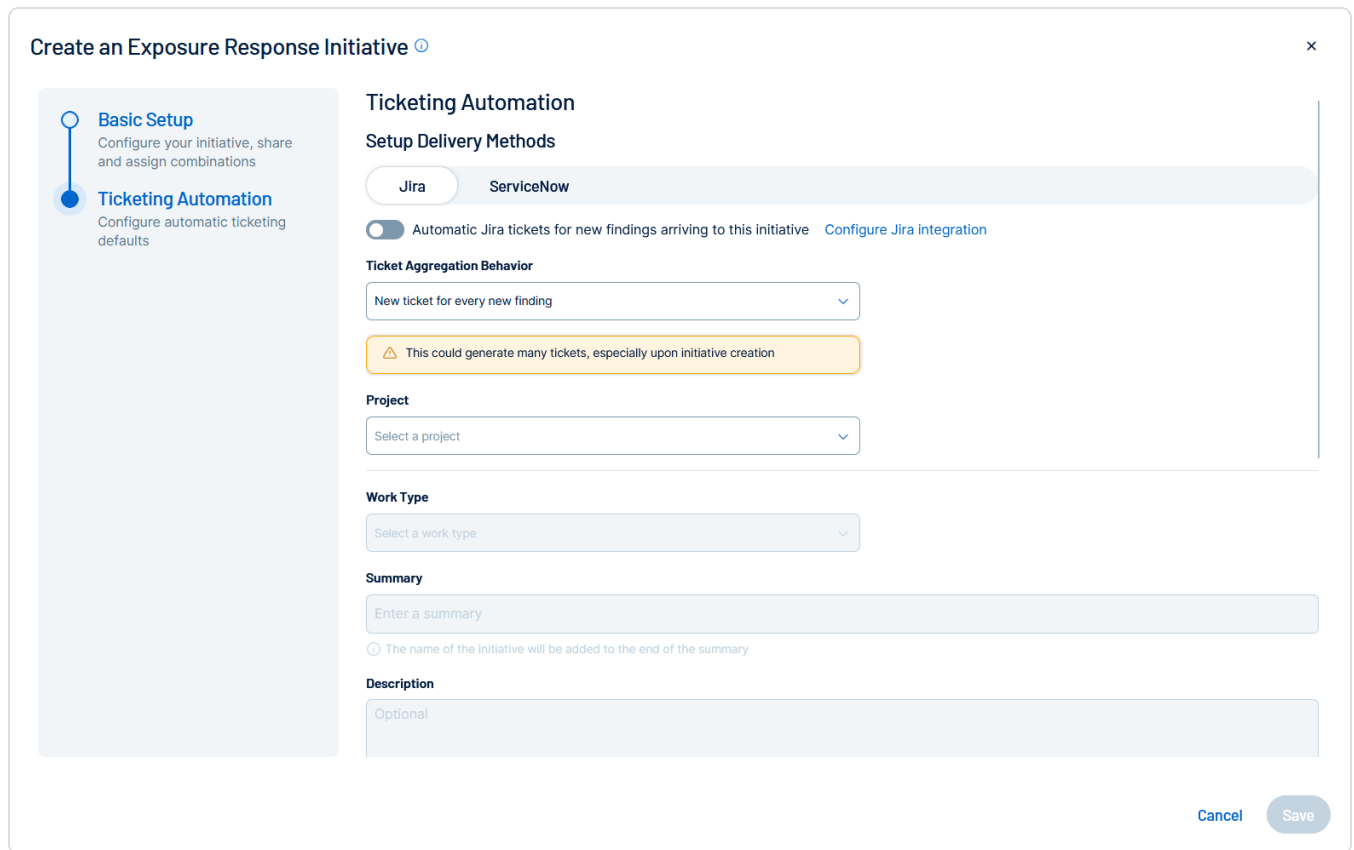


| | |
|---|---|
| Remediate Within (SLA) (required) | Choose an SLA, in days, by which all findings require remediation. For example, to set an SLA of one week, enter 7. |
| Assign Combinations | <p>Select up to ten combinations from the available tabs:</p> <ul style="list-style-type: none">• My Combinations – Your personal combinations, which only you can view. You cannot assign personal combinations to initiatives you do not own.• Shared – Organization-wide combinations, which anyone can view or use, and which your administrators and the combination owners can update. Track updates in the  Combination Timeline.• Tenable – Predefined combinations from the Tenable Research Team. These may be updated infrequently, which can change the resources in your initiatives. Track updates in the  Combination Timeline. |

4. Click the **Ticketing Automation** tab.

The **Setup Delivery Methods** appear.

5. Click **Jira**.



Create an Exposure Response Initiative ⓘ

Basic Setup
Configure your initiative, share and assign combinations

Ticketing Automation
Configure automatic ticketing defaults

Ticketing Automation

Setup Delivery Methods

Jira **ServiceNow**

☐ Automatic Jira tickets for new findings arriving to this initiative [Configure Jira integration](#)

Ticket Aggregation Behavior

New ticket for every new finding

⚠ This could generate many tickets, especially upon initiative creation

Project

Select a project

Work Type

Select a work type

Summary

Enter a summary

ⓘ The name of the initiative will be added to the end of the summary

Description

Optional

Cancel Save

Jira ticketing configuration options appear.

6. Configure the following options:

| Option | Description |
|------------------------------------|--|
| Ticket Aggregation Behavior | Select how you want Tenable Vulnerability Management to aggregate tickets for the finding: <ul style="list-style-type: none">• New ticket for every new finding – Every time a finding appears, a new ticket gets created in Jira.• New findings create subtasks on an existing ticket – Every time a finding appears, a subtask gets created on an existing Jira ticket. |
| Existing Jira | Select the existing Jira ticket from the drop-down list. |



| | |
|--------------------------|---|
| Ticket (optional) | Note: You see this option only if you choose New findings create subtasks on an existing ticket . |
| Project | The Jira project in which you want tickets to be created. Important: You must have at least one Jira project for the configuration to function as expected. |
| Work Type | The specific type of issue created, for example, Story , Task , or Bug . |
| Summary | The Jira Summary combines the finding name, asset name, and this text to create a descriptive ticket title. |
| Description | A detailed explanation of the issue, context, and steps to reproduce (if applicable). |
| Priority | The relative importance or severity of the issue. Default value: Default Mapping . Note: Leave this set to Default Mapping to allow the priority to be set by the finding severity based on your Jira instance configuration. For more information about overriding this severity, see Configure Jira . |
| Reporter | The user who created the issue and submitted it to the project. |
| Assignee | The user to which the ticket or subtask is assigned in Jira. |
| Parent | The larger issue (for example, an <i>Epic</i>) under which the current item is nested. |
| Labels | Custom tags you want to apply to the ticket for flexible categorization and filtering. |

7. Click **Save**.

The initiative appears in the **My Initiatives** panel.

What to do Next

View your Initiative Data and Updates



Within Tenable Vulnerability Management, you can view data about your existing mobilization initiatives and their updates in the following locations:

- [My Initiatives](#) list
- [Initiative Overview](#)
- [How Am I Doing?](#)
- [What's New?](#)
- [Activity](#)
- [Combination Timeline](#)

Manage your Initiatives

Once configured, you can view and manage your Tenable Vulnerability Management mobilization initiatives in the following ways:

- [Edit an Initiative](#)
- [Export Initiative Data](#)
- [Manage Affected Asset Tags](#)
- [Edit Initiative Tickets in the Ticket Log](#)
- [Delete an Initiative](#)

Ticket Creation in Tenable Exposure Management

Within Tenable Exposure Management, you can create tickets based on findings directly from the **Findings** page. These tickets help you to address vulnerabilities in your environment and ensure work items for vulnerability findings are being created and assigned quickly and effectively.

Before you Begin

Review the [Prerequisites](#) and ensure you have the appropriate permissions and configurations enabled for ticket creation.



Create a Ticket in Tenable Exposure Management

You can create the following kinds of tickets within Tenable Exposure Management:

Jira

To create a Jira ticket based off of a finding:

1. In Tenable Exposure Management, access the [Findings](#) view.
2. In the findings list, select the check box next to each finding you want to include in the ticket.
3. In the upper-right corner of the page, click [Take Action](#).

A drop-down menu appears.

4. Click **Create Jira Ticket**.

The **Open Jira Ticket** page appears.

← Back to Inventory

Open a Jira Ticket

Aggregation Behavior*

Create a new jira ticket for each finding

Project*

ANGKor

Work Type*

Tenable Vulnerability

Assignee

Select...

Attachment

Select...

Team

Tenable Severity

2 Included Findings

| Finding Name | Asset Name | Severity | State |
|-----------------------------|--------------|----------|--------|
| Allows insecure protocol... | 23.4.143.133 | Critical | ACTIVE |
| Allows insecure protocol... | 23.4.137.236 | Critical | ACTIVE |

Cancel **Create Ticket**

5. From the **Aggregation Behavior** drop-down box, select how you want Template to aggregate tickets for the finding:



- **Create a new jira ticket for each finding** – Every time a finding appears, a new ticket gets created in Jira.


The configuration options on the page update based on your selection.

- a. From the **Project** drop-down box, select the Jira project in which you want tickets to be created.
- b. From the **Work Type** drop-down box, select the type of ticket you want to create in Jira, for example, **Task** or **Epic**.

The remaining configuration options update based on your selection.

- c. Configure the ticket creation options. Depending on the **Work Type**, these can include, but are not limited to:

Tip: For more information about Jira ticket creation fields and options, see [Configuring Built-In Fields](#) in the *Administering Jira Applications Support Guide*.

| Option | Description |
|---------------------------------|--|
| Project drop-down box | Select the Jira project in which you want tickets to be created. |
| Work Type drop-down box | Select the type of ticket you want to create in Jira, for example, Task or Epic . |
| Assignee drop-down box | Select the user to which you want to assign the ticket. |
| Attachment drop-down box | Where applicable, select any attachments you want to include in the ticket. |
| Team text box | Type the team name to which you want to assign the ticket. |
| Due Date text box | Type the date at which the work for the ticket is due. Optionally, click the  button and select a date from the |



| | |
|-------------------------------|--|
| | calendar. |
| Labels text box | Type any labels you want to assign to the ticket. |
| Priority drop-down box | Select the priority you want to assign to the ticket, for example, Low or High . |
| Reporter drop-down box | Select the user you want to assign as the reporter of the ticket. |

- **New findings create subtasks on an existing ticket** – Every time a finding appears, a subtask gets created on an existing Jira ticket.


The configuration options on the page update based on your selection.

- a. Configure the following options:

Tip: For more information about Jira ticket creation fields and options, see [Configuring Built-In Fields](#) in the *Administering Jira Applications Support Guide*.

| Option | Description |
|---|--|
| Project drop-down box | Select the Jira project in which you want subtasks to be created. |
| Existing Jira Ticket drop-down box | Select the existing Jira ticket on which you want subtasks to be created. |
| Assignee drop-down box | Select the user to which you want to assign the subtask. |
| Attachment drop-down box | Where applicable, select any attachments you want to include in the subtask. |
| Team text box | Type the team name to which you want to assign the subtask. |
| Due Date text | Type the date at which the work for the subtask is due. |



| | |
|-------------------------------|---|
| box | Optionally, click the  button and select a date from the calendar. |
| Labels text box | Type any labels you want to assign to the subtask. |
| Priority drop-down box | Select the priority you want to assign to the subtask, for example, Low or High . |
| Reporter drop-down box | Select the user you want to assign as the reporter of the subtask. |

6. Click **Create Ticket**.

Template creates the ticket within Jira based on the selected finding data.

What to do Next

View your newly created tickets within the selected Jira project. The tickets include information about the findings selected upon ticket creation within Tenable Exposure Management.



Troubleshooting and Frequently Asked Questions

The following are some common errors and questions users may encounter when configuring and managing mobilization initiatives.

How long does it take to see initiative/ticket data?

For initiatives created within Tenable Vulnerability Management:

- Newly created initiatives and their data appear in the user interface within minutes.
- Existing initiatives automatically update once every 24 hours, or when there is a change to the initiative scope that triggers on-demand metric recalculation.

Tip: In Tenable Vulnerability Management, you can view the time at which an initiative's metrics were last calculated in the **Initiative Overview** section.

For tickets created within Tenable Exposure Management:

- It can take up to 10 minutes to see the newly created and updated ticket information in both Tenable Exposure Management and the ticketing system.



Additional Resources

Check out the following additional resources for more information on mobilization and initiatives.

Tenable User Documentation

- [*Tenable Vulnerability Management User Guide*](#)
- [*Tenable Exposure Management User Guide*](#)
- [*Tenable for Jira Cloud Integration Guide*](#)

Jira Documentation

- [Getting Started with Jira](#)
- [Jira Users and Permissions](#)
- [Jira Projects Overview](#)