ThreatQuotient

Jira ITSM Action

Version 1.0.0

January 28, 2025

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.0
Compatible with ThreatQ Versions	>= 5.12.1
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Jira ITSM Action integration allows ThreatQ to automatically export incident, event, or report objects to Jira as tickets (issues), based on a data collection. This enables you to forward security tool alerts or analyst-created alerts to Jira for further tracking, investigation, and remediation.

The integration provides the following action:

- **Jira ITSM - Create Tickets** - exports objects from ThreatQ as tickets/issues in Jira ITSM.

The action is compatible with the following system object types:

- Events
- Incidents
- Reports

Jira Service Management is software designed to streamline IT service management (ITSM). It allows teams to collaborate on requests, centralize knowledge, and deliver services efficiently. Traditionally, Jira is used to manage tickets, incidents, and other requests. However, due to Jira's customizability, it can be used to handle incident response and threat intelligence workflows as well.

This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- A Jira instance, user account, and API Key.
- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one of the following object types:
  - Events
  - Incidents
  - Reports

Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
   - Drag and drop the zip file into the dialog box
   - Select **Click to Browse** to locate the zip file on your local machine

   > ThreatQ will inform you if the action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

You will still need to configure the action.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

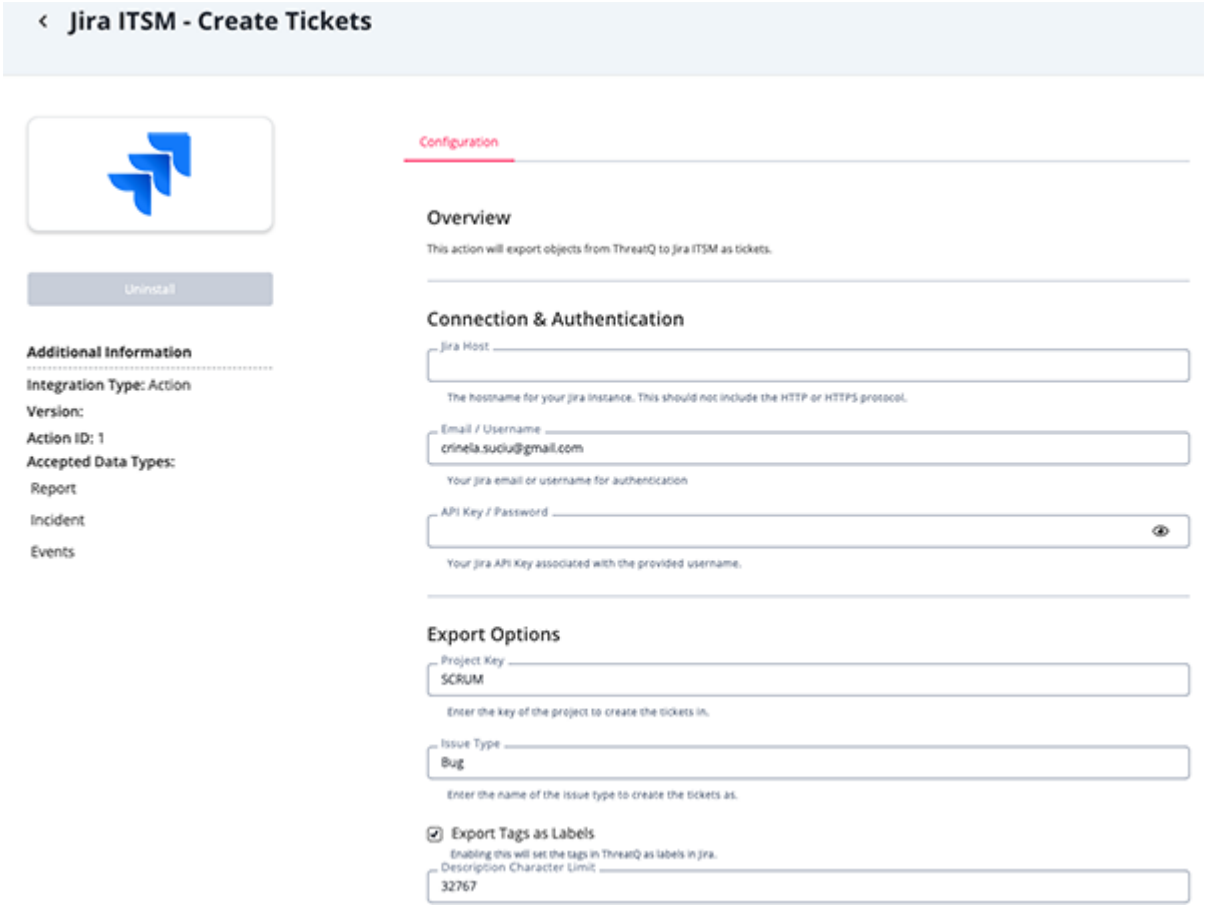
To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
Jira Host	Enter the hostname for your Jira Instance. This should not include the HTTP or HTTPS protocol. The default value is `<tenant>.atlassian.net`.
Email / Username	Enter your Jira email or username used for authentication.
API Key / Password	Enter your API Key associated with the email/username provided above.
Project Key	Enter the key of the project to create the tickets in.
Issue Type	Enter the name of the issue type to create the tickets as.
Export Tags as Labels	Enable this parameter to set the tags in ThreatQ as labels in Jira. This parameter is enabled by default.
Description Character Limit	Enter the maximum number of characters to include in the description field. The Jira Cloud character limit default is 32,767

PARAMETER	DESCRIPTION
	characters, which is also the default value for this parameter. If the description is longer than the set limit, the description will be truncated and a "Read More in ThreatQ" message will be appended to the end. As of this publication, the Jira Cloud default cannot be modified.
Apply Jira Key to Exported Objects	Select how you want the Jira Key to be applied to the ThreatQ object once it's been uploaded to Jira. Options include: ◦ As a Value Prefix (default) ◦ As an Attribute ◦ As a Tag ◦ Do not Apply
Apply Jira Link to Exported Objects	Enable this parameter to add an attribute containing a link to the Jira ticket to the exported objects. This parameter is disabled by default.



5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Jira ITSM - Create Tickets	Creates tickets in Jira from objects in ThreatQ.	Events, Incidents, Reports	N/A

Jira ITSM - Create Tickets

The Jira ITSM - Create Tickets action takes incidents, events, or reports from a data collection and exports them to Jira as tickets/issues. When a ticket/issue is successfully created, the Jira Key will be added back into ThreatQ as either an attribute, tag, or part of the object's value (based on the user-configuration).

The object's value, description, and tags will be transferred to Jira. Currently, this action will not transfer other metadata such as relationships, attributes, or comments.

`POST https://{{ host }}/rest/api/3/issue`

Sample Response:

```
{
  "id": "10209",
  "key": "IR-206",
  "self": "https://<tenant>.atlassian.net/rest/api/3/issue/10209"
}
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.key`	Object Tag, Object Attribute	`Jira Key`	N/A	`IR-206`	Added based on user-field selection
`.self`	Object Attribute	`Jira Link`	N/A	`https://<tenant>.atlassian.net/rest/api/3/issue/10209`	Added based on user-field selection

Enriched Data

Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

METRIC	RESULT
Run Time	1 minute
Reports	2
Report Attributes	4

Use Case Example

1. I have analysts in ThreatQ that are creating incidents and reports based on alerts from our security tools. I want to export these incidents and reports to Jira as tickets so that our IT team can track and remediate them.
2. I am using ThreatQ to aggregate my alerts from my different tools. I can use this action to export these alerts to Jira as tickets so that my IT team can track and remediate them.

Known Issues / Limitations

- The action will not transfer other metadata such as relationships, attributes, or comments.
- Due to Jira's Description field character limit, the description will be truncated if it exceeds the limit. A "Read More in ThreatQ" message will be appended to the end.
- Due to Jira's Description format (Atlassian Document Format; ADF), the description cannot be sent to Jira as raw HTML and instead needs to be converted to the ADF format. During this process, the description may lose some formatting/styling.

Change Log

- **Version 1.0.0**
  - Initial release