ThreatQuotient

ThreatQuotient for JIRA Application

Version 1.4.0

April 29, 2019

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: + 1 703.574.9893

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.

Last Updated: Wednesday, April 29, 2019

Contents

List of Figures and Tables

1 Introduction

1.1 Application Function

The ThreatQuotient for JIRA Application is a bidirectional connector that will sync tickets between a ThreatQ instance and a JIRA instance.

1.2 Preface

This guide provides the information necessary to implement the ThreatQuotient for JIRA Application. This document is not specifically intended as a site reference guide. It is assumed that the implementation engineer has experience installing and commissioning the ThreatQuotient Apps and integrations covered within the document, as well as the experience necessary to troubleshoot at a basic level.

1.3 Audience

This document is intended for use by the following parties:

1. ThreatQ and Security Engineers
2. ThreatQuotient Professional Services Project Team and Engineers

1.4 Scope

This document covers the implementation of the ThreatQuotient for JIRA Application only.

Table 1: ThreatQuotient Software & App Version Information

Software/App Name	File Name	Version
ThreatQ	Version 3.6.x or greater	
ThreatQuotient for JIRA Application	1.4.0	

1.5 Assumptions

The following criteria is assumed to be in place and functional to allow the implementation of the ThreatQuotient for JIRA Application into the managed estate:

- All ThreatQuotient equipment is online and in service.
- All required firewall ports have been opened.

2 Implementation Overview

This document will show how to install the ThreatQuotient for JIRA Application.

2.1 Prerequisites

Throughout this implementation document, we will refer to several files and directories, some of which will be symbolic, and others may change depending on specifics of the environmental setup.

Ensure all ThreatQ devices are set to the correct time, time zone and date, and using a clock source available to all.

To identify which time zone is closest to your present location, use the `timedatectl` command with the `list-timezones` command line option. For example, to list all available time zones in Europe, type:

Figure 1: Time Zone List Example

```
timedatectl list-timezones | grep Europe
Europe/Amsterdam
Europe/Athens
Europe/Belgrade
Europe/Berlin
```

To change the time zone to UTC, type as root:

Figure 2: Time Zone Change Example

```
timedatectl set-timezone UTC
```

2.2 Security and Privacy

For ThreatQuotient Professional Services engineers to configure the system, local network access is required to connect to the managed estate. Therefore, the implementation must occur at an office or data center location.

Passwords have not been provided in this document. Please contact your project team for this information, if required.

All engineers are reminded that all data belonging and pertaining to the business is confidential and should not be disclosed to any unauthorized parties.

The data held within this document is classed as confidential due to its nature.

3 JIRA Application Installation

3.1 Setting up the Integration

From the ThreatQuotient Repository

To install this ThreatQuotient for JIRA Application from the ThreatQuotient repository with YUM credentials.

1. Install the JIRA integration by using the following commands.

Figure 3: Installing From The ThreatQuotient Repository (Example Output)

```
[root@DC01-ThreatQ ~]# pip install tq-conn-jira
Collecting tq-conn-jira
  Downloading https://system-updates.threatq.com/pypi/+f/9ad/eead4d5f5a6af/jira-
2.0.0-py2.py3-none-any.whl (57kB)
    100% |████████████████████████████████| 61kB 173kB/s
Requirement already satisfied (use --upgrade to upgrade): requests>=2.10.0 in
/usr/lib/python2.7/site-packages (from Jira)
Collecting pbr>=3.0.0 (from Jira)
  Downloading https://system-updates.threatq.com/pypi/+f/825/7baf496c85224/pbr-
5.1.3-py2.py3-none-any.whl (107kB)
    100% |████████████████████████████████| 112kB 291kB/s
Requirement already satisfied (use --upgrade to upgrade): setuptools>=20.10.1 in
/usr/lib/python2.7/site-packages (from Jira)
Requirement already satisfied (use --upgrade to upgrade):
oauthlib[signedtoken]>=1.0.0 in /usr/lib/python2.7/site-packages (from Jira)
Collecting requests-toolbelt (from Jira)
  Downloading https://system-
updates.threatq.com/pypi/+f/380/606e1d10dc85c/requests_toolbelt-0.9.1-py2.py3-none-
any.whl (54kB)
    100% |████████████████████████████████| 61kB 174kB/s
Requirement already satisfied (use --upgrade to upgrade): six>=1.10.0 in
/usr/lib/python2.7/site-packages (from Jira)
Installing collected packages: pbr, requests-toolbelt, Jira, pyjwt
Successfully installed tq-conn-jira-1.4.0 pbr-5.1.3 pyjwt-1.7.1 requests-toolbelt-
0.9.1
```

Offline from the .whl File

To install this ThreatQuotient for JIRA Application from a wheel file, the wheel file (.whl) file `tq-conn-jira-1.4.0-py2-none-any.whl` will need to be copied via SCP into your ThreatQ instance.

1. Install the .whl file using the following command.

Figure 4: Installing .whl File (Inc Example Output)

```
$> sudo pip install /file/path/to/app/tq-conn-jira-1.4.0-py2-none-any.whl
Successfully installed tq-conn-jira-1.4.0
```

Once the application has been installed, create a directory structure for all configuration, logs and files, using the `mkdir -p` command. See example below:

Figure 5: Creating Integration Directories (Example)

```
mkdir -p /etc/tq_labs/
mkdir -p /var/log/tq_labs/
```

A driver called `tq-conn-jira` is installed.

2. Issue the following commands to initialize the integration.

   You will be asked the following questions:

   a. **ThreatQ Host:** This is the host of the ThreatQ instance, either the IP Address or Hostname as resolvable by ThreatQ.
   b. **Client ID:** This is the OAuth id that can be found at the **Settings icon** > **OAuth Management**.
   c. **E-mail Address:** This is the *User in the ThreatQ System* for integrations.
   d. **Password:** The password for the above ThreatQ account
   e. **Status:** This is the default status for IoCs that are created by this integration. It is common to set this to "Review", but Organization SOPs should be respected when setting this.

   Figure 6: Running the Integration

   ```
   $>tq-conn-jira -c /file/path/to/config/ -ll /file/path/to/logs/ -v3
   ThreatQ Host: <ThreatQ Host IP or Hostnme >
   Client ID: <ClientID>
   E-Mail Address: <EMAIL ADDRESS>
   Password: <PASSWORD>
   Status: Active
   Connector configured.  Set information in UI
   ```

   The driver will run once, where it will connect to the ThreatQ instance and install the user interface component of the connector.

3.2 Configuring the Connector

To configure the application, navigate to the ThreatQ user interface via the **Settings icon** > **Incoming Feeds** > **ThreatQ Labs** and find the **Jira Integration**. Input the required information:

1. **JIRA Host**: This is the FQDN of your JIRA instance. It MUST include either **http://** or **https://**.
2. **Username**: This is the JIRA username to be used for the integration.
3. **Password**: This is the JIRA password associated with the username above.
4. **JIRA Project**: This is the key of the project you want the integration to sync with. Ensure the key is entered and **not** the name. NOTE: The key will be formatted in all caps.
5. **ThreatQ Event Types**: This is the event types you want to sync with JIRA. The following options are available:
   - '**All**', which will sync all ThreatQ event types.
   - '**None**', which will make it so that ThreatQ events will not be added to JIRA.
   - Individual or list of event types to sync.
6. **JIRA Event Issue Type**: This is the name of the issue type you require the ThreatQ events to be synced with. This field does not apply if you install the ThreatQ Project configuration (this field should be left default).
7. **JIRA Indicator Issue Type**: This is the name of the issue type you want the ThreatQ indicators to be synced with. This field does not apply if you install the ThreatQ Project configuration (leave this field as is).
8. **Historical Timeframe (days)**: This is the number of days to pull historical data from (for the first run). This option only applies to the first time you run the integration. For ThreatQ events, it compares against the **'Happened At'** date. For JIRA issues, it will compare against the '**Updated**' date.

Figure 7: ThreatQ UI Configuration

Once completed, the integration is ready for operation.

To run the integration for sync, simply use the same command used in *Figure 6: Running the* Integration.

3.3 CRON

To run this script on a reoccurring basis, use CRON or some other system schedule. The argument in the cron script ***must*** specify the config and log locations.

This can be run multiple times a day and should not be run more often than once per hour.

3.3.1 Setting Up the CRONJOB

1. Login via a CLI terminal session to you ThreatQ host.
2. Input the commands below.

Figure 8: Command Line Crontab Command

```
$> crontab -e
```

This will enable the editing of the crontab, using vi.

 Depending on how often you wish the cronjob to run, you will need to adjust the time to suit the environment.

3. Input the commands below – this example shows every **4 Hours.**

Figure 9: Command Line Crontab tq-conn-jira Command

```
0 */4 * * * tq-conn-jira -c /path/to/config/directory/ -ll
/path/to/log/directory/ -v3
```

Figure 10: Command Line Crontab tq-conn-jira Command (Bespoke Name)

```
0 */4 * * * tq-conn-jira -n <Bespoke_Name> -c /path/to/config/directory/ -
ll /path/to/log/directory -v3
```

To run this script on a reoccurring basis use CRON or some other on system schedule. CRON is show here.

 The argument in the CRON script ***must*** specify the config and log locations.

For further reference, see the ThreatQ Help Center.

Appendix A: Supplementary Information

Uninstalling the Connector

```
sudo pip uninstall tq-conn-jira
```

Driver command line options

The tq-conn-jira driver has several command line arguments that will help you and your customers execute it. They are listed below. You can see these by executing `/usr/bin/tq-conn-jira --help`.

```
usage: tq-conn-jira Connector [-h] [-ll LOGLOCATION][-c CONFIG] [-v VERBOSITY]
```

optional arguments:

```
  -h, --help
```

Shows the help message and exit.

```
  -ll LOGLOCATION, --loglocation LOGLOCATION
```

This sets the logging location for this connector. The location should exist and be writable by the current user. A special value of 'stdout' means to log to the console (this happens by default).

```
  -c CONFIG, --config CONFIG
```

This is the location of the configuration file for the connector. This location must have read and write permissions for the current user. If no config file is given, the current directory will be used. This file is also where some information from each run of the connector may be put (e.g. last run time, private OAuth, etc).

```
  -v {1,2,3}, --verbosity {1,2,3}
```

This is the logging verbosity level. The Default is 1 (Warning).

Appendix B: using the ThreatQ Project (If Required)

Only continue if you plan on using the ThreatQ Project Configuration.

This section is relevant only if the decision is made to install the ThreatQ project configuration. The configuration creates two new issue types (Event and Indicator). They will be synced with ThreatQ's Event and Indicator types. If the decision is made not to use the ThreatQ Project configuration, there is no more configuration required to use the integration.

As stated before, ensure the time zone of the JIRA instance aligns with the time zone of the machine the integration is running on.

Importing the ThreatQ Project to JIRA

The first thing needed is to import the ThreatQ Project into your JIRA instance. This will bring in all of the ThreatQ fields, screens, and issue types.

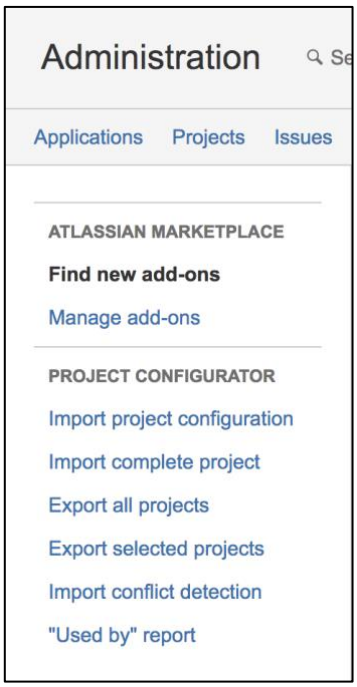
1. Install Project Configurator Add-on to JIRA

The first steps to import the project include installing the Project Configurator add-on from the JIRA marketplace.

1. Navigate to the add-on, located in the JIRA marketplace: Project Configurator.
2. Click the yellow **Try it free** button in the top right.

3. Accept the license agreement.
4. Click the **Download** button to download the Project Configurator jar file.
5. Open up your JIRA instance.
6. Click the **Settings icon** in the top right, and select the **Add-ons** menu option.
7. In the left menu under the **Atlassian Marketplace** tab, click **Manage add-ons**
8. Click the **Upload add-on** link.
    - A popup should show where you can select a file from your computer.

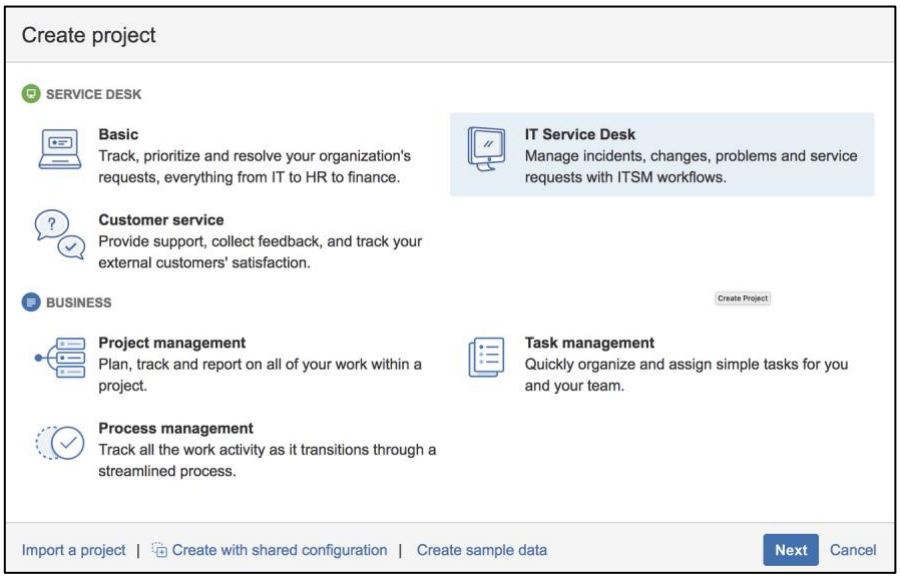
9. Click **Choose File** and select the `.jar` file you downloaded in *Step 4*.
10. Click **Upload** to install the add-on.
    - This may take a few minutes.
    - If it is still installing after five minutes, refresh the page. It should now be installed.
11. Expand the **Project Configurator** entry in the **User-installed add-ons** list.
12. Click the **Free trial** button and accept the license agreement.
    - You should now see a **Project Configurator** tab in the left menu of the **Add-ons** page (a page refresh may be required).



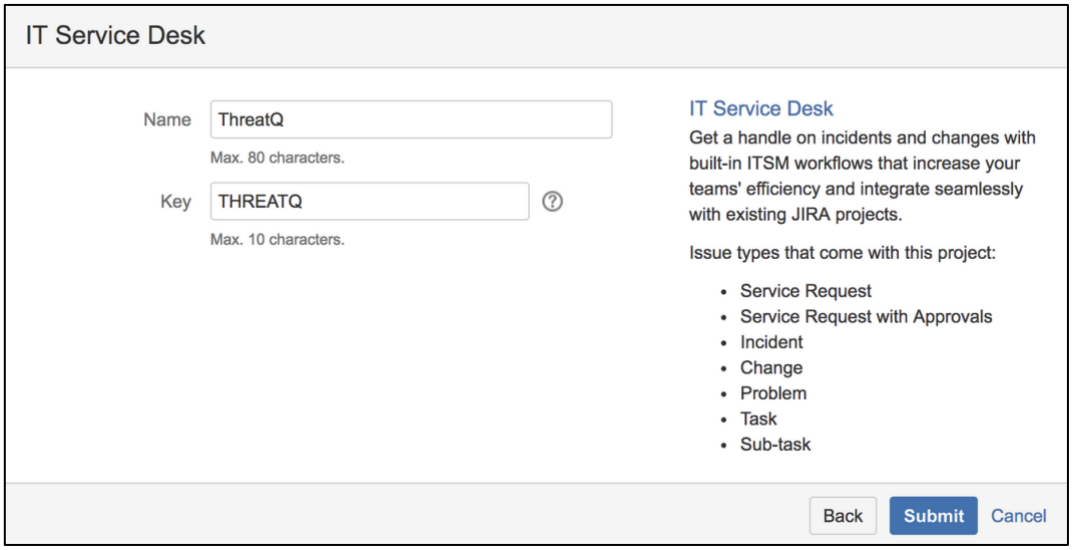
2. Creating the ThreatQ Project

This section will detail the installation process for adding the ThreatQ Project to JIRA.

1. Click the **Projects** dropdown in the JIRA navigation bar, and select the **Create Project** item.
2. Select **IT Service Desk** and click **Next**.

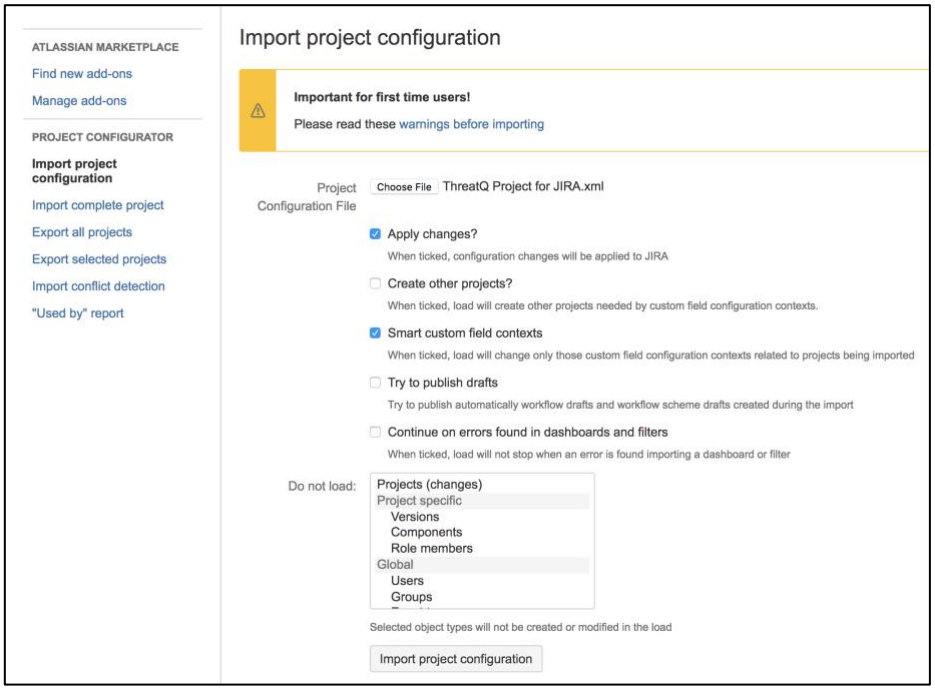


3. For name, enter **ThreatQ**, and for the key, enter **THREATQ** (all caps). Then click the **Submit** button.
    - This will create the ThreatQ base project.



4. Now we will need to import the ThreatQ Project using the Project Configurator add-on you previously installed. Go back to the Add-ons page in your JIRA settings.
5. Click the **Import project configuration** link in the **Project Configurator** tab in the left menu.
6. Click the **Choose File** button and select the **ThreatQ Project Configuration for JIRA.xml** file.
7. Check the **Apply Changes?** and **Smart custom fields contexts** fields and click **Import project configuration**.
    - This will start the import process.
    - If there are any errors, please forward them to your ThreatQ representative.
    - If there are any warnings, they should be ignorable.

    If a warning has anything to do with **THREATQ: Event** or **THREATQ: Indicator**, forward it to your ThreatQ representative via support@threatq.com.



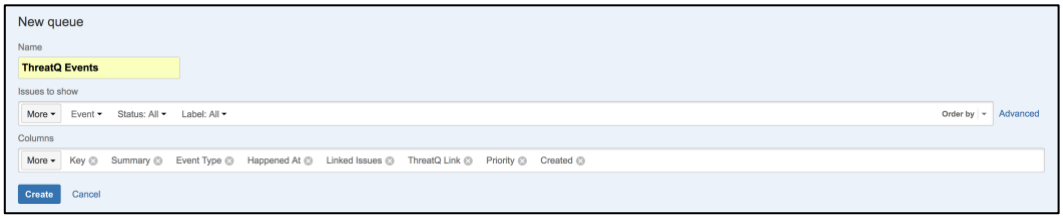
8. The custom configuration should now be in your ThreatQ Project.

3. Adding ThreatQ Event and Indicator Queues

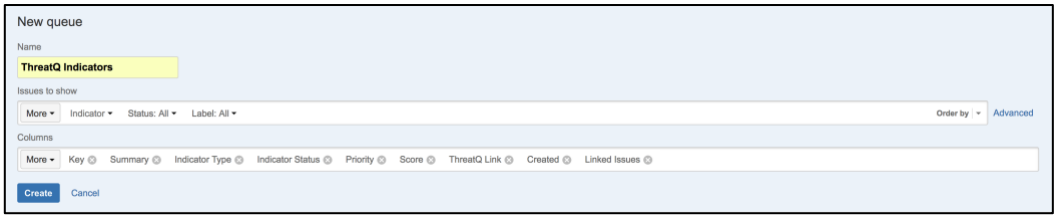
A restriction of the project configurator add-on is that it does not support exporting/importing queues. It is possible to manually create queues from the ThreatQ Project. Adding the additional queues are optional, by adding them, this will separate them from other issues that may be created.

1. In the JIRA navigation bar, click the **Projects** dropdown and select the **ThreatQ** Project.
    - Ensure you are on the **Queues** page or navigate to it. It is the first icon in the left sidebar.
2. In the **Queues** tab, there should be a **+ New queue** button at the bottom of the list. Click it add a queue.

3. The first queue to be added is the **ThreatQ Events** queue, in the name field, enter **ThreatQ Events**.
4. For the **Issues to show** field, set the **Type** to **Event**. Leave the remainder set to **All**.
5. For the **Columns** field, ThreatQuotient recommends the following columns (in order):
    - Key
    - Summary
    - Event Type
    - Happened At
    - Linked Issues
    - ThreatQ Link
    - Priority
    - Created



6. Click **Create** to create the Queue.
7. The second queue to be added is the **ThreatQ Indicators** queue, so click the **+ New queue** button again and enter **ThreatQ Indicators** for the name field.
8. For the **Issues to show** field, set the **Type** to **Indicator**, and leave the rest set to **All**.
9. For the **Columns** field, ThreatQuotient recommends the following columns (in order):
    - Key
    - Summary
    - Indicator Type
    - Indicator Status
    - Score
    - Linked Issues
    - ThreatQ Link
    - Created



10. Click **Create** to create the Queue.
11. The Queues are now fully setup.

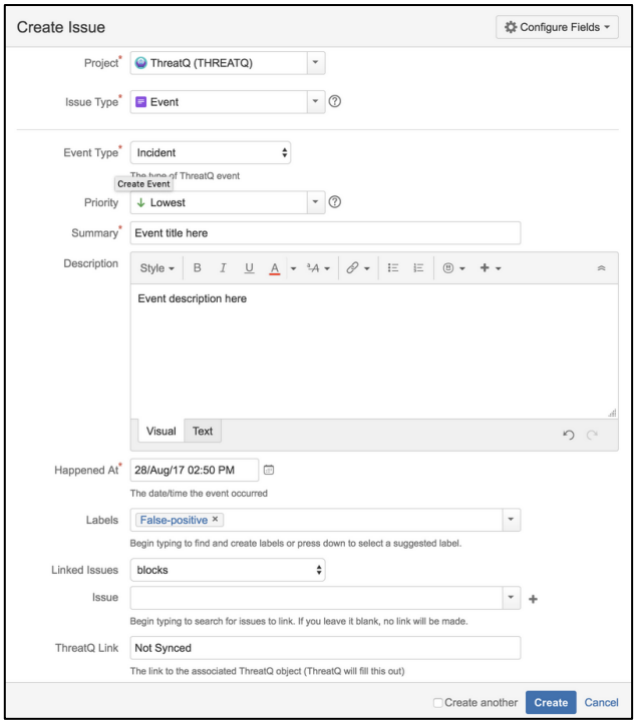
Using the ThreatQ Project

This section will outline how to create events and indicators as well as editing the fields.

1. Creating Events

Creating an event is a simple process. Events can also be linked to indicators.

1. Click the **Create** button in the JIRA navigation bar. This should bring up a popup to create an issue.
2. For the **Project** dropdown, select the **ThreatQ** project.
3. For the **Issue Type** dropdown, select **Event.** Hit **Next** if required.
4. Fill out the fields:
    - **Event Type** (required): The type of event, corresponding with the ThreatQ event types
    - **Priority**: This field will be synced as an attribute in ThreatQ.
    - **Summary** (**required**): This will be the title of the event.
    - **Description**: The description of the event.
    - **Happened At** (**required**): The date/time the event occurred.
    - **Labels**: These will be synced as attributes in ThreatQ.
    - **Linked Issues**: If you have a created indicator or event already, it can be linked using this field. For the dropdown, select **relates to**.
    - **ThreatQ Link**: ***Do not edit this field. It will be overridden by ThreatQ when synced***.

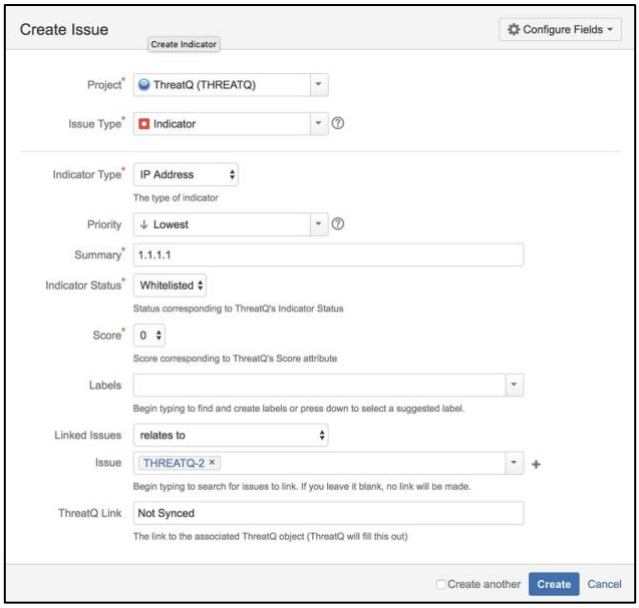


5. Click the **Create** button.
6. Once created, you can view the issue from the queue you created in the previous section.
7. If you would like to add a linked issue after creating the issue, you will need to open the issue, and then click the **Edit** button.

2. Creating Indicators

Creating an indicator is simple, and indicators can be linked to events.

1. Click the **Create** button in the JIRA navigation bar. This should bring up a popup to create an issue.
2. For the **Project** dropdown, select the **ThreatQ** project.
3. For the **Issue Type** dropdown, select **Indicator**. Click **Next**, if required.
4. Fill out the fields:
    - **Indicator Type** (**required**): The type of indicator, corresponding with the ThreatQ indicator types
    - **Priority**: This field will be synced as an attribute in ThreatQ
    - **Summary** (**required**): This will be the value of the indicator
    - **Indicator Status**: The status of the indicator, corresponding with the ThreatQ Status
    - **Score** (**required**): The score of the indicator, corresponding with ThreatQ's Scoring System
    - **Labels**: These will be synced as attributes in ThreatQ
    - **Linked Issues**: If you have a created indicator or event already, it can be linked using this field. For the dropdown, select **relates to**.
    - **ThreatQ Link**: Do not edit this field. It will be overridden by ThreatQ when synced.



5. Click the **Create** button.
6. Once created, you can view the issue from the queue you created in the previous section.
7. If you would like to add a linked issue after creating the issue, you will need to open the issue, then click the **Edit** button.

Editing the ThreatQ Project

If you would like, you can edit the ThreatQ Project; however, it is advised that you do not remove any of the default configurations that were imported. This may cause issues with the integration. You may add fields to the screens or field configurations; however, they will not be synced with the integration. They will exist only for your company's viewing purposes.

Trademarks and Disclaimers

THE SUBJECT AND SPECIFICATIONS INCLUDING ALL INFORMATION REGARDING THE PRODUCTS IN THIS DOCUMENT ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENT ARE BELIEVED TO BE ACCURATE AT THE TIME OF WRITING BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE TERMS AND CONDITIONS WHEN PURCHASED. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR THREATQUOTIENT REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THIRD PARTY SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. THREATQUOTIENT AND THIRD-PARTY SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL THREATQUOTIENT OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF THREATQUOTIENT OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

It is wholly the customers responsibility for any design requirements and the utilization of any recommendations provided by ThreatQuotient. ThreatQuotient recommendations are based upon customer information provided to ThreatQuotient at the time of the services. ThreatQuotient shall not be liable for the accuracy or completeness of the customer information contained in the ThreatQuotient recommendations.

All documentation and deliverables shall be provided in the English language, unless specifically stated otherwise. or agreed before the commencement of any services in writing.
Any costs incurred by ThreatQuotient as a result of translations requested by Customer shall be Customer’s responsibility.
In the event of any conflict between this English version and the translation(s), the English version will prevail.

ThreatQuotient and the ThreatQuotient Rhino Logo are trademarks of ThreatQuotient, Inc.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.