



# Release Notes

Version 5.28.0

Released Date: April 03, 2024


# What's New in Version 5.28.0


The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.28.0. Below is a list of enhancements, important bugs that have been addressed, and upgrade instructions.


You can access these release notes, along with other ThreatQ product documentation on the ThreatQ Help Center.




## Upgrade Impact

The upgrade is expected to take the standard amount of time for a ThreatQ upgrade. The exact time to complete the upgrade depends on your specific environment and resources.

 Upgrades to ThreatQ v5.19.0 or later require a minimum version of 5.13.0.

 Customers upgrading to ThreatQ v5.19.0 or later may be prompted to enter the MariaDB root user password to apply Process and Connection Admin grants.

 After you start the upgrade, do not cancel the installation. Doing so will leave your system in an unusable state.

Upgrading from...	Full Reindex Required	Data Migration Required	Server Reboot Required
5x (most recent version)			



## ThreatQ Platform (TQ)

The following is a list of new features and bug fixes for the ThreatQ platform included when you upgrade from ThreatQ v5.27.0, or earlier, to 5.28.0.

### NEW/UPDATED FEATURES

#### Object Details and Preview | Primary Descriptions

For all new and existing system objects, one description is labeled as the primary description. In the object details page and object preview panel, this primary description is listed first and identified with a white star on an orange background as well as a hover tooltip that displays the Primary Description label.

STIX exports include an object's primary description only. If an object has multiple descriptions, only the primary description is included in the STIX export.

After upgrading to ThreatQ v5.28, the first description added to an object is designated as the primary description by default. For existing objects, the oldest description is the primary description. For objects with multiple descriptions, you can change which description is the primary description.

#### Threat Library | STIX Export of Confidence Values

ThreatQ supports STIX exports for Confidence values that range from zero to one hundred. These values are exported as object attributes.

#### Integrations | Manual Run Options for TAXII 2x Feeds

The Start and End date fields for manual runs allow you to specify that the ThreatQ platform pulls new and updated information published by the feed provider within that time range. Since TAXII 2.1 does not support the selection of an end date, we updated the Trigger Manual Run options for TAXII 2.0 and 2.1 integrations to suppress the display of the End date and time fields and display the following helper text: This feed only supports a Start Date for manual runs and will use the current time as the End Date.

### NOTABLE BUG FIXES

- The Indicator parser included unnecessary leading and trailing characters in filenames. To resolve this, we updated filename parsing to remove leading or trailing:
  - Double, single, or Greek quotation marks
  - Parentheses
  - Pipes or braces



- Indicators listed as expired in the database were not listed as expired in the Threat Library.
- Upon upgrade from ThreatQ 4x to 5x, some attribute tables contained zero value dates (0000-00-00 00:00:00.000).
- After you updated or deleted an attribute from an object's details page, the deleted attribute remained selected which prevented a user from editing other attributes without refreshing.
- The Calculate Impact option in the Scoring page did not reflect the actual number of indicators affected by a scoring policy change.
- The Point of Contact field drop down list only displayed the first one hundred points of contact (POCs) available. As such, you could not select any POCs not among the first one hundred records. Now, the Point of Contact field allows you to scroll the first one hundred entries and use the type ahead function for subsequent POCs.
- When you created a dashboard pie chart widget that grouped results by an attribute with a large number of attribute values, the pie chart did not display.
- When you updated the object types and/or filters for a data collection and clicked Save, your changes to the data collection were not saved and the data collection reverted to its previous parameters.
- In some instances, changes to other Threat Library column display options for Indicator objects also changed the display options selected for the Source and Score columns. For instance, if the Score column was selected for display and you unselected the Type column, the Score column was also unselected. We resolved this issue so that selecting/deselecting the display of one column does not affect the display of any other column.
- In the Descriptions pane of the object details page, the Last Modified field was displayed slightly lower than the source field. We aligned the vertical display of these fields.
- When a ThreatQ instance's users were assigned as points of contact (POCs) for a large number of objects, the Search by name field in the Sharing window did not allow you to select a user to share a data collection with. In addition, the User Management page did not display a list of the instance's users.
- For customers with SSL Client Certificate Authentication enabled, when a non-maintenance user tried to log in, the Store Fingerprint to Profile window was not displayed and the user was unable to store a certificate fingerprint or log in.

## ThreatQ Investigations (TQI)

The following is a list of new features and bug fixes for the ThreatQ Investigations included when you upgrade from ThreatQ v5.27.0, or earlier, to 5.28.0.

### NEW/UPDATED FEATURES

#### Action Panel | Object Descriptions

For all new and existing objects, one description is labeled as the primary description. Within the object Descriptions section of the Action panel, this primary description is displayed first and identified with a white star on an orange background as well as a hover tooltip that displays the Primary Description label.

### NOTABLE BUG FIXES

- The initial display of the Investigations overview page took longer than usual.



## ThreatQ Data Exchange (TQX)

The following is a list of new features for the ThreatQ Data Exchange included when you upgrade from ThreatQ v5.27.0, or earlier, to 5.28.0.

### NEW/UPDATED FEATURES

#### TAXII Data Collections | Confidence Values

STIX files generated from TAXII data collections now include Confidence values listed as object attributes. Confidence values must fall within a range from zero to one hundred to be included in the STIX file.

#### Open DXL Transport | Primary Descriptions

Descriptions ingested via a Open DXL data feed are displayed in the same order on the Subscriber instance as the Publisher instance. As a result, ingested primary descriptions are listed first and identified with a white star on an orange background as well as a hover tooltip that displays the Primary Description label.



## Security and System Updates

The following System update has been made:

- Updated to Apache Solr 8.11.3.

## Install Notes

- To upgrade from a 4x version to versions 5.6 through 5.18, you must be on the most recent 4x release. To upgrade to 5.19 or later, you must first upgrade to release 5.13 or later.
- For the upgrade from the most recent 4x release to versions 5.6 through 5.18, you will need to enter your MariaDB root password during the upgrade process. To upgrade from 5.13 or later to 5.19 or later, you may need to enter your MariaDB root password during the upgrade process.
- The following warning will be displayed during the upgrade process:  
Warning: RPMD altered outside of yum.  
\*\*Found 5 pre-existing rpmdb problem(s), 'yum' check output follows  
This warning does not require any action on your part and will be resolved during the upgrade.
- Do not restart your instance during the upgrade process.



We highly recommend that you perform a backup of your ThreatQ instance before upgrading.

## How to Upgrade

### Platform Check

ThreatQ version 5x provides you with the ability to run an independent preflight check, prior to upgrading, to ensure adequate disk space. The system will also scan your installed integrations for any incompatible versions. You will be unable to perform the upgrade if an incompatible integration version is detected.



This scan does not apply to integrations installed on third-party systems such as the ThreatQ App for QRadar.

Run a platform check for the most recent ThreatQ version:

```
# sudo /usr/local/bin/tqadmin platform check
```

Run a platform check for a specific version:

```
# sudo /usr/local/bin/tqadmin platform check -v <version number>
```





## Upgrade Commands

To upgrade, run the following command:

```
# sudo /usr/local/bin/tqadmin platform upgrade
```

To upgrade to a specific version, run the following command:

```
# sudo /usr/local/bin/tqadmin platform upgrade -v <version number>
```

To discuss planning your upgrade, do not hesitate to get in touch with your Customer Success Engineer.

As always, contact our Customer Support Team if you encounter problems when upgrading or need assistance.

Thank you,

The ThreatQuotient Team

✉ [support@threatq.com](mailto:support@threatq.com)

💻 [support.threatq.com](https://support.threatq.com)

☎ 703.574.9893