



Release Notes

Version 5.10.0

Released Date: January 10, 2023


What's New in Version 5.10.0







The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.10.0. 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.

 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			
4x			

ThreatQ Platform (TQ)

The following is a list of new features, bug fixes, and new identified issues for the ThreatQ platform.

NEW/UPDATED FEATURES

Offline Bulk Delete | Remove Object Relationships

The offline bulk delete process now supports the ability to delete all relationships for an object or delete relationships created by a specified source. Contact [ThreatQuotient Support](#) for assistance with these new options.

Threat Library | Assets Object

A new system object type, Assets, is now seeded in the Threat Library. The seeding of this object type does not impact customers who already have the Assets object in place as a custom object.

NOTABLE BUG FIXES

- When you used the indicator parser to import a file with a filename longer than 128 characters, the import failed. We addressed this issue by increasing the maximum filename length to 246 and displaying the following error message when you attempt to upload a file with a name exceeding this length:
`Filename is too long to process resumable upload.`
- You were unable to change an event's type from the Threat Library object details page.
- The US-Cert Alerts CDF failed to parse TTP data from the feed.

ThreatQ Orchestrator (TQO)

The following is a list of new features, bug fixes, and new identified issues for ThreatQ Orchestrator.

NOTABLE BUG FIXES

- TQO returned an `Undefined index: sources` error under the following conditions:
 - You added an action that did not include a source key in its attribute ingestion rules to a workflow and attempted to save the updated workflow.
 - You updated a workflow that already included an action that did not include a source key in its attribute ingestion rules and tried to save your changes.

We resolved this issue by adding validation to ensure that actions contain sources.

ThreatQ Data Exchange (TQX)

The following is a list of new features, bug fixes, and new identified issues for ThreatQ Data Exchange.

NOTABLE BUG FIXES

- TQX feeds that included event objects did not include type data. As a result, feed subscribers received an error and were unable to ingest the event objects in the feed.

Install Notes

- To upgrade from a 4x version to 5x, you must be on the most recent 4x release.
- For the upgrade from the most recent 4x release to 5x, you will need to enter your MySQL 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

The TQAdmin tool used for platform checks and upgrades requires elevated privileges and must be run as root.

To elevate to root, run the following command:

```
# sudo su -
```

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:

```
# tqadmin platform check
```

Run a platform check for a specific version:

```
# tqadmin platform check -v <version number>
```

Upgrade Commands

To upgrade, run the following command:

```
# tqadmin platform upgrade
```

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

```
# tqadmin platform upgrade -v <version number>
```

To discuss planning your upgrade, don't 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

💻 support.threatq.com

📞 703.574.9893