Release Notes

Version 6.10.0

Released Date: June 25, 2025

What's New in Version 6.10.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.10.0. 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.

Migration Impact

> The migration process for ThreatQ 6.9.1 and later releases requires a ThreatQ 5.29.5 backup file. The migration process for releases prior to ThreatQ 6.9.1 requires a ThreatQ 5.29.4 backup file. If you attempt to use a backup file from a different ThreatQ 5x release, the restore process will return an error.

If you are deploying ThreatQ 6x for the first time, the upgrade requires setting up a new Ubuntu 22.04 LTS or Red Hat Enterprise Linux (RHEL) 8.10 or 9.4 instance, installing ThreatQ 6x in this new instance, and then restoring the data from your ThreatQ 5x instance. The exact time to complete the upgrade depends on your specific environment and resources.

Access the ThreatQ Help Center to view or download the ThreatQ Version 6 Installation guides. Contact our Customer Support Team or your Customer Success Engineer to request the ThreatQ Version 6 Migration guide for detailed information on migrating to ThreatQ 6x.

Upgrade Impact

If you are upgrading from one ThreatQ 6x version to another, see the How to Upgrade section for more information on executing a platform check and upgrade.

ThreatQ Platform (TQ)

The following is a new feature and list of bug fixes for the ThreatQ platform.

NEW/UPDATED FEATURES

Threat Library | Processed by Workflow Filter

The new Processed by Workflow filter allows you to filter Threat Library results by the TQO workflow that processed the objects and the time period during which the objects were processed.

User Management | Object Creation

We updated the system object parsers and system object creation modals so that if a user does not have Create, Edit, Delete permission for Sources, these parsers and modals default to the user's login as the object source.

NOTABLE BUG FIXES

- When you ingested indicators that met the criteria defined in a whitelisting rule by adding a file via the indicator parser, ThreatQ did not whitelist them. We resolved this issue so that indicators ingested via the indicator parser are whitelisted based on whitelisting rules.
- The Job Management page did not list the Search Criteria for selected objects associated with bulk change or bulk delete jobs. Now, the Job Management Search Criteria section lists the objects you selected in the Threat Library for each bulk change or bulk delete job.
- In the object details page, the whitespace around the Actions button decreased as you resized the page vertically. We resolved this issue so that resizing the page does not decrease the whitespace.
- We updated the ThreatQ TAXII Server date headers to support TAXII 2.1 specifications. TAXII 2.1 requires that the `X-TAXII-Date-Added-First` and `X-TAXII-Date-Added-Last` headers are timestamps.
- We updated the following containers to always pull the most recent version: Solr, Redis, Mongo, NGINX, and RabbitMQ.
- When you generated a PDF report for a system object with multiple descriptions, the object's primary description was not listed first. We resolved this issue so that the primary description is listed first.
- The Threat Library Flagged Objects filter continued to list objects after you bulk deleted related objects and/or unlinked object relationships to reduce object relationships to below 10,000. We updated the object deletion and relationship unlinking processes to resolve this issue.

NEW KNOWN ISSUE

- Upon upgrade from ThreatQ versions 6.7.0 through 6.7.4 to ThreatQ versions 6.8.0 through 6.10.0, users assigned to a custom role that specifies Maintenance as the default role are mapped to both the custom role and the Maintenance default user role. As a result, these users are assigned to two roles and must be manually updated to remove one role assignment.

ThreatQ v6 Installation

- Migrating to ThreatQ v6:
  - The migration process for ThreatQ 6.9.1 and later releases requires a ThreatQ 5.29.5 backup file. The migration process for releases prior to ThreatQ 6.9.1 requires a ThreatQ 5.29.4 backup file. If you attempt to use a backup file from a different ThreatQ 5x release, the restore process will return an error.
  - Access the ThreatQ Help Center to view or download the ThreatQ Version 6 Installation guides. Contact our Customer Support Team or your Customer Success Engineer to request the ThreatQ Version 6 Migration guide for detailed information on migrating to ThreatQ 6x.
- TQO Advanced Workflow Check:
  - If the preflight check for the upgrade to ThreatQ 6.8.0 or later determines that your instance includes a ThreatQ TDR Orchestrator (TQO) advanced workflow (CDW), it halts the upgrade process and returns the following message: CDW Check failed. Exiting Installation. Please reach out to TQ Support for steps to continue your upgrade. Contact ThreatQuotient Support for assistance in upgrading your system.
- Custom Group Checks:
  - If the preflight check for the upgrade to ThreatQ 6.7.4 or later encounters a user assigned to more than one user role, it halts the upgrade process and returns the following message: Custom Group check failed. Exiting Installation. Please reach out to TQ Support for steps to continue your upgrade.
    Contact ThreatQuotient Support for assistance in upgrading your system.
  - If the preflight check for the upgrade to ThreatQ 6.7.0 or later encounters a custom group, it halts the upgrade process and returns the following message: Exiting Installation. Please reach out to TQ Support for steps to continue your upgrade. Contact ThreatQuotient Support for assistance in upgrading your system.
- Pinning your RHEL 9 release:

  The following steps allow you to pin your current RHEL 9 release so that you cannot inadvertently upgrade your RHEL 9 environment to an unsupported release. See the Red Hat Enterprise Linux 9 Support section of the Help Center for more information on currently supported RHEL 9 versions.

  > Run the following commands as root or prefix them with sudo.

  1. Set release to minor version:
  2. subscription-manager release --set=<release number>
  3. Clean repositories:
  4. yum clean all
  5. Check which release is set locally:
  6. subscription-manager release --show
- Pinning your Ubuntu release:
  ThreatQ recommends you update the release-upgrades file to disable manual Ubuntu upgrades so that you cannot inadvertently upgrade your Ubuntu 22.04 environment to an unsupported release.

- Use a text editor, such as vi, to access `/etc/update-manager/release-upgrades`.
- Change the `Prompt=` setting to `Prompt=never`.
- Save your changes and exit the file.

How to Upgrade

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

Platform Check

ThreatQ 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, 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