



Release Notes

Version 6.7.3

Released Date: March 11, 2025



What's New in Version 6.7.3

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.7.3. Below is a list of 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

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 are bug fixes for the ThreatQ platform.

NOTABLE BUG FIXES

- ThreatQ returned the following error when ingesting data from a TAXII integration: Error applying filter ParseSTIX. This error occurred when the feed included more than one STIX object with a relationship to the same location. We resolved this error by updating the parsing of location information.
- In the object details page, we changed the helper text displayed in the Audit Log and and Operations search fields from Object Object to Search # records where # represents the total number of records listed in the section.
- To improve performance, we modified the process the STIX parser uses to compare objects.



ThreatQ Investigations (TQI)

The following is a bug fix for ThreatQ Investigations.

NOTABLE BUG FIXES

- When you added a comment to an investigation, the Add Comment window displayed text from a previously entered comment.



Security and System Updates

The following Security updates have been made:

- Updated the load balancer configuration on hosted systems to start applying various security-related HTTP headers.
- Upgraded to Apache Tika 3.1.0 (CVE-2024-8184).
- Websocket server:

UPDATED TO	CESA REFERENCE
axios 1.7.9	CVE-2024-39338
cookie 1.0.2	CVE-2024-47764
socket.io 4.8.1	N/A


- Frontend server:

UPDATED TO	CESA REFERENCE
axios 1.7.9	CVE-2024-39338
express 4.21.2	N/A

ThreatQ v6 Installation

- If the preflight check 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.
- The installation process for ThreatQ 6.7.3 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.

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