Release Notes

Version 6.7.2

Released Date: February 19, 2025

What's New in Version 6.7.2

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.7.2. 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 is a bug fix for the ThreatQ platform.

NEW/UPDATED FEATURES

Exports | Endpoint Access

We updated export endpoints so that users logged into ThreatQ no longer require the authentication token. For example, a user who has logged in can access the GET export endpoint without supplying the additional query parameter.

Users who are not logged into ThreatQ will continue to use the authentication token to access the export endpoint.

NOTABLE BUG FIXES

- Data collections only applied the first source in a filter set. We resolved this issue so that data collections apply all sources included in a filter set.
- When you performed a bulk update involving over 10,000 objects, the following text in the Relationships section overlapped the section's fields:
  Note: The Relationships feature is disabled when making bulk changes to over 10,000 objects.
  In addition, the relationship fields were not disabled and allowed you to update the objects. We resolved these issues by displaying the Note text below the relationship fields and disabling these fields when the bulk update involves over 10,000 objects.
- Improvements were made to hosted deployments to enhance system stability and reliability.
- The `/api/objects` endpoint returned soft deleted properties, such as object types and statuses, and included the deleted at timestamp. We resolved this issue so that the endpoint does not include these soft deleted properties nor does it include a deleted at timestamp.
- As a precaution to increase the security of on-premise ThreatQ instances, we have blocked external access to all internal ThreatQ service ports. It is still recommended that all users review the ThreatQ Version 6 Installation guide and implement a host-based firewall that blocks access to all but the listed ports.
- Resolved an issue with the ThreatQ platform where the following data failed to be ingested when utilizing the NCFTA MISP CDF integration:
  - Person: {'other', 'email', 'phone-number'}
  - Attribution: {'threat-actor'}

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 6.7.2 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