Release Notes

Version 6.11.2

Released Date: August 08, 2025

What's New in Version 6.11.2

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.11.2. 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

> Customers with large numbers of system object relationships may experience a longer than normal upgrade process. These customers should contact ThreatQuotient Support for assistance in estimating upgrade duration.

> The preflight check for the upgrade to ThreatQ 6.11.0 or later requires that your instance is running at least ThreatQ 6.10.0. See the ThreatQ v6 Installation section for more details on this preflight check.

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.

ThreatQuotient Customer Portal

ThreatQuotient will be updating the Customer Portal in the coming weeks. We will share additional details as the transition date approaches. If you have any concerns or questions, please contact ThreatQuotient Support.

ThreatQ Platform (TQ)

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

NEW/UPDATED FEATURES

ThreatQ Logo Update

We have updated the ThreatQ logo to reflect ThreatQuotient's acquisition by Securonix.

User Permissions |Custom User Roles Updates

ThreatQ v6.11.2 introduces the following enhancements to custom user roles:

- Object creation modals display only the object context fields for which you have Create, Edit, Delete permissions.
- Indicator parsers only allow you to import indicator context for which you have Create, Edit, Delete permissions.

  > For ThreatQ's Generic Text/PDF parser, ThreatQuotient requires that the parsed file only includes the indicator and its value. As such, no additional object context permissions are required.

- The Perform Bulk Manual Import permission now requires Create, Edit, Delete permissions for Attributes and Relationships as well as Objects.

  > Upon upgrade, all existing custom roles that include the Perform Bulk Manual Import permission will be updated to include Create, Edit, Delete permissions for Attributes and Relationships. Admin users and the affected custom role users will be notified of this change via the ThreatQ notification center.

- Custom role permissions control access to the pages that allow you to execute manual runs of integrations or TQO workflows. However, custom role permissions do not apply to the objects and object context created/ingested.

API | Error Logging

ThreatQ API logs now contain more detailed information on some errors.

Dynamo Multiple Workers

ThreatQ's architecture now distributes Dynamo across multiple worker pods. As such, Dynamo is able to better scale for your organization's feed processing requirements. This change improves performance and addresses scenarios where high volume or resource intensive feeds could interfere with the running and scheduling of other feeds.

Exports |Performance Improvements

We updated the export process to improve memory usage during exports that include system object descriptions or attributes.

Exports | Securonix Export

The Securonix Export is now a standard export seeded in ThreatQ. It is also the first export listed in the Exports page. This export enables the dissemination of prioritized IOCs from ThreatQ to Securonix, to be used for log enrichment and policy alerts.

NOTABLE BUG FIXES

- When you generated a PDF report for a task that was related to another task, the PDF displayed an incorrect Assigned User for the related task.
- Upon upgrading to ThreatQ 6.10.0, when you disabled the CI Army IPs integration after it began ingesting objects, the integration continued to ingest objects.
- When you exported a report object with a description that included zero-width spaces to PDF, ThreatQ returned the following error message: **There was an error retrieving records.** We resolved this issue by updating the export process to handle zero-width spaces.
- In some instances, a ThreatQ v6 install or upgrade returned the following error when the new registry pod was not available: **error executing jsonpath.** We updated the install and upgrade processes to log these errors and allow the install/upgrade process to continue.
- ThreatQ 6.8.0 introduced increased Solr CPU usage associated with ThreatQ's logging method. To resolve this issue, we changed the logging methods for a Solr transform.
- We restructured the count and handling of object relationships, improving performance and count accuracy.
- We updated the text displayed in the Integration Flagged banner to remove a reference to a list of objects displayed below the banner. The Integration Flagged banner is displayed in the configuration page of integrations that have exceeded the relationship limit for at least one system object.
- When you ingested STIX data that included an invalid STIX bundle, ThreatQ stopped the feed run and returned the following error: **AttributeError("'Location' object has no attribute 'values'")**. We updated the ingestion process so that when ThreatQ encounters a invalid STIX bundle it logs the error and continues to ingest data.

- The search field in the Indicator Type tab contained incorrect helper text. We changed this text from **Filter by Source Name** to **Filter by Indicator Type**.
- Now, the Threat Library Flagged Objects filter returns all objects that have exceeded the relationship limit.
- Upon upgrading to ThreatQ v6.10.0, customers were unable to install an operation that uses Python v3.11 due to a ModelsComponent import error. We resolved this issue by reinstating the ModelsComponent removed in ThreatQ v6.10.0.
- We updated the display of tooltips in ThreatQ so that, when you hover on a field, the tooltip is displayed above the field instead of below it.
- In some instances, when Customer Support ran an artisan command to adjust an instance's relationship limit maximum, the update process took longer than expected. As a result, if you applied the Threat Library Flagged Objects filter before the update process completed, the filter listed system objects that did not exceed the new relationship limit maximum. We resolved this issue by modifying the relationship limit update process.
- The Score Summary popover in the object details page omitted attributes whose value case did not match the case used in the Scoring Sensitivity Configuration. However, the attribute's score was included in the object's total score. For example, if your scoring algorithm assigned a score of 1 to a Product Affected attribute with a value of ThreatQ and an indicator's Product Affected value was THREATQ, the attribute was not listed in the Score Summary but its value was included in the indicator's total score. We resolved this issue by updating the Scoring Summary to display attributes whose values match the Scoring Sensitivity Configuration regardless of case.
- We updated the process for exporting a PDF summary of an object to handle additional zero-width characters: U+200C (Zero Width Non-Joiner), U+200D (Zero Width Joiner), U+FEFF (Zero Width No-Break Space)

Security and System Updates

The following Security update has been made:

- For ThreatQ hosted customers, updated to Falco helm chart 4.21.3.

ThreatQ v6 Installation

- **ThreatQ v6.10.0 Check:**
  - If the preflight check for the upgrade to ThreatQ 6.11.0 or later determines that your instance is running ThreatQ 6.9.1 or earlier, it halts the upgrade process and returns the following message: **Your installed version of <version number> does NOT meet the minimum requirement for this upgrade. Please upgrade to version 6.10.0 by running 'tqadmin platform upgrade -v 6.10.0' before proceeding to the latest.**
- **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.
- **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

> Air gapped customers should reference the **Upgrading an Air Gapped ThreatQ Instance** section of the Help Center.

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