Release Notes

Version 6.9.0

Released Date: May 15, 2025

What's New in Version 6.9.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.9.0. 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

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.

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

System Objects | Relationship Limits

ThreatQ v6.9.0 introduces a relationship limit system to assist you in managing the object relationship volume that ThreatQ ingests.

For a smaller subset of ThreatQ objects, some feed providers may include a very large number of relationships in their feeds. In some cases, these large relationship counts may have performance impacts on Threat Library queries and other ThreatQ capabilities. This feature allows you to balance the impact of excluding data that may be of limited intelligence value with the benefits of improved system performance.

Functionally, relationship limits prevent a source from adding more than a configured number of relationships to an object via an integration, bulk update, manual creation at the object level, import, or parser. Upon upgrade, ThreatQ will automatically apply the default limit setting of 10,000 relationships per object/source. The existing object relationships will not be removed. However, ThreatQ will prevent the ingestion of any additional relationships from the integration for the specific object and will flag the object and integration. See the Relationship Limits section of the Help Center for more information. The relationship limit generally applies to a small percentage of the overall objects in most ThreatQ systems.

> Please contact ThreatQuotient Support, if you have questions or concerns about the impact of relationship limits on your ThreatQ instance.

Threat Library | Workflow Runs Column

The new Workflow Runs column displays the workflows that have processed the corresponding system object.

> If an object is included in a data collection processed by a workflow run but not enriched by the workflow, the Workflow Run column for the object lists the workflow. For example, if the data collection for the Indicator Enrichment workflow includes an adversary object, Adversary1, the Workflow Run column for Adversary1 lists Indicator Enrichment.

NOTABLE BUG FIXES

- To ensure consistency with ThreatQ standards, we updated the font and icon colors used for the dark mode view of the Scoring Summary window available from the object details page and object preview pane.
- When you updated the subnet used by RKE2 via configuration changes during a ThreatQ v6 install, the terraform deployment overrode your changes and reverted to the default 10.42.0.0/15 subnet for container and service networking.
- When you added new scoring algorithms based on indicator attributes and clicked the Calculate Impact option before saving, ThreatQ displayed the same number of indicators updated for each attribute. However, if you saved your changes before clicking the Calculate Impact option, ThreatQ displayed the correct number of indicators updated for each attribute. We updated the Attributes tab to display the correct number when you click the Calculate Impact option before saving.
- When a user's role included action permissions to Edit TLP and Edit Scoring, the dark mode hover highlight for the TLP and Scoring options on the Threat Library menu extended beyond the menu. We updated the hover display in this scenario so that the highlighting does not extend beyond the menu.
- We added a Select All/Deselect All option to the Additional Permissions Required window displayed when you select the Perform Bulk Changes action permission in the User Management Roles tab or the Create Roles page.
- For read only users, related object panes displayed the options to change a related object's Confidence value and add a Comment. However, ThreatQ did not save the Confidence value change or the new Comment. We updated the object details page and object preview panel to remove the options to change Confidence values or add Comments for read only users.
- We updated the selection boxes displayed for interdependent permission options in the User Management Roles tab and the Create Roles page to prevent the borders from overlapping permission names or helper text.
- We resolved the following issues with the role deletion process:
  - ThreatQ displayed two modals that prompted you to confirm a role deletion. The first modal remained displayed after you clicked the Remove button. We updated the deletion process to display one confirmation modal, the Are you sure? modal, instead of two.
  - When you removed users from a role and then began deleting the role, ThreatQ displayed the Reassign Users & Remove Roles modal. We resolved this issue so that the Are you sure? modal is displayed in this scenario.
  - The Select a Role field in the Reassign Users & Remove Roles modal did not display available user roles. We updated the modal to allow you to select and assign a new user role for each user assigned to the user role selected for deletion.
- We updated the Add Incident modal to display the First Seen and Last Seen fields. In addition, you can now update these fields in the object details page or object preview panel.
- For on premise customers, we updated ingress configuration to disable retries on timed-out exports. This reduces the system load when long running exports are in use, and helps prevent future exports from failing.
- We updated the Spearphish Parser page to suppress the display of the Powered by CKEditor logo in the bottom right corner of the Description field.

- Upon upgrading to ThreatQ v6.8.0, any user role with permission to Run Manual Workflows (Orchestration permission) saw this permission displayed twice in the Roles tab. This was a display issue only and did not affect the function of the user role. We resolved this issue so that the permission is only displayed once.
- User roles with Perform Bulk Changes permissions were able to update object context, such as source, attributes, tags, relationships, status, and expiration date during a bulk update even if the user role did not include permission for the corresponding object context. We resolved this issue so that users cannot update object context during a bulk change without the corresponding permission(s).
- User roles with Perform Bulk Manual Import permissions were able to update object context, such as source, attributes, relationships and comments, during Indicator, Signature, Spearphish, and STIX parser imports even if the user role did not include permission for the corresponding object context. We resolved this issue so that users cannot update object context during a bulk manual import without the corresponding permission(s).

  > If a user does not have permission to update Status values, the Status field will default to Review.

- The Run Frequency field name was displayed twice in the integration Configuration tab. We resolved this issue so that the field name is displayed only once.
- Customers whose ThreatQ instances include a ThreatQ TDR Orchestrator (TQO) advanced workflow (CDW) were unable to complete an upgrade to ThreatQ v6.8.0. We resolved this by adding a preflight check for CDWs to ThreatQ v6.8.0 and by updating the migration process for ThreatQ v6.9.0 to handle CDWs.
- We updated the Spearphish and STIX parsers so that if the user does not have Create, Edit, Delete permissions for Sources, the source for in the import defaults to the user's username.
- ThreatQ returned an ERR_INVALID_RESPONSE error when you attempted to export incident objects to STIX from the object details page or object preview panel.
- When you clicked a Key field near the bottom of the Scoring Attributes tab page, the dropdown list of keys overlapped the Apply button.
- The Add Relationships and Filter by Relationship modals displayed Investigations as an option in the Limit search to field. We resolved this issue by removing Investigations from the dropdown list.
- When a CDF ingested custom objects with attributes, ThreatQ returned a Bulk Job <job number> failed to complete notification. We resolved this issue so that the ingestion of custom objects with attributes does not generate a bulk job error notification.
- The refresh button in the following locations did not refresh the page:
  - Activity Log tab
  - Feed Run Activity tab
  - Job Management page

  We resolved this issue so that when you click the refresh button, the data displayed is updated. We also resolved an issue with the expand/minimize buttons in the Add Description modal as well as the display of timezone tooltips.

ThreatQ Investigations (TQI)

The following is a bug fix for ThreatQ Investigations.

NOTABLE BUG FIXES

- When you attempted to add an indicator with an extremely large amount of data to an investigation, the indicator was not displayed on the evidence board and ThreatQ's CPU usage increased to a higher level than normal. We implemented performance improvements to resolve this issue.

ThreatQ Data Exchange (TQX)

The following is a list of bug fixes for ThreatQ Data Exchange.

NOTABLE BUG FIXES

- We changed the display of the Disabled/Enabled toggle in the Edit TAXII Collection page from left-aligned to centered.
- We updated the Relational Data section in the Create TAXII Collection and Edit TAXII Collection pages to allow you to click the object type to check/uncheck its selection checkbox. Previously, the only way to select/unselect an object type was to click the corresponding checkbox.
- When you selected all object types in the Relational Data section of the Create TAXII Collection page and clicked Save, all of the checked object types were unchecked. We resolved this issue so that the fields remain checked after you click Save.
- The refresh button in the Client Access Log tab did not refresh the page. We resolved this issue so that when you click the refresh button, the data displayed is updated.

ThreatQ TDR Orchestrator (TQO)

The following is a list of bug fixes for ThreatQ TDR Orchestrator.

NOTABLE BUG FIXES

- TQO workflows did not apply the Value Contains filter specified by a data collection to objects that used a name or title field instead of a value field. As a result, the workflow enriched objects that should have been filtered out or omitted objects that should have been included. We resolved this issue by updating the Value Contains filter to apply to objects that use name or title fields instead of value fields.
- The refresh button in the Activity Log tab did not refresh the page. We resolved this issue so that when you click the refresh button, the data displayed is updated.

ThreatQ v6 Installation

- TQO Advanced Workflow Check:
  - If the preflight check for the upgrade to ThreatQ 6.8.0 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 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 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.
- Migrating to ThreatQ v6:
  - The migration process for ThreatQ 6.8.0 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