
# Release Notes

Version 6.8.0

Released Date: May 07, 2025

# What's New in Version 6.8.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.8.0. 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 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.

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 list of new features and bug fixes for the ThreatQ platform.

## NEW/UPDATED FEATURES

### Role Based Access Control | New Action Permissions

Custom Roles now include additional Action Permissions that provide more options for controlling user access to your ThreatQ instance including permission for individual and bulk object updates, integration installation and configuration, as well as the ability to run operations.

In addition, we have updated custom roles configuration to allow you to create a custom role without selecting a default role to control object and integration permissions. Instead, you can configure object and integration permissions via more granular Action Permissions.

> After the upgrade process, existing custom roles will no longer use a default user role for object and integration level permissions. You will need to update your existing custom roles using Action Permissions.

To reflect the changes in User Management, we changed the name of the Groups column in the User Management page to Roles. This column lists the default or custom role assigned to a user.

> After you upgrade to ThreatQ 6.8.0, all Administrator users will receive the following in-app notification: New permission options are now available for custom roles. Please visit the User Management page to update your role configurations.

## NOTABLE BUG FIXES

- After upgrading to ThreatQ v6.7.0, users encountered the following issues with the Overview dashboard:
  - Under the following conditions, a user with a custom user role that included full Artifact Management permissions and a default role of Administrative Access could not view the Overview Dashboard:
    - The custom user's primary dashboard was a shared dashboard.
    - The shared dashboard owner removed the custom user's sharing permission.
  - The My Open Tasks and All Open Tasks links did not display a Threat Library list of the associated tasks.
  - Some users were unable to view the Overview of Intelligence by Score widget.
- When Read Only users accessed the object details or object preview panel, the Actions dropdown menu listed options to which they did not have access. Now, the Actions menu only lists the Export to STIX option for Read Only users.

- When a Read Only user or a custom user with view only permission for Objects performed an object search that did not return a match, the Search window displayed a Create <object name> option. This option is no longer displayed for these user types.
- The Roles tab in the User Management and the Create Role pages allowed you to assign a different role to the last Maintenance user for a ThreatQ instance. Now, if you attempt to do this, ThreatQ returns the following error message: At least one user must remain assigned to the Maintenance role to ensure continued access to system maintenance functions. Please assign another user to the Maintenance role before taking this action.
- To resolve an issue where a ThreatQ upgrade stalled during the creation of the hostpath-provisioner directory, we made the following changes to TQAdmin's handling of this directory:
  - TQAdmin now creates the directory only if it does not already exist on the RHEL or Ubuntu ThreatQ instance.
  - TQAdmin only changes the directory's SELinux context if it does not already exist on a RHEL ThreatQ instance.
- Read Only users were able to run operations on system objects. We resolved this issue so that Read Only users cannot run operations.
- When you resized the width of an Add <object type> modal, the dropdown text for some fields were not aligned correctly.
- To ensure consistency with ThreatQ standards, we updated the font color and opacity used for the Score Summary tooltip.

## NEW KNOWN ISSUES

- Upon upgrading to ThreatQ v6.8.0, any user role with permission to Run Manual Workflows (Orchestration permission) will see this permission displayed twice in the Roles tab. This is a display issue only and does not affect the function of the user role.
- User roles with Perform Bulk Manual Import permissions are 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 does not include permission for the corresponding object context.
- User roles with Perform Bulk Changes permissions are able to update object context, such as source, attributes, tags, relationships, status, and expiration date during a bulk update even if the user role does not include permission for the corresponding object context.

# ThreatQ TDR Orchestrator (TQO)

The following is a new feature for ThreatQ TDR Orchestrator.

## NEW/UPDATED FEATURES

### Workflow Optimization

Workflows apply TQO actions to objects within a data collection. This can lead to objects being processed by a workflow multiple times which increases the processing load on your ThreatQ instance and the number of requests sent to integration APIs. Workflow optimization allows you to manage system overhead associated with reprocessing data and the limits/restrictions on requests to integration APIs by providing a new configuration option to control the frequency of data reprocessing and provide greater visibility into workflow processing at the Threat Library and object level. This can mean that your existing workflows and associated data collections may need changed to match this new behavior, depending on your use case.

- Workflow Configuration - The new Allow data to be reprocessed option in the workflow builder allows you to specify how many days must elapse before an object is reprocessed. The field defaults to 30 days.

  > The number of days before reprocessing must be zero or greater. If you enter a value of zero, TQO applies the workflow action to all applicable objects in the data collection during each workflow run, which is the previous behavior

- Object Details - The Threat Library object details page and preview panel now display an Orchestrator pane that lists the workflows applied to an object. A link to the Orchestrator panel is also included in the left navigation menu above the Audit Log option. If a workflow has been applied to an object, this pane lists the workflow name and run timestamp. You can use the Orchestrator pane to view information on the last ninety days or last 10,000 workflow runs applied to the object, whichever is greater.

## Security and System Updates

The following Security update has been made:

- Python Dockerfile

| UPDATED TO | CESA REFERENCE |
|---|---|
| setuptools 78.1.0 | CVE-2024-6345 |

# 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
- 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