Release Notes

Version 6.9.1

Released Date: June 05, 2025

What's New in Version 6.9.1

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.9.1. 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 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.

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

CKEditor Upgrade and Text Field Enhancements

ThreatQ uses CKEditor to allow more formatting options for freeform text fields such as the system object description field. ThreatQ v6.9.1 includes an upgrade to CKEditor 5 to version 45.0.0.

In conjunction with this upgrade, we have added the following additional formatting options:

- Select font family. This option allows you to select from the following list of fonts:
    - Albert Sans
    - Arial
    - Bebas Neue
    - Bentham
    - Encode Sans
    - Gabarito
    - Helvetica
    - IBM Plex Mono
    - Koulen
    - Lato
    - Lisu Bosa
    - Open Sans
    - Palanquin Dark
    - Pathway Extreme
    - Playfair Display
- Remove formatting
- Increase/decrease indent.

NOTABLE BUG FIXES

- In some instances, the Remember this computer for 30 days option available to multi-factor authentication (MFA) users did not work correctly. Now, when a user with MFA enabled selects this option at login, ThreatQ will not prompt the user for MFA for thirty days when using the current browser.

  > When you upgrade to this release, ThreatQ clears all existing Remember this computer for 30 days requests and requires each user to use MFA and reselect the option if applicable/desired.

- When you selected a ThreatQ username and password from your browser’s autocomplete list during login, the username you selected overlaid the field name.
- For related objects, the Sources column in the object details page and object preview panel did not display the color icon corresponding to the related object’s TLP label. We updated the Sources column for related objects so that it now displays the object’s TLP color icon.
- When the spreadsheet cells you pasted into an object’s Description field exceeded the field width or length, the pasted data was either truncated or not displayed. We resolved this issue so that pasted fields are displayed correctly.
- In some instances, ThreatQ exports returned a 504 Gateway Time-out error. We resolved this by increasing the timeout interval.
- We addressed an intermittent issue which prevented the retrieval of data for dashboard widgets during automatic updates.

- Upon upgrade to ThreatQ v6.9.0, some customers encountered API and Redis log errors as well as issues with feed ingestion due to Redis persistent volume claims (PVCs). We resolved these issues by updating the Redis configuration. In addition, the 6.9.1 upgrade process includes an updated relationship limit count migration.

Security and System Updates

The following Security update has been made:

UPDATED TO	CESA REFERENCE
fluentbit 4.0.1	CVE-2024-5535 CVE-2024-4741 CVE-2024-2511 CVE-2024-12133 CVE-2023-5678 CVE-2024-9143 CVE-2024-0727

ThreatQ v6 Installation

- Migrating to ThreatQ v6:
    - The migration process for ThreatQ 6.9.1 requires a ThreatQ 5.29.5 backup file. The migration process for release 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.
- TQO Advanced Workflow Check:
    - If the preflight check for the upgrade to ThreatQ 6.8.0 or later 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 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

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

THREATQ

✉ support@threatq.com
🖥 support.threatq.com
☎ 703.574.9893