Release Notes

Version 6.7.4

Released Date: April 02, 2025

What's New in Version 6.7.4

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.7.4. 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 6.7.4 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 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

Integrations | STIX Attribute Updates

Previously, when you imported a STIX 2.0 or 2.1 object attribute update from the same TAXII feed, the updated attribute was added as a new attribute in ThreatQ. Now, when you import updated values for the following attribute types from the same feed, the attribute value is updated in ThreatQ instead of being saved as a new attribute:

- administrative_area
- city
- county
- country
- identity_class
- last_seen
- latitude
- longitude
- number_observed
- postal_code
- precision
- primary_motivation
- region
- resource_level
- sophistication
- street_address
- tool_version
- valid_from
- valid_until

For example, the CAR54 object has a valid_until attribute of 04/02/2025 with a source of YellowCab. When you import an updated valid_until attribute of 05/02/2025 from the YellowCab feed, ThreatQ updates the valid_until attribute to 05/02/25.

Same-source updates to attributes types not listed above as well as attribute updates from a different source are stored as new attributes in ThreatQ.

Integrations | ACE Parser

To reduce false positives, we updated the ACE parser's matching process and stop list. Now, the matching process filters matched malware and adversaries with quotes or the first letter capitalized. For example, this change would exclude [spyware bears]. However, the matching process remains the same if the adversary name is in quotes ("spyware bears"). In addition, matched numbers are now filtered out. For example, [BitHurt 2.0] becomes [BitHurt].

In updating the stop list, we added several known false positives, such as taskhost.exe, to the list.

NOTABLE BUG FIXES

- When the number of exports displayed in the Exports page equaled the value in the Row count field, the Previous and Next button were displayed. Both buttons were greyed out/inactive. We resolved this issue so that the Previous and Next buttons are only displayed when the number of exports exceeds the number specified in the Row count field.

- When a user with a default user role other than Administrator or Maintenance User, accessed the Exports page all export toggles were greyed out/inactive. However, when the user clicked an export's toggle to enable/disable it, ThreatQ returned the following error message: Failed to update export. We resolved this issue so that ThreatQ does not return an error message when these users click an inactive export toggle.
- When you viewed ThreatQ using a display width compatible with a tablet, some Limit search to field options in the Add *<system object type>* modal overflowed the field and some of the option text was displayed below the field. Now, in this scenario, the option text is truncated instead of overflowing the field.
- We updated the amber and amber+strict TLP colors displayed in ThreatQ to match the hex value (#FFC000) specified by Traffic Light Protocol standards.
- OAuth2 clients received the following error message when attempting to access the scoring endpoint: You are not permitted to access this resource.
  We resolved this issue by updating the OAuth2 artisan command to map OAuth2 clients to RBAC roles and moving the source creation process into this command. In addition, integrations and plugins are mapped to the Administrator role.
- In some instances, the LDAP debugging artisan command succeeded in connecting to an ADFS server, but returned an Unable to bind to server error if the port was secure. We updated the command so that the bind process can now succeed with a secure port.
- When you configured a ThreatQ instance's disclaimer text to display in red, ThreatQ displayed the text in blue. We resolved this issue so that the disclaimer is displayed in the configured color.
- ThreatQ now returns the following error message when you attempt to upload an integration with an unsupported or invalid file extension: *<filename>* is not allowed, please upload a yaml, yml, whl or zip file.

ThreatQ Data Exchange (TQX)

The following is a bug fix for ThreatQ Data Exchange.

NOTABLE BUG FIXES

- We updated the Create Feed and Edit Feed pages to display the Add button below the This feed has no recipients message instead of beside it.

ThreatQ TDR Orchestrator (TQO)

The following is a bug fix for ThreatQ TDR Orchestrator.

NOTABLE BUG FIXES

- TQO now returns the following error message when you attempt to upload a workflow with an unsupported or invalid file extension: *<filename>* is not allowed, please upload a yaml, yml, whl or zip file.

Security and System Updates

The following Security updates have been made:

- To address Ingress NGINX Controller for Kubernetes vulnerabilities, we upgraded the following components. We also took additional steps to reduce potential ingress-nginx attack surface.

UPDATED TO	CESA REFERENCE
ingress-nginx-controller v1.12.1 helm_chart_version 4.12.1	CVE-2025-24513 CVE-2025-24514 CVE-2025-1097 CVE-2025-1098 CVE-2025-1974

- TAXII Server Container:

UPDATED TO	CESA REFERENCE
aiohttp 3.11.13	CVE-2024-52303 CVE-2024-52304
jinja2 3.1.6	CVE-2024-56201 CVE-2024-56326

ThreatQ v6 Installation

- 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.
- 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
- 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 migration process for ThreatQ 6.7.4 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