



Release Notes

Version 6.7.0

Released Date: February 01, 2025



What's New in Version 6.7.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.7.0. 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.

ThreatQ 4x End of Life

ThreatQuotient provides support for the most current major version of ThreatQ and the immediately previous major version of ThreatQ only. With the general availability of ThreatQ 6x, support for ThreatQ 4x has reached end of life as ThreatQ 6x is the current major version and ThreatQ 5x is its immediate predecessor.

As such, we recommend that any customer still on a ThreatQ 4x version upgrade as soon as possible. Contact [ThreatQuotient Support](#) if you have questions or need assistance with upgrading to a supported version.

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 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 a bug fix for the ThreatQ platform.

NEW/UPDATED FEATURES

Role Based Access Control (RBAC)

You can now combine granular action permissions and permissions settings from default user roles (Administrator, Maintenance, Primary Contributor, and Read Only) to create custom roles that customize user access and provide more robust role-based action control (RBAC). This approach to managing user access allows you to ensure that users have the access they need and minimize their exposure to data and functions they do not require access to.

You will continue to have access to use the existing default roles: Administrator, Maintenance, Primary Contributor, and Read Only. Users currently assigned to these roles will continue to reside under these after migration and these defaults will remain available for use in managing user roles going forward. You can choose to reassign these users to any custom roles created after this upgrade.

See the Custom Roles section of the ThreatQ Help Center for more information on creating and updating custom roles.



The upgrade to ThreatQ v6.7.0 preserves all your existing user accounts and their currently assigned default user groups.



ThreatQ v6.7.0 includes a preflight check for custom groups. If the preflight check encounters a custom group, it halts the upgrade process and returns the following message: Exiting Installation. Please see the release notes relating to Custom Groups.

Contact ThreatQuotient Support for assistance in upgrading your system.


Integrations | Filter Feed Run Activity by Status

The new Status field in the Feed Run Activity tab allows you to filter the information displayed by feed run status. By default, the tab displays all feed runs and gives you the option to limit the list to All, Completed, Completed with errors, or Run failed statuses.



Integrations | ACE Parser

We have updated and improved how the ACE Parser matches against Threat Library system objects.

 If you have integrations that utilize the ACE parser, upgrading to ThreatQ 6.7.0 may result in the ingestion of unwanted data from those integrations due to the updates made to the parser. To prevent this, the ThreatQ version 6.7.0 preflight check will alert you if you have any of the affected integrations. You will be directed to contact ThreatQ Support for further assistance with your platform upgrade.

NOTABLE BUG FIXES

- Resolved a No_Proxy issue where using an IP Address in the No_Proxy UI field resulted in the following message: `ValueError: too many values to unpack`.

ThreatQ Data Exchange (TQX)

The following is a bug fix for ThreatQ Data Exchange.

NOTABLE BUG FIXES

- In ThreatQ v6.6.0 instances, subscribers were unable to unsubscribe from feeds.

ThreatQ v6 Installation

- 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 see the release notes relating to Custom Groups.
Contact ThreatQuotient Support for assistance in upgrading your system.
- The installation process for ThreatQ 6.7.0 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