



Release Notes

Version 5.9.0

Released Date: December 20, 2022


What's New in Version 5.9.0







The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.9.0. 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.

Upgrade Impact

The upgrade is expected to take the standard amount of time for a ThreatQ upgrade. The exact time to complete the upgrade depends on your specific environment and resources.

 After you start the upgrade, do not cancel the installation. Doing so will leave your system in an unusable state.

Upgrading from...	Full Reindex Required	Data Migration Required	Server Reboot Required
5x			
4x			

ThreatQ Platform (TQ)

The following is a list of new features, bug fixes, and new identified issues for the ThreatQ platform.

NEW/UPDATED FEATURES

Threat Library | Relationship Criteria Filter Option

The new Tag option for Relationship Criteria filters allows you to filter your results based on the tag(s) associated with related objects. In addition, you can specify that a related object must meet all or at least one of your Tag criteria.

Threat Library | Query Optimization

We restructured the Threat Library query process to significantly improve the efficiency and performance of Threat Library searches.

Common Access Card (CAC) and SSL Client Certificate Authentication

ThreatQ now supports SSL Client Certificate Authentication by allowing on-premise customers to upload PEM-encoded CA certificate files. After this file is uploaded and configured, individual ThreatQ logins can be associated with a user's certificate SHA-1 fingerprint. This allows users to authenticate and access ThreatQ via their:

- Common Access Cards (CACs)
- Personal Identity Verification (PIV) cards
- Smart cards
- SSL client certificates

See the [SSL Client Certificate Authentication](#) section of the Help Center for more information on configuring and using this authentication method.

The configuration page for all CDFs now displays a Run Now button upon enabling.

NOTABLE BUG FIXES

- When you created a dashboard table or line widget that included expiration dates, the widget did not display any expiration dates.
- When you used the Indicator Parser to import indicators, you could not add a relationship to the imported indicators.
- An upgrade from 4.58.1 to 5.8 failed due to the presence of system objects configured to never expire.
- After an upgrade from 4.58 to 5.8, a customer's Threat Library did not contain any system objects. This was caused by a conflict during the migration between system and custom objects with similar names.
- When you created a Threat Library Relationship Criteria filter and then selected the Any Object and Value Contains options, the Apply button in the Relationship Criteria window was inactive/grayed out and did not allow you to apply the filter.
- We resolved the following indicator parsing issues:
 - When parsing for indicators, part of an XML start tag could be included in filename indicators.
 - Filenames that end in .sys and .pnf were not parsed.
- When you reloaded a dashboard after adding widgets to it, the widgets were displayed in different positions from the layout you created.

Security and System Updates

The following Security Updates have been made:

- Remote CentOS Linux 7 host:

UPDATED TO	CESA REF
Device Mapper Multipath 0.4.9	CVE-2022-41974
Kerberos 5 Release 1.15.1	CVE-2022-42898

Install Notes

- To upgrade from a 4x version to 5x, you must be on the most recent 4x release.
- For the upgrade from the most recent 4x release to 5x, you will need to enter your MySQL root password during the upgrade process.
- The following warning will be displayed during the upgrade process:
Warning: RPMD altered outside of yum.
**Found 5 pre-existing rpmdb problem(s), 'yum' check output follows
This warning does not require any action on your part and will be resolved during the upgrade.
- Do not restart your instance during the upgrade process.



We highly recommend that you perform a backup of your ThreatQ instance before upgrading.

How to Upgrade

The TQAdmin tool used for platform checks and upgrades requires elevated privileges and must be run as root.

To elevate to root, run the following command:

```
# sudo su -
```

Platform Check

ThreatQ version 5x 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:

```
# tqadmin platform check
```

Run a platform check for a specific version:

```
# tqadmin platform check -v <version number>
```

Upgrade Commands

To upgrade, run the following command:

```
# tqadmin platform upgrade
```

To upgrade to a specific version, run the following command:

```
# 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