



Release Notes

Version 5.11.0

Released Date: February 02, 2023


What's New in Version 5.11.0







The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.11.0. 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			

 If you are upgrading to this release from 5.6 or earlier, a full reindex is required.

ThreatQ Platform (TQ)

The following is a list of new features and bug fixes for the ThreatQ platform available when you upgrade from ThreatQ v5.10.1, or earlier, to 5.11.0.

NEW/UPDATED FEATURES

System Configurations | Display Mode

Maintenance and Administrative Access users can use the Screen Display options in the General tab on the System Configurations page to select a system-wide Light, Dark, or Split display mode for ThreatQ. The display mode defaults to Split mode which reflects the pre-upgrade mix of light and dark pages currently displayed in ThreatQ. If you change the display mode, the new mode updates the display for all users the next time they log in.

Threat Library | Updating Filters

When you create a With Attribute, Without Attribute, or Relationship Criteria filter and add attributes to it, you now have the option to delete the last attribute row. Previously, the last attribute row for these filters did not display a delete button.

Text Wrapping

We standardized text wrapping within the ThreatQ Platform and all associated ThreatQ products such as ThreatQ Investigations (TQI), ThreatQ TDR Orchestrator (TQO), and ThreatQ Data Exchange (TQX). These products now wrap text by word with the exception of hash values which are wrapped by character.

NOTABLE BUG FIXES

- Restoring a ThreatQ instance caused the following issues:
 - The restore process reset permissions for `/var/files/log/threatq-dynamo.log`.
 - The system was unable to ingest Spearphish events.

- Feed data was not removed by the restore process.
- The Indicator Parser stopped parsing a URL when it encountered a double forward slash (//).
- When you created an Expiration Date filter, the filter date displayed and applied in the Threat Library results page was one day prior to your selected date. For instance, if you selected 1/23/2023, the filter pill and Threat Library results reflected 1/22/2023.
- The Disabled/Enabled toggle, Run Integration button, and Install/Uninstall button were displayed without space between them. We updated the display to include space between each.
- All configuration driven feeds (CDFs) require a source. This made it difficult to use a feed strictly for its filters chain. To resolve this issue, we added the ability to nullify a CDF source.
- In some instances, Dynamo could become stuck processing tasks. This in turn blocked other feeds from running.
- When you added an attribute to an object, it took longer than normal to populate value results associated with the attribute name.
- Data collections that contained an attribute filter did not return the expected data in some cases.
- The Add New TAXII Feed tab in the Add New Integration window did not allow you to select a 2.1 as the TAXII Server Version.
- Imports failed when Solr encountered a value that exceeded 32,766 bytes and returned a `RuntimeException`. To resolve this, we updated value truncation to be based on bytes instead of characters so that the system truncates values over 32,766 bytes and continues the import process.
- When loading dashboard widgets, the system sent multiple requests. We streamlined this process so that the system sends a single request when loading dashboard widgets.
- When you applied a Threat Library keyword filter with a leading or trailing space, the system returned a 500 error.
- The Incoming Intelligence Dashboard did not list individual enabled feeds or their indicator ingestion totals.
- The expiration migration portion of the ThreatQ upgrade process took longer than anticipated.

NEW KNOWN ISSUES

- You cannot upgrade a previously installed Operation to a new version. When you upload the new version's WHL file via the Add New Integration window and click the Upgrade button, the button becomes inactive and the upgrade is not initiated. The ThreatQuotient team is actively working on this issue. If you need to upgrade an existing operation, you can delete the existing operation and then install the new version.




Deleting an operation does not delete the data it has ingested into the platform.

Security and System Updates

The following System updates have been made:

- Configured the `PermitRootLogin` parameter to prevent root logins over SSH.

 After upgrading to 5.11.0, you will no longer be able to use root to log into the console. You will need to create an alternate non-root OS/Linux user with sudo privileges to access the console.

- Updated firstboot Apache configuration to mitigate against the HTTP TRACK/TRACE method vulnerability and added security-tuned header configurations.
- Remote CentOS Linux 7 host:

UPDATED TO	CESA REF
CKEditor 35.4.0	CVE-2022-31175

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