



# Release Notes


Version 5.18.0

Released Date: August 10, 2023

# What's New in Version 5.18.0


The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.18.0. 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.







 To prepare for future upgrades, ThreatQuotient recommends you upgrade to ThreatQ v5.13.0 or later. All upgrades after ThreatQ v5.18.0 will require a minimum version of 5.13.0.

## 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.

 Customers upgrading from a 5x release prior to 5.12.1 will be prompted to enter their MySQL root password during the upgrade process to allow an adjustment of the subnet mask of the Solr MySQL user's host.

 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 (most recent version)			
4x (most recent version)			

 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 v5.17.0, or earlier, to 5.18.0.

### NEW/UPDATED FEATURES

#### Threat Library | TLP Label Updates

ThreatQ now supports the Amber+strict TLP label assigned to sources. In addition, we updated the name of the White TLP label to Clear to reflect current TLP designations.

As such, these labels can be mapped to sources imported into ThreatQ through integrations, assigned as a source default through the system-level TLP settings, and assigned to a specific object's source via the Threat Library object details page. They are also available as an output format option for Exports as well as a Threat Library TLP filter option.

Upon upgrade, ThreatQ updates all existing sources with a White TLP label to Clear and handles all integration, data collection, and export references to the White label as references to the Clear label. Ingested sources with the White TLP label are automatically converted to Clear. Existing data collections and exports that reference the White TLP label will continue to work as before.

#### Job Management | System Delete Tab

The new System Delete tab in the Job Management page lists attribute deletions initiated by consuming data from integrations.. These jobs are only listed in the System Delete tab and are not listed in the All tab. In addition, data retention policy jobs are only listed in the Retention Policy tab and are no longer listed in the All tab.

### NOTABLE BUG FIXES

- The Group By search field in the Bar Chart and Pie Chart window did not adjust the options listed to reflect your entry. For example, if you typed "author", the group by list continued to display tags, sources, and author instead of listing only the option that matched your entry.
- During an upgrade, permissions for the /var/fi le/I og directory were not updated. We updated permission handling to ensure that permission updates are applied during upgrades.
- In the Threat Library, the Must Match: Any/All options were not displayed for CIDR block or author filters. We updated these filters to display the Must Match options and to default to the Any option.
- When you used the ThreatQ Ace Operation to parse a non-indicator system object with the Dry run option selected, you could not add the indicators extracted to the Threat Library. Instead, when you clicked the Add Selected Indicators button, the button displayed a Saving message and did not complete the process.

- When you created a Threat Library attribute search that included double quotes around a term (for example, "dib") and applied a bulk update to the search results, the process completed without returning an error or updating any of the selected objects.
- We resolved the following display issues in the Bar Chart window:
  - Increased the bottom margin of the No results found message displayed for the Group By field.
  - Updated the Group By field helper text to reference a bar chart instead of a pie chart.
  - When you ingested a custom object with a value that exceeded the field maximum, ThreatQ truncated the value. However, when you ingested the custom object again, the system returned an internal server error.



## ThreatQ Investigations (TQI)

The following is a bug fix for ThreatQ Investigations available when you upgrade from ThreatQ v5.17.0, or earlier, to 5.18.0.

## NOTABLE BUG FIXES

- When you had a large number of investigations, it took more time than usual to load all of the investigation cards in the TQI overview page. To improve performance, we updated the investigation card load process.



## ThreatQ TDR Orchestrator (TQO)

The following is a list of bug fixes for ThreatQ TDR Orchestrator available when you upgrade from ThreatQ v5.17.0, or earlier, to 5.18.0.

### NOTABLE BUG FIXES

- In some instances, TQO returned a timeout error when you attempted to create or edit a workflow.



## Security and System Updates

The following Security updates have been made:

- Remote CentOS Linux 7 host:

UPDATED TO	CESA REF
Bind 9.11.4	CVE-2023-2828
Linux Kernel 3.10.0	CCVE-2022-3564

## 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.
- Customers upgrading from a 5x release prior to 5.12.1 will be prompted to enter their MySQL root password during the upgrade process to allow an adjustment of the subnet mask of the Solr MySQL user's host.
- 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

### 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:

```
# 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, do not 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](mailto:support@threatq.com)

💻 [support.threatq.com](https://support.threatq.com)

📞 703.574.9893