



Release Notes

Version 5.14.0

Released Date: April 27, 2023


What's New in Version 5.14.0


The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.14.0. 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.

 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 v5.13.1, or earlier, to 5.14.0.

NEW/UPDATED FEATURES

Backup and Restore Process Changes

We made the following changes to the ThreatQ backup and restore processes:

- If you run a standard backup and encounter an error during the Solr backup, the backup process continues without backing up Solr. Restoring from the backup file will require a Threat Library re-index.
- A new backup command parameter allows you to perform an online backup which backs up your database without performing a Solr backup and allows users to work in the ThreatQ instance as the backup runs.



The new online backup process takes longer to complete and generates a larger backup file.

- When you restore from an online backup, the following message prompts you to decide when to perform a Solr re-index.

Do you want to re-index Solr now? If not, you may do this manually later. [y/n]

See the Backup and Restore section of the Help Center for more information on the new online backup option.

Job Management | Estimated Time Remaining for Jobs

The Percent Complete column in the Job Management page now lists the estimated time remaining for a job.

Integrations | OAuth Registration Command Options

We added list and update options to the OAuth Registration command. The list option allows you to generate a list of clients based on their assigned group. The update option allows you to change the client secret for existing credentials. See the OAuth Credentials section of the Help Center for more information.

Integrations | Containerized Operations

To increase security and provide process isolation, we modified Operation Integrations to run in separate containers.



See the New Known Issues section for details regarding specific operations affected.

Object Details | Read Only Access Permissions

Read Only Access users are now unable to delete a system object's source or edit a source's TLP status from the object details page. Also, since Read Only Access users cannot delete tags, we updated the display of tags for Read Only Access users to a format that does not contain the x (delete) icon.

Threat Library | New Action Buttons

The drop-down list of Actions displayed above your Threat Library results has been replaced by the Export and Bulk Actions buttons. These buttons allow you to export your results list to a CSV file and/or apply bulk changes/deletes to the listed system objects.



The Action buttons displayed vary based on your account role. Maintenance Account, Administrative Access, and Primary Contributor Access users can access both the Export and Bulk Actions buttons. Read-only users can only access the Export button.

NOTABLE BUG FIXES

- When you updated the sharing permissions for a Data Collection used in a TQO workflow, the system returned the following error: Error adding sharing permissions.
- When you applied a Source filter without an Is Only parameter to your Threat Library and then bulk deleted/updated the results, the Job Management page listed the Is Only parameter in the job details search criteria section.
- When you created a pie or bar chart widget that included grouping by Author and clicked it to view the associated Threat Library page, the system returned the following error message: A Threat Library filter doesn't exist for this. In addition, the Threat Library page listed an incorrect object count and did not display the author filter.
- When you created and enabled a Disclaimer, the text displayed at login included HTML formatting tags.
- In the Threat Library, the display of task objects with IDs of two or more digits was wrapped so that the digits were displayed on separate lines. In addition, these tasks were sorted incorrectly when you sorted tasks by ID.
- When you clicked the more option to expand a long attribute value in the object details page, the expanded value field continued to display an ellipsis before the less option.
- Upon upgrade to ThreatQ v5.13.0, CSV exports of Indicators did not include the expired_at column.
- A Threat Library With Attribute filter that specified a value of 0 (zero) did not filter out non-zero attribute values.
- The Signature Parser did not accept YARA rules that contained a \r escape sequence to indicate a carriage return.
- When you accessed the object details page and clicked the preview icon to view a system object's signatures or events, the system returned the following error message: Failed to retrieve object details.
- In integration details pages, the Helper text for configuration options was displayed beside the options instead of under them.
- In the Job Management page, when you viewed job details that included lengthy Relationship Criteria parameters, the display of this field pushed the subsequent Update and Activity fields outside of the jobs table.

NEW KNOWN ISSUES

- If you attempt to install the ThreatQ ACE Operation after upgrading to 5.14, the installation fails. In addition, current installations of the operation are not compatible

with 5.14. An updated version of the operation will be available in the near future to address this issue. Contact ThreatQ Support if you require access before the operation's release on the ThreatQ Marketplace.

- If you are using VirusTotal Operation v2.3.0 (released December 2020) or older, you must upgrade to the latest version, version 3.0.1. Updates included in version 5.14.0 are not compatible with older versions of the VirusTotal operation (2.3.0 and older). Customers using VirusTotal Operation v3.0.0 and v3.0.1 are not affected by this update.

ThreatQ TDR Orchestrator (TQO)

The following is a list of new features and bug fixes for ThreatQ TDR Orchestrator available when you upgrade from ThreatQ v5.13.1, or earlier, to 5.14.0.

NEW/UPDATED FEATURES

Manually Triggered Workflows

We increased the flexibility of TQO by giving Maintenance Account and Administrative Access users the option to run workflows on-demand from the Threat Library against a group of indicators or a single indicator. After you filter your Threat Library results or select a Data Collection, the new Start Workflow button allows you to select the workflow(s) you want to run and begin workflow processing. From the object details page, the new Start Workflow option on the Actions menu allows you to select the workflow(s) you want to run for a specific indicator.

In addition to these changes, we consolidated workflow configuration options including data collection, scheduling, notification, and debug options into the workflow node panel. And, a new scheduling option, No Schedule, allows you to create a workflow that runs only when manually triggered either from the workflow node view or the Threat Library. Workflows that use this scheduling option must include at least one action. A workflow configuration that does not contain a data collection can only be used for manual workflow runs from the Threat Library results or object details pages.

NOTABLE BUG FIXES

- When you installed a group of actions from a single YAML file, any action with a namespace value that included a capital letter failed to install.
- When you uninstalled an action, the Are You Sure? confirmation window listed the action name as undefined.
- When you created a workflow without selecting a run schedule, TQO ran the workflow as soon as you enabled it.
- In the Orchestrator page, the display of workflows with IDs of two or more digits was wrapped so that the digits displayed on separate lines.

ThreatQ Investigations (TQI)

The following is a list of new features and bug fixes for ThreatQ Investigations available when you upgrade from ThreatQ v5.13.1, or earlier, to 5.14.0.

NOTABLE BUG FIXES

- We changed the confirmation message displayed when you delete a timeline entry to:
Are you sure you want to delete this timeline entry? This cannot be undone.

Security and System Updates

The following System updates have been made:

- Resolved a firewall configuration issue that exposed a series of services to the external interface of an on-premise instance of ThreatQ.
- Updated WebSocket to version 4.35.0.
- Updated RabbitMQ to version 3.11.13.

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

💻 support.threatq.com

📞 703.574.9893