



Release Notes

Version 5.19.0


Released Date: September 06, 2023


What's New in Version 5.19.0


The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.19.0. 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.

 Upgrades to ThreatQ v5.19.0 require a minimum version of 5.13.0.

 Customers upgrading to ThreatQ v5.19.0 may be prompted to enter the MariaDB root user password to apply Process and Connection Admin grants.

 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 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 v5.18.0, or earlier, to 5.19.0.

NEW/UPDATED FEATURES

Threat Library | STIX Export for Indicators

ThreatQ supports STIX export for the following indicator object types:

- ASN
- Binary String
- CIDR Block
- CVE
- Email Address
- Email Attachment
- Email Subject
- File Path
- Filename
- FQDN
- IP Address
- IPv6 Address
- MAC Address
- MD5
- Mutex
- Password
- SHA-1
- SHA-256
- SHA-512
- x509 Serial
- x509 Subject
- URL
- User-agent
- Username
- X-Mailer



The STIX export does not include related objects.

Each STIX export can contain up to 50,000 indicators. If you attempt to exceed this maximum, a tooltip is displayed indicating that the export option is available for searches under 50,000 objects.

Threat Library | Default Cache Update

We increased the default cache for Threat Library searches from two to ten minutes.

TQAdmin | Minimum Version Requirement for Upgrade

TQAdmin's preflight check now requires that customers upgrading from a 4x or 5x release to 5.19.0 or later have a minimum version of 5.13.0. If a ThreatQ instance does not meet the minimum version requirement for the upgrade, the upgrade process halts and TQAdmin provides information on the requirements to resume the upgrade.



Indicator and Signature Status Overrides

ThreatQuotient created new artisan commands that allow you to change status handling on indicators and signatures updated via feed ingestion. When you run the artisan command to enable this functionality:

- An existing indicator's status is overridden with the default status configured in the CDF.
- An existing signature's status is overridden with the default status of Active.

A second artisan command disables this functionality and returns your system to default handling of indicator and signature status updates. See the Commands section of the Help Center for more information on these artisan commands.

Job Management | Job Archiving

A job archive process runs each day at 2 AM to archive user-initiated jobs ninety days after their creation date and system-initiated jobs 365 days after their creation date. The archived jobs no longer display in the Job Management page but are stored in a historical partition that can be queried.

NOTABLE BUG FIXES

- If your ThreatQ environment contained over 100,000 attributes, when you entered an attribute name in the Add Details window, the type ahead process took more time than usual to return potential matches.
- If your Threat Library results list contained more than 10,000 objects and you selected a subset for a bulk update, the Relationships fields in the Bulk Changes page were inactive. This occurred because the validation for these fields was based on the total number of objects in your search results instead of the number of objects selected for the update.
- In some instances, a MISP import resulted in duplicate indicator records.
- Users with Read Only access were unable to view scores in the object details page. However, they could view scores in the Threat Library.
- To prevent the ingestion of duplicate indicator objects, we updated the indicator deduplication process to mirror the signature deduplication process.
- When you created a Threat Library relationship criteria filter with a Date Created parameter and selected the is within the last days option, you could not change the default value of 1 displayed in the Days field.
- When you checked or unchecked a Threat Library checkbox, the page display flickered. We resolved this display issue.
- We updated the option names displayed when you click the Threat Library Export button. The dropdown now lists the options to Export to CSV and Export Selected to CSV if you have selected a subset of your object list or lists the option to Export to CSV if you have not selected a subset/selected all the objects in your current list.
- To improve performance, we updated ThreatQ to ensure that the application runs only one Solr delta at a time.

- In some situations, Dynamo logs caused an increased usage of memory and disk space. The increased memory usage sometimes triggered process restarts. To resolve this issue, we improved memory efficiency and shortened long logs.
- In some instances, a failed preflight check did not stop the upgrade process.
- The import abort command now requires that the threatquotient MariaDB user has Process and Connection Admin grants. This requires the upgrade process to prompt for the MariaDB root user password to apply those grants.
- We updated the upgrade migration process to resolve TLP/Source duplication.



ThreatQ Data Exchange (TQX)

The following is a bug fix for ThreatQ Data Exchange available when you upgrade from ThreatQ v5.18.0, or earlier, to 5.19.0.

NOTABLE BUG FIXES

- You could not rename publisher or subscriber nodes in the topology view.



ThreatQ TDR Orchestrator (TQO)

The following is a list of bug fixes for ThreatQ TDR Orchestrator available when you upgrade from ThreatQ v5.18.0, or earlier, to 5.19.0.

NOTABLE BUG FIXES

- When you clicked an existing action in the workflow builder page and selected a new action to replace it, TQO saved your change in the details pane but continued to display the original action name in the node view. In addition, the system returned an error when you attempted to run the workflow.
- Even though template values are optional, when you attempted to add an action without template values to a workflow, TQO returned the following error:
`The workflow or action information has been saved, but the definition could not be built due to the following errors: AttributeError: "list" object has not attribute "items"`

Security and System Updates

The following Security updates have been made:

- Remote CentOS Linux 7 host:

| UPDATED TO | CESA REF | |
|------------------------|---|--|
| Apache Tika 2.8.0.0 | CVE-2022-25169 CVE-2022-30126 | |
| Apache Zookeeper 3.8.1 | CVE-2022-42004 CVE-2022-42003 CVE-2023-26049 CVE-2023-26048 CVE-2022-2047 CVE-2023-26049 CVE-2023-26048 | CVE-2022-24823 CVE-2023-26049 CVE-2023-26048 CVE-2023-26049 CVE-2023-26048 CVE-2022-24823 |

Install Notes

- To upgrade from a 4x version to versions 5.6 through 5.18, you must be on the most recent 4x release. To upgrade to 5.19, you must first upgrade to release 5.13 or later.
- For the upgrade from the most recent 4x release to versions 5.6 through 5.18, you will need to enter your MariaDB root password during the upgrade process. To upgrade from 5.13 or later to 5.19, you may need to enter your MariaDB 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

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