



Release Notes

Version 5.29.1

Released Date: May 16, 2024


What's New in Version 5.29.1


The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.29.1. 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 or later require a minimum version of 5.13.0.

 Customers upgrading to ThreatQ v5.19.0 or later 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)			



ThreatQ Platform (TQ)

The following is a list of new features and bug fixes for the ThreatQ platform included when you upgrade from ThreatQ v5.29.0, or earlier, to 5.29.1.

NEW/UPDATED FEATURES

Integrations | Seeded TQO Actions

The following TQO actions are no longer seeded in new ThreatQ installations:

- GreyNoise Community
- IPInfo
- Shodan
- VirusTotal

Instead, these actions can be downloaded from the ThreatQ Marketplace. This change does not remove these actions from any existing ThreatQ instances.

NOTABLE BUG FIXES

- In some instances, scores remained pending recalculation until you ran an artisan command to score indicators.
- We updated the restore process to include data import properties. This change prevents unnecessary Solr full imports.
- When customers using SAML authentication attempted to parse a file for indicators, they experienced an intermittent error where the second page of the import process did not load due to a 500 error. This occurred when the customer's URL parameters from SAML authentication were not removed after a successful login. We updated ThreatQ to ensure these parameters are removed after login.
- We made the following updates to the handling of tag data ingested from the MISP Import CDF:
 - Updated the Save Tags As option to apply to indicators as well as events.
 - Added NCSC and TLP tags to the CDF's mapping.

ThreatQ Data Exchange (TQX)

The following is a new feature for the ThreatQ Data Exchange included when you upgrade from ThreatQ v5.29.0, or earlier, to 5.29.1.

NOTABLE BUG FIXES

- TAXII collection runs did not select the most recently modified STIX objects. As a result, if a run included more than 50K of a STIX object type, the TAXII collection run did not always include the most recently modified objects for the object type. We updated this process to pull up to 50K of the most recently modified STIX objects for each STIX object type. For example, if your data collection includes 250K objects, of which 75K are adversaries, 80K are campaigns, and the remainder are not STIX objects, the TAXII collection run will pull information on the most recently modified 50K adversaries and 50K campaigns.



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 or later, 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 or later, 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