Release Notes

Version 6.14.0

Released Date: November 10, 2025

What's New in Version 6.14.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.14.0. 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.

Migration Impact

> The migration process for ThreatQ 6.9.1 and later releases requires a ThreatQ 5.29.5 backup file. The migration process for releases prior to ThreatQ 6.9.1 requires a ThreatQ 5.29.4 backup file. If you attempt to use a backup file from a different ThreatQ 5x release, the restore process will return an error.

If you are deploying ThreatQ 6x for the first time, the upgrade requires setting up a new Ubuntu 22.04 LTS or Red Hat Enterprise Linux (RHEL) 8.10, 9.4, or 9.6 instance, installing ThreatQ 6x in this new instance, and then restoring the data from your ThreatQ 5x instance. The exact time to complete the upgrade depends on your specific environment and resources.

Access the ThreatQ Help Center to view or download the **ThreatQ Version 6 Installation** guides. Contact our Customer Support Team or your Technical Account Manager to request the **ThreatQ Version 6 Migration** guide for detailed information on migrating to ThreatQ 6x.

Upgrade Impact

If you are upgrading from one ThreatQ 6x version to another, see the How to Upgrade section for more information on executing a platform check and upgrade.

ThreatQ Platform (TQ)

The following is a list of new features and bug fixes for the ThreatQ platform.

NEW/UPDATED FEATURES

Audit Logging

ThreatQ now includes comprehensive audit logging that records detailed user, admin, and system actions across the ThreatQ Platform as well as ThreatQ Data Exchange (TQX), and ThreatQ TDR Orchestrator (TQO). This allows you to track activities such as logins/logouts and configuration updates, and to export these logs securely to your SIEM or Syslog Server. You can now monitor and review platform activity for compliance, security auditing, and operational visibility directly from ThreatQ or your connected logging system. See the Audit Log section of the Help Center for more information.

To begin exporting your audit log to your SIEM or Syslog Server, you must update the threatq.tfvars file with the following information: syslog hostname, syslog port, path to client certificate, and path to client private key

For hosted customers, ThreatQuotient will perform the required tfvars file update. On premise customers will use TQAdmin to update the tfvars file. See the TQAdmin Configuration section of the Help Center for more details.

End User License Agreement Update

The End User License Agreement (EULA) has been updated to reflect Securonix's acquisition of ThreatQuotient. This update requires the first user who logs in after the upgrade to review and accept the updated EULA on behalf of their organization.

NOTABLE BUG FIXES

- In ThreatQ 6x, the artisan command used to generate a list of OAuth2 clients by group returned an error. To resolve this issue, we updated the command to utilize the `--user_role` parameter instead of the `--user_group` parameter.
- When a CDF or TQO workflow contained unpopulated custom fields, Dynamo failed to complete its startup routine, which stopped all scheduled feeds and workflows from running automatically. We updated Dynamo to log the error and continue to process all valid items.
- An indicator's Score Summary listed only the attributes currently visible in the Attributes pane on the object details page. As such, it did not list attributes displayed due to pagination. We updated the Scoring Summary to include all attributes that contribute to the score.
- We resolved the following issues with CDF and TQO workflow runs:
  - When you ran a CDF or workflow manually, the manual run never finished.
  - When you scheduled a CDF or workflow run, the initial scheduled run did not start.

- In some instances, an indicator's score label, such as High, Very High, Low, etc, was listed as Undefined. We resolved this by updating the logic that retrieves indicator scores, so the correct label is displayed.

ThreatQ v6 Installation

- If you are migrating from ThreatQ v5 to ThreatQ v6, see the Migration Impact section.
- **Pinning your RHEL 9 release:**

  The following steps allow you to pin your current RHEL 9 release so that you cannot inadvertently upgrade your RHEL 9 environment to an unsupported release. See the **Red Hat Enterprise Linux 9 Support** section of the Help Center for more information on currently supported RHEL 9 versions.

  > Run the following commands as root or prefix them with sudo.

  1. Set release to minor version:
  2. subscription-manager release --set=**<release number>**
  3. Clean repositories:
  4. yum clean all
  5. Check which release is set locally:
  6. subscription-manager release --show
- **Pinning your Ubuntu release:**
  We recommend you update the release-upgrades file to disable manual Ubuntu upgrades so that you cannot inadvertently upgrade your Ubuntu 22.04 environment to an unsupported release.
  - Use a text editor, such as vi, to access `/etc/update-manager/release-upgrades`.
  - Change the `Prompt=` setting to `Prompt=never`.
  - Save your changes and exit the file.

How to Upgrade

> After you start the upgrade, do not cancel the installation. Doing so will leave your system in an unusable state.

Platform Check

ThreatQ 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

> Air gapped customers should reference the **Upgrading an Air Gapped ThreatQ Instance** section of the Help Center.

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, don't hesitate to get in touch with your Technical Account Manager.

As always, contact our Customer Support Team if you encounter problems when upgrading or need assistance.

Thank you,

The ThreatQuotient Team

tq-support@securonix.com
ts.securonix.com
703.574.9893