



Release Notes

Version 6.3.0

Released Date: September 18, 2024



What's New in Version 6.3.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.3.0. 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.

ThreatQ 4x End Of Life

ThreatQuotient provides support for the most current major version of ThreatQ and the immediately previous major version of ThreatQ only. With the general availability of ThreatQ 6x, support for ThreatQ 4x is drawing to a close as ThreatQ 6x becomes the current major version and ThreatQ 5x is its immediate predecessor.

As such, we recommend that any customer still on a ThreatQ 4x version upgrade as soon as possible. Contact [ThreatQuotient Support](#) if you have questions or need assistance with upgrading to a supported version.

Migration Impact

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) 9.4 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.

Contact our [Customer Support Team](#) or your Customer Success Engineer to request the ThreatQ Version 6 Installation and Migration guides for detailed information on installing and 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 Help Center

NEW/UPDATED FEATURE

ThreatQ Version Filter

With the release of ThreatQ version 6, a platform version filter has been added to the ThreatQ Help Center. This will allow you to filter topic contents to a specific major version of ThreatQ (v5 or v6). This filter will only affect the web view. You will still be able to open or download PDF files, such as release notes and install guides, using either view.

Your Help Center view defaults to ThreatQ 6x content. However, you can click the filter icon in the upper right navigation bar to change your view to ThreatQ 5x content.

In addition, a version pill in the upper left corner of each page displays TQv6 or TQv5 to reflect the version you selected.



ThreatQ Platform (TQ)

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

NEW/UPDATED FEATURES


ThreatQ | Architecture Update


ThreatQ's new, fully containerized service architecture deployed as a Kubernetes application is now available for deployment to ThreatQuotient on-premise and self-hosted customers who plan to deploy ThreatQ 6x in Ubuntu 22.04 LTS or Red Hat Enterprise Linux (RHEL) 9.4 with the latest, stable RKE2 version as the Kubernetes application.

System and User Timezone Display Options

ThreatQ now supports system and user-level configuration of the timezone displayed in the ThreatQ user interface. Upon upgrade to ThreatQ 6x, the system-level timezone display defaults to Greenwich Mean Time (GMT) which reflects the Coordinated Universal Time (UTC) time standard. You can use the General tab in the System Configurations page to select a different system display timezone. The system-level timezone applies to each user unless you use the Edit User page to select a different timezone for the user.

The system and user-level timezone settings only affect the display of timestamps in the user interface and PDFs. ThreatQ continues to store timestamps in UTC and share UTC timestamps with resources such as ThreatQ Data Exchange (TQX), ThreatQ TDR Orchestrator (TQO), exports, and TAXII.

 Customers who currently use a system timezone other than UTC, must contact ThreatQ Support or Customer Success to request a patch to update all date fields to UTC before upgrading to ThreatQ v6.3.0. You can run the `ti medatectl` command to verify your current ThreatQ timezone standard.

 After upgrading to ThreatQ v6.3.0, review new custom object definition/JSON files before installing to verify that the custom object does not use `datetime(3)`. These objects should instead use `timestamp(3)`.

User Management

The Edit User page has been reorganized to group display settings and account maintenance settings together. These changes also reduce the amount of vertical scrolling required to view/update user settings.

Resource Limit Management

With the architecture changes in ThreatQ 6x, MariaDB resides in a Kubernetes pod and resource limits are managed by Kubernetes based on deployment size.

Proxy Settings

ThreatQ proxy configuration entered in the user interface is now stored as a Kubernetes secret.

SSL Client Certificate Authentication | Configuration Updates

Upon upgrade to ThreatQ 6x, the ability to enable/disable SSL Client Certificate Authentication and add a CA Certificate moves from the CAC/PIV SSL tab in the User Management page to the TQAdmin tool. The CAC/PIV SSL tab in the User Management page only displays the current enabled or disabled status.

In addition, the LDAP and SAML tabs in the User Management page now display a warning message indicating that SSL Client Certificate Authentication/CAC must be disabled before you can enable LDAP/SAML. The Disabled/Enabled toggles in these tabs cannot be set to Enabled until you disable SSL Client Certificate Authentication.

TQAdmin Tool Enhancements

We added the following new functionality to the TQAdmin tool:

- Support for the installation of ThreatQ 6x.
- The ability to display user credentials for the Admin user.
- The ability to configure your ThreatQ installation by enabling OpenDXL, TAXII, and SSL Client Certificate Authentication as well as adding an SSL certificate.



Since TQAdmin allows you to enable SSL Client Certificate Authentication and add your CA certificate, the CAC/PIV SSL tab in the User Management page only displays the current enabled or disabled status.



Restore Process | Instance ID

When you upgrade to ThreatQ 6x by restoring a ThreatQ 5x backup, the restore process pulls the instance ID from the backup file instead of using any instance ID value found in the 6x instance. This change allows ThreatQ 6x to use Kubernetes to manage the instance ID.

Server Administration | Removed

The Server Administration option is no longer applicable with the new ThreatQ architecture and has been removed from the Settings menu.

Artisan Commands

Due to the architecture changes in ThreatQ 6x, the commands to run artisan commands have changed. Artisan commands are now run in the api-schedule-run pod.

Artisan Commands | Minimum Version for Restores

The artisan command for restores now supports the use of the migration flag which calls the migrate artisan command. When you include the migration flag, the command requires a ThreatQ v5.29.4 backup file. If you attempt to restore a backup file from a different version, ThreatQ returns an error.

Deprecated Artisan Commands

In conjunction with a review of artisan commands in ThreatQ 6x, we have deprecated the following unneeded commands: adversary description cleanup, list queues, indicator scoring, and troubleshooting package.

Integrations | Custom Connectors

In ThreatQ 6x, the file system within the custom connector container is independent from the file system of the host operating system. The directories writable within the container are persistent across instances of the custom connector container so that restarts of the custom connector container do not destroy the custom connector installation.



Important Note: Existing custom connectors (that were installed on your 5x instance) are not included in the migration process due to these changes. See the Installing Custom Connectors in ThreatQ v6 section of the Help Center for more information. Contact

Integrations | Support for JSON Web Tokens

ThreatQ now supports signing and verifying JSON Web Tokens (JWTs) from YAML-based integrations.

Maintenance Mode Notification

When you log into a ThreatQ instance that is in maintenance mode, ThreatQ displays a maintenance notification that includes the following message: ThreatQ is down for maintenance.

Object Detail | Descriptions Source Display

The Descriptions pane now truncates description source names that are over thirty characters long. You can view the full source name by hovering on the truncated version.

Object Detail | Internal Description Options

Object descriptions with internal sources no longer display the Protect from feed updates option. This option is not needed for internal descriptions since they do not come from feeds and cannot be updated by feeds.

Create Button | New Menu Layout

We updated the Create menu to support the future addition of STIX objects. The Import options are now located on the left side of the menu instead of the bottom.

Threat Library | Object Description Edit View

The Add Description and Edit Description windows now include an expand view option in the upper right corner. Click this option to access a full page view which reduces the need for scrolling when adding or updating a description. Click the minimize view option to return to the original window size.



Integration | No Proxy Setting

We introduced a `NO_PROXY` environment setting for customers who use a proxy and need a custom connector to bypass the proxy. The Proxy tab in the System Configurations page includes the following new field that allows you to add/update your proxy bypass: Bypass Proxy Setting for these Hosts and Domains

AGDS | Export and Import Directories

Upon upgrade to ThreatQ 6x, the `/var/lib/threatq/agds_transfer` directory is created and becomes the default location for exporting and importing AGDS zip files. As such, AGDS commands only need to specify the relative path to the folders you created within this directory for AGDS exports or imports. Then, use the `--target` parameter to specify the location when exporting the AGDS zip file and the `--file` parameter to specify the location from which to import the .gz file.

Usability Enhancements

To increase consistency and improve usability, we made the following display changes:

- Reduced the size of text inputs and select boxes/dropdowns.
- Changed the helper text displayed in the My Integrations page from Start typing to Search installed integrations.
- In the Bulk Change page:
 - Increased field padding
 - Indented and darkened the font color of the No results found message displayed when your search criteria do not match an existing value.

SAML Authentication | Remove SessionIndex Requirement

We updated the SAML Login process to support credentials services that do not provide a sessionindex during authentication. As such, sessionindex is no longer required during SAML authentication.

Threat Library | Date Filters

We added is, is not, and is greater than filter options to the Date Created, Published Date, Source Ingest Time, Last Modified, and Due Date filters.



The Generate PDF window now gives you the option to include/exclude the system object overview section.

In addition, when you generate a PDF that includes only the system object's description(s), the Description section header text is omitted as is the last modified date and divider line. If the PDF export includes only a single description, the description source is also omitted.

Object Details | Descriptions Pane Display

We updated the background and button colors in the Descriptions pane to support ThreatQ UI standards.

NOTABLE BUG FIXES

- When ThreatQ parsed indicators with the Normalize URL Indicators option disabled, incorrect strings were parsed as FQDNs.
- The Events Heatmap dashboard widget did not calculate adversary relationship counts correctly. We updated the widget so that Adversary counts displayed equal the number of sightings in the Threat Library when the appropriate filters are applied.
- Feed activity logs displayed incorrect timestamps due to ThreatQ incorrectly parsing the activity log's UTC datetime as the user's local timezone.
- When you configured an indicator's scoring algorithm to include a wildcard (*) attribute value, the Score Summary available from the object details page or preview panel did not display the Attributes option.
- The Save Tags As configuration option for the MISP Import CDF was not applied to indicator objects. We resolved this issue so that ThreatQ ingests MISP attribute tags as tags or attributes based on the Save Tags As option specified.
- In the Indicator Analytics dashboard, the Attribute pie chart widget did not accurately show the top 10 attributes. We resolved this issue so that the pie chart displays the top 10 attributes.



If there are multiple attributes with the same number of indicators, the pie chart key and the table below the pie chart may list attributes in a different order since the key and table use different sorting methods.

- PDFs generated by ThreatQ did not display Spanish language special characters correctly.
- In some instances, scores remained pending recalculation until you ran an artisan command to score indicators.
- When you accessed the Scoring page for a ThreatQ instance with a large number of adversary objects, the page loaded slowly because it referenced object descriptions. We resolved this issue by removing the description field reference.
- We updated the restore process to restart the operations manager to ensure that restored operations are installed.

- We changed the operations install process to support the installation of operations whose file names contain special characters.
- We modified the ACE operation to handle system objects with multiple descriptions.
- When an operation failed, ThreatQ did not display traceback or error messages. We updated operation error handling to log errors and display them in the ThreatQ UI.
- When you filtered the Threat Library by author, ThreatQ only allowed you to select authors with an ID lower than 100. We resolved this issue so that you can select from the full list of authors.
- Keyword searches in the Files Analytics dashboard did not filter the results displayed.
- After you configured SAML, ThreatQ returned an error upon initial SSO login. However, ThreatQ did not return an error for subsequent logins.
- If you clicked the Test Connection button in the Authenticated Bind LDAP Settings tab before you enabled LDAP and saved your settings, ThreatQ returned an error.
- The `/api /reports/events/adversary-spearphi sh-monthly` endpoint did not filter data by event date.
- When you ingested indicators through a feed or the indicator parser with the Parse FQDN option enabled, ThreatQ parsed incorrect strings as FQDNs. We resolved this issue by updating FQDN parsing and validation to exclude some special characters and apply the correct structure, `<domain>.<valid tld>`.
- When you performed an air gapped data sync (AGDS), the import process only populated indicator objects in the target instance; no other object types were included.
- Upon upgrading to ThreatQ v5.27.0, a customer could not ingest data from a TAXII v1.0 feed due to a Dynamo error.
- When you downloaded a file from an object's details page, ThreatQ displayed the Overview Dashboard after the file download. We updated the download process to return to the original details page after the file download.
- We updated the Description pane in the object detail to suppress the display of the Edit option for objects without descriptions.
- We modified the display of the Descriptions section in PDF exports of object details to make the PDF display more consistent with the display of the Descriptions pane in ThreatQ.
- The time field in the Run Frequency section of the integration configuration page displayed two borders. We removed the inner border to ensure consistency with ThreatQ standards.
- When the first description you added to an object was lengthy, the Show More option, which expands the description display, was not displayed after you saved the description.
- When you ran the merge source artisan command, it did not update object description sources correctly. We updated this command to ensure that object description sources as well as the primary description indicator are updated correctly.
- Operations installed via a dependency archive were improperly attempting to install dependencies from the Internet.
- ThreatQ allowed you to manually add an object description without a description source. We updated the Add Description window to return the following error message if you attempt to save a description without a source or if you enter a description source name longer than 255 characters: Error adding description
- A custom script for merging attributes returned an HTTP_CODE: 000 error due to a request timeout. This occurred when you attempted to merge a very large set of attributes. We

resolved this issue by modifying the script to apply the merge process to groups of 10,000 objects.

- After you used the Owned By Me tab in the Load Data Collection window to locate a data collection, you were unable to check the checkbox next to any of the data collections in your search results. This prevented you from deleting data collections in your search results.
- The User Management page took longer than expected to load as ThreatQ checked the following data for each user:
 - Point of Contact Assignments - System objects to which a user was assigned a point of contact.
 - Ownership Status - Dashboards, investigations, data collections, TOX feeds, and tasks to which a user was assigned ownership.

We improved query performance and updated them to run only when necessary.

- When you entered an attribute name and value in the Bulk Changes page and then selected an attribute source, your previously entered attribute name and value information was removed.
- Source, Tag, and Attribute fields displayed in the Update sections of the Job Management page displayed more than fifty characters and were truncated. We updated the display of this information to display up to fifty characters and include an appended ellipsis to indicate you can hover to view the full text.
- Since you cannot restore an online backup in a ThreatQ 6x instance, we removed the option to generate an online backup. In addition, ThreatQ returns the following error message if you attempt to restore a ThreatQ 5x online backup in a ThreatQ 6x instance: Online backups are not supported in this version. Try again using an offline backup.



ThreatQ Investigations (TQI)

The following is a list of bug fixes for ThreatQ Investigations.

NOTABLE BUG FIXES

- When you clicked the preview option for an object's related object, the preview panel did not display the down arrow on the manage columns button.
- When you clicked a node on an evidence board, the Relationships section of the action panel displayed the attribute name but did not display the attribute value.



ThreatQ TDR Orchestrator (TQO)

The following is a new feature and a list of bug fixes for ThreatQ Orchestrator.

NEW/UPDATED FEATURE

Orchestrator Page | Updated Delete Options

The Orchestrator page now includes a Remove column that lists a delete icon for each workflow. This replaces the previous method for deleting a workflow where you checked the checkbox to the left of the workflow name and clicked the delete icon in the top right corner of the page.

NOTABLE BUG FIXES

- When you clicked the Select a data collection field in the workflow builder page, the dropdown list was embedded in the field instead of displaying on top of the field.
- We updated the workflow node view to automatically resize each action's icon.
- When you executed a manual workflow run of a TQO bulk changes action from the Threat Library or an object's details page, the workflow was applied to all objects in the data collection instead of to the selected object(s). We updated the manual workflow process for TQO bulk changes actions to apply to selected objects only.

ThreatQ Data Exchange (TQX)

The following is a bug fix for ThreatQ Data Exchange.

NOTABLE BUG FIX

- When you attempted to send a query for multiple types of objects to the TAXII server, you received an Internal Server error. We resolved this issue so that you can send a query for multiple object types using comma-delimited parameters.



Security and System Updates

The following Security and System updates have been made:

- Updated ThreatQ deployments to generate unique Illuminate encryption keys.
- Moved the API container to an Alpine Linux base image that does not include ImageMagick. This addresses multiple security vulnerabilities associated with ImageMagick.
- Updated to Apache Tika 2.9.2.1.
- Modified the user image upload endpoint to prevent remote code execution (RCE).
- Updated the ws package in the frontend and websocket-server repositories to 8.17.1.
- Modified the Falco Rules update process to allow more frequent updates to security monitoring rules for hosted customers.
- Enabled the Web Application Firewall for hosted customers.
- To support Security Technical Implementation Guide (STIG) installs of ThreatQ 6x, updated installer to add the executables embedded in the terraform provider directories to the trusted executables database for the file access policy daemon (fapolicyd).

ThreatQ v6 Installation

- The installation process for ThreatQ 6.3.0 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.
- Contact our Customer Support Team or your Customer Success Engineer to request the ThreatQ Version 6 Installation and Migration guides for detailed information on installing and migrating to ThreatQ 6x.

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

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 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