



Release Notes

Version 6.21.0

Release Date: September 30, 2026

What's New in Version 6.21.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.21.0. Below is a list of enhancements, important bugs that have been addressed, and upgrade instructions.

ThreatQ Platform

The following is a list of new features and bug fixes for the ThreatQ platform included when you upgrade to 6.21.0.

NEW/UPDATED FEATURES

Scoring Enhancements | Adversaries & Vulnerabilities

ThreatQ Scoring now supports Adversary and Vulnerability objects. Score information for these object types is available on object details pages, in the Threat Library Managed Score column, score summaries, quick filters, and the dashboard score overview. Users can also review and update Adversary and Vulnerability scores from the object details page and create scoring algorithms from the Attributes tab on the Scoring Sensitivity Configuration page.

See the [Manually Setting an Object's Score](#) and [Scoring Algorithms](#) topics for more details.



Vulnerability and Adversary score values cannot be exported or used as Special Parameters to filter data from the Exports wizard. These issues will be addressed in a future ThreatQ platform release.

Threat Research Agent | LiteLLM Model Support

LiteLLM is now supported as an LLM provider for the Threat Research Agent. Customers can select LiteLLM as their provider and specify the applicable LLM host address on the Agentic Assistance Configuration page in ThreatQ.

TQAdmin | Enable Threat Research Agent MCP & Agent Services

TQAdmin now includes a prompt for enabling the MCP and Agent services required by the Threat Research Agent. Administrators of on-prem instances can enable these services directly through TQAdmin, eliminating the need to manually update the `threatq.tfvars` file.

Air-Gapped Data Sync Enhancements

Air-Gapped Data Sync (AGDS) has been upgraded to use ThreatQ UUIDs for consistently identifying and updating objects across ThreatQ environments. AGDS can now apply changes from the external, source ThreatQ instance to previously synchronized objects in the internal, downstream instance.

The enhanced synchronization process supports:

- Updating object names and descriptions.
- Removing relationships, attributes, tags, and sources that were removed from the source instance.
- Replacing updated attribute values instead of creating duplicate values.
- Treating the source ThreatQ instance as authoritative when resolving synchronization conflicts.

These enhancements use the existing scheduled, file-based export and import process. Real-time synchronization and inbound connectivity across the air gap are not supported.

Attribute Management Enhancements

Improved the performance, reliability, and accuracy of Attribute Management, particularly in environments with large attribute datasets. Updates include optimized queries and more efficient handling of large responses to reduce processing time and prevent memory-related errors.

This release also resolves issues affecting attribute searches and merge operations, including:

- Attribute values can now be merged when they appear on different result pages.
- Resolved an issue that could cause the merge screen to carry over values from a previously selected attribute, so each merge now uses only the values for the current attribute.
- Attribute searches return the correct results when filtered by source.
- The Indicator attribute values API returns existing values as expected.

Threat Library | Filter-Aware Type Selection

The searchable type-selection menus in the Threat Library have been updated so that bulk-selection actions respect the active search:

- In the **Type** quick filter and the filter set builder's **Add Type** menu, **Select All** now selects only the types matching the current search.

- **Clear** removes only the types included in the filtered results.
- Selection indicators and object counts update to reflect the filtered selection.
- When no search is entered, **Select All** and **Clear** continue to apply to all available types.

NOTABLE BUG FIXES

The following list of issues and bugs that have been resolved with ThreatQ v6.21.0.

- **Description Image Resizing** - Resolved an issue where resizing images within object Description fields could distort the images by altering their original aspect ratio. Images now resize proportionally, preserving their visual quality and readability.
- **Notification Center Display** - Resolved an issue where the unread notification indicator could overlap notification text in the Notification Center. The indicator is now properly aligned and spaced, ensuring notification content remains fully visible and readable.
- **Source Values in Exported Reports** - Resolved an issue introduced in ThreatQ 6.19.1 where source values could be omitted from exported reports even though the source count was displayed correctly. Exported reports now include the applicable source values, regardless of whether TLP filtering is enabled or disabled.
- **Signature Source Code Editing** - Resolved an issue introduced in ThreatQ 6.19.0 where the Edit option for Signature source code was unavailable to authorized users. Signature source code can now be edited and saved according to the user's assigned permissions.
- **ThreatQ Data Exchange Object Replication** - Resolved an issue where Reports, Events, and Custom Objects with an assigned Point of Contact could fail to replicate from a Publisher to a subscribed ThreatQ instance. Affected objects now replicate successfully, with the Point of Contact left unassigned when it cannot be resolved on the Subscriber.
- **MISP Import Processing** - Improved MISP Import processing to prevent malformed signature attributes from interrupting an import. Invalid attributes are now skipped, allowing the integration to continue processing valid MISP data without generating repeated error notifications.
- **Bulk Operations** - Resolved an issue where bulk operations could fail for certain ThreatQ object types and display a Bulk Job failed to complete notification. Bulk operations now process successfully across supported object types.
- **Bulk Relationship Limits** - Resolved an issue where the Bulk Changes interface allowed users to submit relationship updates that exceeded the configured object limit. The Relationships field is now disabled when the limit is exceeded, and a

message displays the applicable limit. Bulk relationship changes remain available for selections below the configured threshold.

- **Dashboard Widgets Data Refresh** - Resolved an issue affecting ThreatQ versions 6.20.0 and 6.20.1 where dashboard widgets would display outdated data instead of the latest objects available in the associated data collection. Dashboard widgets now remain synchronized with Threat Library data without requiring users to re-save or recreate the widget.
- **Resolved RKE2 Ingress Controller Port Conflicts** - Fixed an issue that could prevent ThreatQ from installing successfully in environments when the RKE2 1.36 ingress controller occupied ports 80 and 443. TQAdmin now disables the new traefik ingress controller as well as the previous nginx ingress controller during installation to ensure these ports remain available for ThreatQ services.
- **Resolved Exporter Object Type Selection** - Fixed an issue that could prevent users from selecting or saving certain exporter object types and cause associated fields to be missing from the Exporter Fields menu. Exporter object types and their corresponding fields now load and save correctly.
- **Restored Campaign Additional Dates Editing** - Fixed an issue affecting ThreatQ versions 6.16.0 through 6.20.1 that prevented users from editing Additional Dates after creating a Campaign. Users with the appropriate write permissions can now add or modify Additional Dates on existing Campaign objects.
- **Removed Excess Blank Space from Object Details Pages** - Fixed an issue introduced in ThreatQ 6.20.0 that displayed excessive blank space below the Audit Log on object details pages. Users can now reach the end of the page without unnecessary scrolling, while context-menu navigation continues to work as expected.
- **Restored Show More for Long Descriptions** - Fixed an intermittent issue where the Show More option did not appear for long descriptions containing externally hosted images. Long descriptions can now be expanded and collapsed without requiring users to enter and cancel edit mode.
- **Improved Relationship Data Synchronization** - Improved relationship processing to prevent object relationship data from becoming out of sync across the Threat Library, relationship-based searches, and exports following an interruption in background processing.
- **Resolved Air-Gapped Upgrade Package Image Mismatch** - Fixed an issue affecting air-gapped upgrades from ThreatQ 6.19.1 to 6.20.0 where the offline package did not include the required container registry image, causing the upgrade to fail. The updated package now includes the correct registry image and no longer attempts to retrieve it from an external source.
- **Restored Signature Source Code Editing** - Fixed a permissions issue introduced in ThreatQ 6.19.0 that prevented authorized users from editing Signature source

code. Users with the appropriate permissions can now edit and save source code, while read-only access remains unchanged.

NEW KNOWN ISSUES

The following new issue has been reported with ThreatQ v6.21.0:

- **Adversary and Vulnerability Scores Not Included in Exports** - Adversary and Vulnerability scores are not currently included in data exports. In addition, users cannot use these scores as filters in the Special Parameters field of the Export Wizard. This issue will be addressed in a future ThreatQ platform release.
- **Object Relationship Creation** - In certain instances, creating an object with a relationship may return an HTTP 500 error when the related object is identified only by its object ID. In this scenario, the primary object is created successfully while the associated relationship is not.

Security and System Updates

The following updates have been made with ThreatQ v6.21.0:

- **Enhanced Database Credential Protection** - Strengthened the handling of database credentials used by Solr. This update improves runtime credential protection and safeguards sensitive information from unintended exposure.
- **Strengthened Directory Permissions** - Strengthened file-system permissions for persistent storage directories in on-premises ThreatQ deployments. Fresh installations and upgrades now apply appropriately restricted access controls to these directories.
- **Strengthened Persistent Storage Permissions** - Strengthened access controls for persistent storage directories in on-premises ThreatQ deployments. Fresh installations and upgrades now apply appropriately restricted permissions to enhance platform security and support compliance requirements.
- **Air-Gapped Upgrade Package** - Updated the container registry component included with air-gapped ThreatQ deployment packages to ensure compatibility with the platform configuration. This update enables offline upgrades to complete successfully without requiring access to external image repositories.
- **Enhanced SAML SSO Security** - Improved the SAML SSO authentication flow to strengthen the protection of sensitive authentication data while maintaining the existing login experience.
- **Enhanced Authentication Token Security** - Improved authentication token handling and session management to strengthen the protection of sensitive authentication data across authenticated ThreatQ requests.



- **Enhanced User Information Display Security** - Improved how usernames and titles are rendered in Investigations to prevent unsafe content from being processed while preserving the correct display of legitimate values.
- **Updated Third-Party Components** - Updated RKE2 to version 1.35.7, containerd to version 2.2.6, Apache Tika to version 3.3.1, and Log4j to version 2.26.0 to incorporate current security fixes.



Upgrading

Perform the following steps to upgrade your ThreatQ v6 instance.

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

1. Perform a platform check to ensure adequate disk space and that your installed integrations are compatible with the new ThreatQ version. You will be unable to proceed with the upgrade until clearing this check. It is important to note that the command does not apply to integrations installed on third-party systems such as the ThreatQ App for QRadar.

Platform Check Against the Most Recent ThreatQ Version

```
# sudo /usr/local/bin/tqadmin platform check
```

Platform Check Against a Specific ThreatQ Version

```
# sudo /usr/local/bin/tqadmin platform check -v 6.21.0
```

2. Run the upgrade command:

Upgrade to the Latest ThreatQ Version

```
# sudo /usr/local/bin/tqadmin platform upgrade
```

Upgrade to a Specific ThreatQ Version

```
# sudo /usr/local/bin/tqadmin platform upgrade -v 6.21.0
```

New Installations

If you are installing ThreatQ version 6 for the first time, it is highly recommended that you review the ThreatQ 6x Installation section and guides before proceeding with installation. The guide provides useful information including:

- Required Firewall Ports
- Suggested Partitioning Scheme
- System Requirements (Hardware Specifications, Core CPUs, RAM etc.)
- Steps to pin your RHEL 9 and Ubuntu versions to prevent upgrades to unsupported environments
- Security Hardening Guides

Migrating ThreatQ v5 to v6

It is important that you use the correct ThreatQ version when migrating a ThreatQ v5 instance to ThreatQ v6.

- Migrating to **ThreatQ v6.9.1 or greater** requires a **ThreatQ v5.29.5** backup file.
- Migrating to **ThreatQ v6.9.0** and prior requires a **ThreatQ v5.29.4** backup file.

 Using a backup other than the ones listed above will result in a restore error.

Contact ThreatQ Support or your Technical Account Manager for additional information and to obtain the ThreatQ Migration Guide. The ThreatQuotient team highly recommends that you review the ThreatQ 6x Installation guide when planning your migration.



Support

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