

Release Notes

Version 6.22.0

Release Date: November 09, 2026

What's New in Version 6.22.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.22.0. 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 6.22.0.

NEW/UPDATED FEATURES

Threat Research Agent | Feature Updates

The following updates have been made to the Threat Research Agent:

- **TQO Workflow Support** - ThreatQ Orchestrator (TQO) workflows are now available as tools for the Threat Research Agent. Once a TQO workflow is configured and enabled for MCP server access on its configuration page, users can ask the Agent to run it against a single existing ThreatQ object. Results are returned directly in the chat, while the run is recorded in the Orchestrator Activity Log and its outputs continue to be ingested into ThreatQ.
- **Additional Model Support** - Support for the following model providers has been added for the Threat Research Agent:
  - **LM Studio**
  - **vLLM**
- **Custom Host URL Support** - The Threat Research Agent now supports custom host URLs for OpenAI, Anthropic, and Gemini providers, enabling connections to regional or compatible endpoints. LiteLLM configurations now distinguish between direct provider connections and LiteLLM proxy mode, so adding a custom URL does not automatically enable proxy mode.
- **AI Token Usage** - Added an **AI Token Usage** section to the AI Settings page, where users with Administrator or Maintenance permissions can review per-user token consumption and request statistics for the last 24 hours, 7 days, or 30 days. Usage is recorded in hourly UTC windows and associated with the authenticated user, so signing in again or restarting an agent no longer resets recorded usage.

Integrations Management | Page Redesign

The Integrations Management page has been redesigned to improve the user experience and is now organized into three tabs:

- **Intelligence Feeds & Connectors**
- **Feed Run Activity**
- **Operations & Actions**

The **Intelligence Feeds & Connectors** tab displays CDFs, custom connectors, and TQO advanced workflows in a table. The table includes integration names and versions, last and next run times, run rescheduling options, highly relational flags, and the results of the five most recent runs. Users can filter integrations by name, schedule status, errors, and highly relational status. They can also download, clone, or uninstall integrations from this tab.

The **Feed Run Activity** tab lists feed runs and provides filters for feed name, date range (from the last 24 hours to the last 90 days), and run status.

The **Operations & Actions** tab retains the card-based layout. Select an integration card to review its configuration options.

Integrations | Configuration Updates

The following new features have been added for installed integrations:

- **Reset Schedule Option** - You can now reset the schedule for a disabled CDF or TQO advanced workflow by clearing its last-import timestamp from the integration's details page. This helps prevent a long backlog of missed time windows when restarting a feed that has been disabled for an extended period.

  
  Resetting does not enable the feed; you can re-enable it when you're ready.

- **Clone Integration** - You can clone a feed with the cloned feeds receiving a new name and namespace.
- **Download Integration** - You can also download an installed feed.
- **Pipeline De-Duplication** - You can retain existing de-duplication behavior for CDFs and TQO workflows. When disabled, all objects are forwarded to ThreatQ, allowing re-ingested indicators to refresh Last Seen and work with Indicator Expiration policies.

Attribute Value Merge Improvements

Attribute value merges now run as background jobs, improving performance for large merge operations. After submitting a merge, you can track its status and receive a completion notification when processing and search indexing are finished.

NOTABLE BUG FIXES

The following list of issues and bugs that have been resolved with ThreatQ v6.22.0.

- **Bulk Delete Search Flagged Filter** – fixed an issue where the Job Management page did not display the Is Flagged filter in the Search Criteria for Bulk Delete jobs created using the Flagged filter in the Threat Library.
- **ACE Parser Hashes** – fixed an issue where the ACE Parser could ingest hash-like values from image URLs as MD5 indicators when parsing reports. The parser now ignores hash matches found within URLs while continuing to extract hashes from report content.
- **Improved Indicator Query Performance for Data Collections** – fixed an issue that could cause indicator queries and related orchestrations to time out when a Data Collection contained many source-name filters. Query processing is now more efficient with larger filter sets.
- **Bulk Update Jobs Now Report Completion Status Correctly** – fixed an issue that could leave a Bulk Update job in "In Queue" after its changes had already been applied. The job status now updates to "Completed" without the prolonged delay.
- **MCP Query Result Limit** – fixed an issue where the Threat Research Agent's MCP query tool could return fewer results than requested when the limit exceeded 25.
- **SSO Login Error on Initial Attempt** – fixed an issue where stale idle-timeout state could cause an SSO login to fail on the first attempt. Users can now sign in successfully without retrying.
- **SAML SSO Login for Existing Users** – fixed an issue that could prevent existing non-Maintenance users from signing in through SAML SSO. Eligible users with previously deleted accounts can now authenticate with the correct role restored. Maintenance accounts remain restricted from SSO.
- **TQI Investigation Workbench Search Results** – fixed an issue that could cause searches for certain objects to remain in a loading state even when results were returned. Search results now display correctly.
- **Extra Space at the Bottom of Pages** – fixed an issue that caused blank space at the bottom of some pages. Page sizing and scrolling now work as expected across short and long pages.

Security and System Updates

The following updates have been made with ThreatQ v6.22.0:

- **OAuth2 Client Credentials** – Older customer-created OAuth2 clients with lowercase-only client IDs will receive new, more secure client IDs and secrets during the upgrade. ***Applications and integrations that use these clients must be updated with the new credentials to continue authenticating with ThreatQ.*** ThreatQ's built-in system clients are not affected.
- **Improved Bulk Ingestion Performance** – ThreatQ now processes large, relationship-heavy data ingests more efficiently across feeds, connectors, TQX/TAXII, and bulk API inserts.

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 6.22.0
   ```

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 6.22.0
   ```

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

Don't hesitate to get in touch with your Technical Account Manager to discuss planning your upgrade.

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