Release Notes

Version 6.20.1

Released Date: August 12, 2026

What's New in Version 6.20.1

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.20.1. Below is a list of enhancements, important bugs that have been addressed, and upgrade instructions.

> ⚠ Upgrading to ThreatQ 6.20.1 may take longer than a typical release upgrade due to database index operations performed during the upgrade. The overall duration depends on the size of your indicators table and may be significantly longer for environments upgrading from versions earlier than 6.20.0. Contact ThreatQ Support if you have questions or concerns about your upgrade.

ThreatQ Platform

The following is a list of new features and bug fixes for the ThreatQ platform included when you upgrade to 6.20.1.

NEW/UPDATED FEATURES

Audit Log Export Command

ThreatQ now includes an **Audit Log Export** command that enables administrators to export audit logs from the command line to a consolidated **CSV** or **JSON** file. The command supports exporting all audit logs or filtering by object type, audit table, or date range, making it easier to archive audit data, meet compliance requirements, and integrate with external reporting or retention workflows.

Designed for enterprise environments, the command supports scheduled execution using tools such as **cron**, automatically includes custom object types, and is optimized to efficiently process large audit datasets with minimal impact on normal ThreatQ operations.

NOTABLE BUG FIXES

The following list of issues and bugs that have been resolved with ThreatQ v6.20.1.

- **Improved IPv6 Upgrade Performance** - Resolved an issue introduced in ThreatQ v6.20.0 that could significantly increase upgrade times for environments with large Indicator datasets when applying the IPv6 CIDR support database migration. The migration has been optimized to complete more efficiently at scale, reducing upgrade duration and minimizing maintenance windows for large ThreatQ deployments. This update preserves all IPv6 CIDR functionality introduced in v6.20.0 while improving the overall upgrade experience.

Security and System Updates

The following updates have been made with ThreatQ v6.20.1:

- **Improved SAML Authentication Token Handling** - Enhanced the security of the SAML authentication process by improving how temporary authentication tokens are handled during sign-in. These changes reduce the exposure of authentication data during the login process while maintaining a seamless user experience.
- **Strengthened SAML Session Validation** - Improved SAML authentication security by strengthening validation of temporary authentication tokens during the sign-in process. This enhancement ensures authentication tokens are handled more securely throughout the authentication lifecycle and further protects user sessions.

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 6.20.1
   ```

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 6.20.1
   ```

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