

ThreatQuotient



ThreatQ Version 5 Installation Guide

Version 1.0.9

September 11, 2024

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

Warning and Disclaimer	3
ThreatQ Installation Options	4
ThreatQ as a Virtual Instance	4
ThreatQ on Your Own Device.....	4
Hosting Services	4
Air Gapped Environments	4
ThreatQ System Requirements	5
Virtual and BYOD System Requirements.....	5
Minimum Screen Resolution	5
ThreatQ as a Virtual Instance (OVA).....	6
Virtual Prerequisites.....	6
Installing ThreatQ as a Virtual Instance	6
ThreatQ on Your Own Device (BYOD)	8
BYOD Prerequisites.....	8
Amazon Web Services (AWS) Guidelines.....	8
BYOD Partitioning.....	8
BYOD Pre-installation	9
Downloading and Running TQAdmin	11
Downloading TQAdmin	11
Using TQAdmin to Install ThreatQ.....	11
Logging In for the First Time	12
What to Do Next	14
Configuring Network Connectivity.....	15
Converting to a Static IP Address	15
Checking Connectivity to ThreatQ Servers.....	18
Setting Up Your Proxy Server	18
Hosting Services.....	20
FIPS 140-2 Compliance	22
ThreatQ FIPS 140-2 Compliance	22
Modes of Operation	22
TLS	23
Enabling FIPS Mode	23
Change Log	24

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Copyright © 2024 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

ThreatQ Installation Options

Based on your business needs, you can install ThreatQ as a virtual instance (OVA) or on your own device (BYOD). Virtual installs involve downloading the ThreatQ OVA on your Hypervisor. Bring Your Own Device (BYOD) installs leverage the TQAdmin tool.

In addition, ThreatQuotient also provides hosting services and support for air-gapped instances.

ThreatQ as a Virtual Instance

1. Review and verify compliance with the [ThreatQ system requirements](#) as well as the [virtual machine prerequisites](#).
2. [Install ThreatQ as a virtual instance](#).
3. [Log into ThreatQ for the first time](#).
4. [Configure network connectivity](#).
5. [Download TQAdmin](#) for future use in upgrading ThreatQ.

ThreatQ on Your Own Device

1. Review and verify compliance with the [ThreatQ system requirements](#) as well as the [BYOD prerequisites](#) and [Amazon Web Services guidelines](#) (if applicable).
2. [Configure network connectivity](#).
3. [Prepare your device for installation](#).
4. [Download and run TQAdmin](#).
5. [Log into ThreatQ for the first time](#).

Hosting Services

ThreatQuotient offers [hosting services](#) for your ThreatQ applications.

Air Gapped Environments

ThreatQuotient provides installation steps for Air Gapped environments - which differ slightly from the standard installation steps for non-air gapped environments. The install guide is available on the ThreatQ Installation Landing page.

See the AGDS section for details regarding AGDS commands, functions, and upgrade procedures.

ThreatQ System Requirements

For the best performance, your system should meet the following requirements. Failing to meet the minimum system requirements can cause serious platform degradation and loss of functionality.

Virtual and BYOD System Requirements

For Virtual and Bring Your Own Device (BYOD) installations, your system must meet the following requirements:

DEPLOYMENT SIZE	TYPICAL USAGE	RECOMMENDED SETTINGS
< 2M indicators	Development or PoC (Small)	<ul style="list-style-type: none">• 4- 8 Core CPUs• 64 GB of RAM• 800 GB of hard disk provisioned size
2 - 10M indicators	Medium Production	<ul style="list-style-type: none">• 8 - 16 Core CPUs• 128 GB of RAM• 800 GB of hard disk provisioned size
> 10M indicators	Large Production	<ul style="list-style-type: none">• 16 - 32 Core CPUs• 256 GB of RAM• 2 TB of hard disk provisioned size

Minimum Screen Resolution

For ThreatQ to display properly, set your screen resolution to at least 1024 x 768 pixels.

ThreatQ as a Virtual Instance (OVA)

Virtual Prerequisites

The OVA works on ESX(i) 5.5 and above. When you install the OVA in an ESX(i) 5.5 or higher environment, the system asks if you want to upgrade the hardware level of the virtual machine. This is a supported choice as the OVA has been validated to run in both versions with the default hardware levels.



For instructions on installing the OVA on your Hypervisor, consult your Hypervisor's documentation.

Installing ThreatQ as a Virtual Instance



The page does not automatically refresh when the host has finished the reboot. Reboot times can vary based on the environment and may take up to several minutes.

1. Use the URL provided in your Welcome Letter to download a virtual machine image.
2. Import the OVA into your virtualization platform.



Do **not** accept the OVA's default allocations. Instead, allocate the system requirements described in [Virtual and BYOD System Requirements](#).

3. From the virtualization platform, launch the ThreatQ console and log in using the following credentials:

User: root

Password: fln75g98 (*see phonetic spelling below*)



The root user cannot SSH by default. For SSH access, you must create a new user.

PASSWORD CHARACTER

PHONETIC

f

foxtrot

l

lima

n

November

PASSWORD CHARACTER	PHONETIC
-----------------------	----------

7	seven
---	-------

5	five
---	------

g	golf
---	------

9	nine
---	------

8	eight
---	-------

4. Enter the following command to obtain the IP Address:

```
ip addr
```





The system enables DHCP by default. See [Configuring Network Connectivity](#) for static IP configuration.


5. Navigate to the returned IP Address in a web browser.
The ThreatQ first boot page loads. You can now [log in for the first time](#).

ThreatQ on Your Own Device (BYOD)

ThreatQuotient supports bring your own device (BYOD) installations of ThreatQ. We provide the following warnings to ensure the success of these installations and optimize your use of the application:

 After you install ThreatQ, it must be treated as an appliance. As such, you should not enable custom repos, install custom packages, or manually upgrade packages to unsupported versions since these changes may have a negative impact on performance.

 Using repositories other than ThreatQ's to install or upgrade your instance is not supported and may result in package conflicts during the install/upgrade process. ThreatQuotient recommends that you disable all repositories other than ThreatQ.

 For the ThreatQ platform to function optimally, EFI should be disabled because it is not supported.

BYOD Prerequisites

- A functional CentOS/RHEL 7.2 or later minimal install (7.2 to 7.9 minimal)
- Whitelisting of the following repository servers for software upgrades and system updates:
 - rpm.threatq.com
 - system-updates.threatq.com
- [ThreatQuotient Version 5 install script](#) (tqadmin)
- System time standard set to UTC.

Amazon Web Services (AWS) Guidelines

If you are using AWS for your installation, we recommend using an r5 instance family of at least a size matching the Virtual and BYOD System Requirements table found in the [ThreatQ System Requirements](#) chapter.



Throughout this document, **\$** identifies commands that can be run as any user, and **#** identifies commands that must be run as root.

BYOD Partitioning

For BYOD installations, we recommend the following partitioning scheme to attain the best ThreatQ experience:

FILESYSTEM	SIZE	USED	AVAILABLE	USE %	MOUNTED ON
/dev/mapper/VolGroup00-LogVol00	1.9T	66G	1.8T	4%	/
devtmpfs	63G	0	63G	0%	/dev
tmpfs	63G	0	63G	0%	/dev/shm
tmpfs	63G	17M	63G	1%	/run
tmpfs	63G	0	63G	0%	/sys/fs/cgroup
/dev/sda1	244M	164M	80M	68%	/boot
tmpfs	13G	0	13G	0%	/run/user/1002

BYOD Pre-installation

Before running the installation script, double-check the following system Timezone and SELinux configuration settings:

Timezone

The system time standard must be set to UTC.

```
$ ls -l /etc/localtime -> /usr/share/zoneinfo/UTC
```

If not, change where the /etc/localtime symlink points.

```
# unlink /etc/localtime
# ln -s /usr/share/zoneinfo/UTC /etc/localtime
```

SELinux

SELinux must be enabled. You can check this with the `sestatus` command.

```
$ sestatus
```

SELinux status: **enabled**

SELinuxfs mount: /sys/fs/selinux

SELinux root directory: /etc/selinux

Loaded policy name: targeted

Current mode: permissive

Mode from config file: disabled

Policy MLS status: enabled

Policy deny_unknown status: allowed

Max kernel policy version: 28

If SELinux is not enabled, enable it by editing the `config` file in the SELinux root directory as output by `sestatus`.



You are not required to change the `SELINUX=`line in the configuration file to `SELINUX=permissive`. However, the install process changes this value to `permissive` and resets it to the original value during the first boot process.

After this configuration change, you must reboot the system.

Downloading and Running TQAdmin



TQAdmin requires elevated privileges and must be run as root.

The TQAdmin yum installs the TQAdmin CLI on your device and allows you to use TQAdmin CLI commands, such as the `install` or `upgrade` commands.

Regardless of your install type, you need the TQAdmin tool either to for your initial install and/or for future version updates. If you are [installing ThreatQ on your own device \(BYOD\)](#), you must download TQAdmin to complete the install process. If you are [installing ThreatQ as a virtual instance](#), we recommend that you download TQAdmin since you will need it for future upgrades.

Downloading TQAdmin

1. To download dependencies for the TQAdmin yum package, run the following command:

```
# yum install https://vault.centos.org/7.9.2009/os/x86_64/Packages/bash-completion-2.1-8.el7.noarch.rpm
```

2. To download the TQAdmin yum package, run the following command:

```
# yum install https://download.threatq.com/tqadmin.rpm
```

Using TQAdmin to Install ThreatQ

1. To install the most recent version of ThreatQ, run the following command:

```
# /usr/local/bin/tqadmin platform install
```

2. To install any other ThreatQ version, add the `-v x.x.x` parameter to the install command:

```
# /usr/local/bin/tqadmin platform install -v <release number>
```




```
# /usr/local/bin/tqadmin platform install -v 5.29.4
```

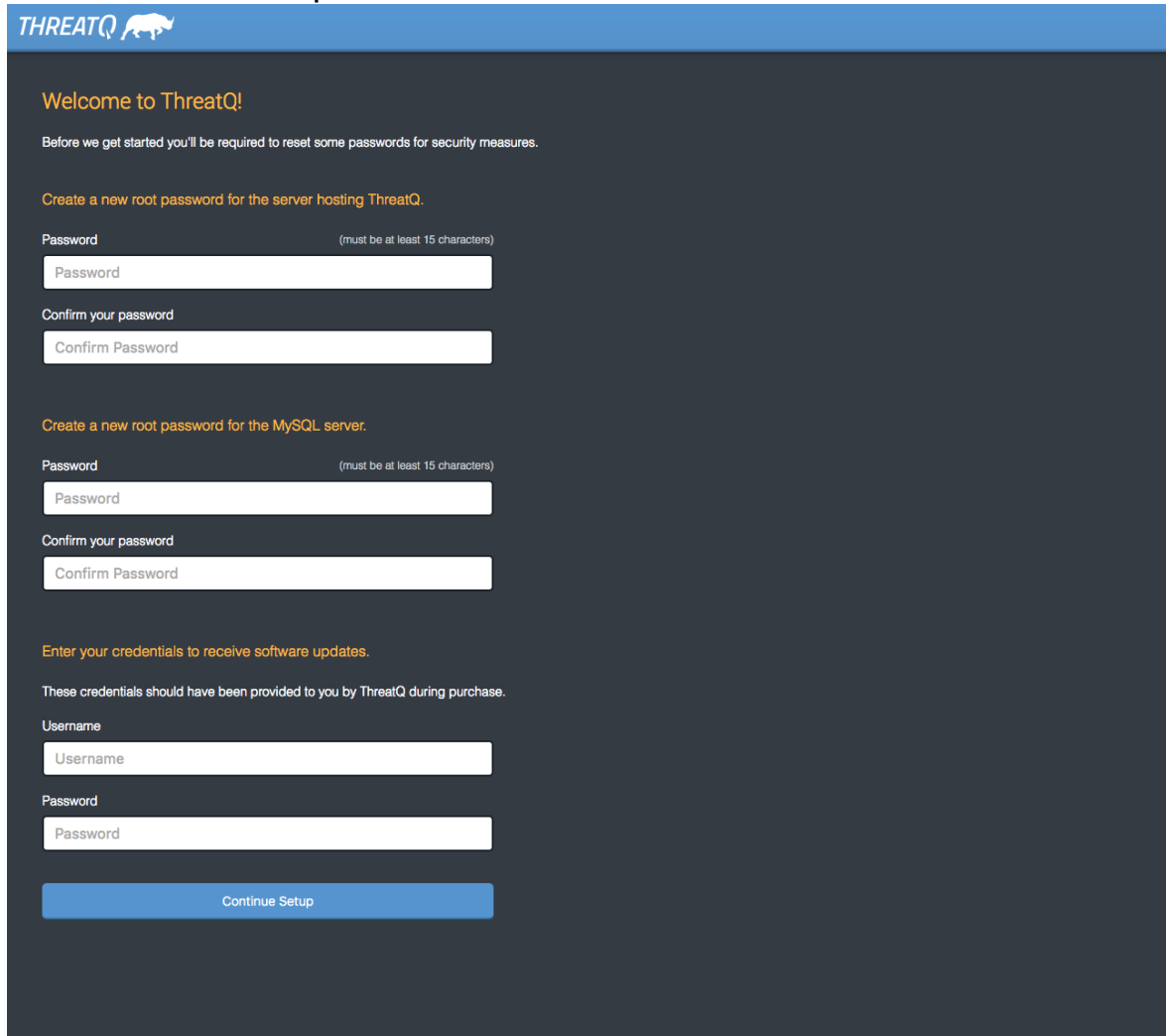
3. The install process prompts you for the `rpm.threatq.com` credentials provided to you by your ThreatQ field representative. If you do not have these credentials (username and a multi-character string), contact either your field sales contact or [ThreatQ Support](#). You also need these credentials for the first boot process.
4. After the install is complete, the server reboots.
5. On return to the prompt, you can [log in for the first time](#).

Logging In for the First Time

Regardless of your install type, your initial login to ThreatQ is an important step of the process that requires you to enter credentials and license information.

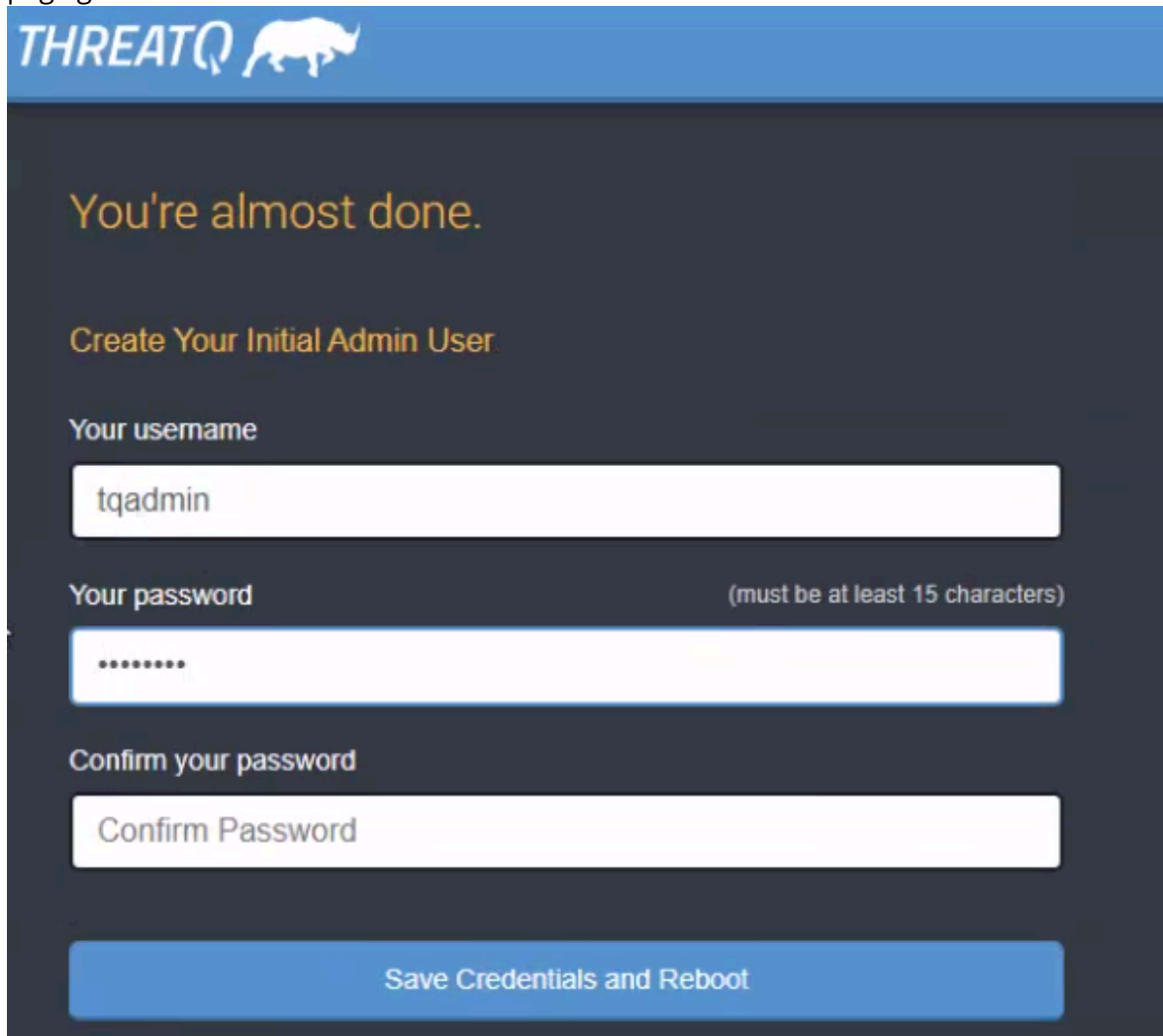
 You have one chance to enter these credentials.


1. Create new passwords and enter update credentials.
 - Provide and confirm a new root server password for the server hosting ThreatQ.
 - Provide and confirm a new root MySQL password.
 - Enter your YUM credentials to receive updates to the application.
 - Click the **Continue Setup** button.



2. Create the first ThreatQ admin user.
 - Create the initial admin user.
 - Provide and confirm a password.

- Click the **Save Credentials and Reboot ThreatQ** button. After you click this button, the page goes blank due to the server reboot.



THREATQ 

You're almost done.

Create Your Initial Admin User

Your username (must be at least 3 characters)

tqadmin

Your password (must be at least 15 characters)

.....

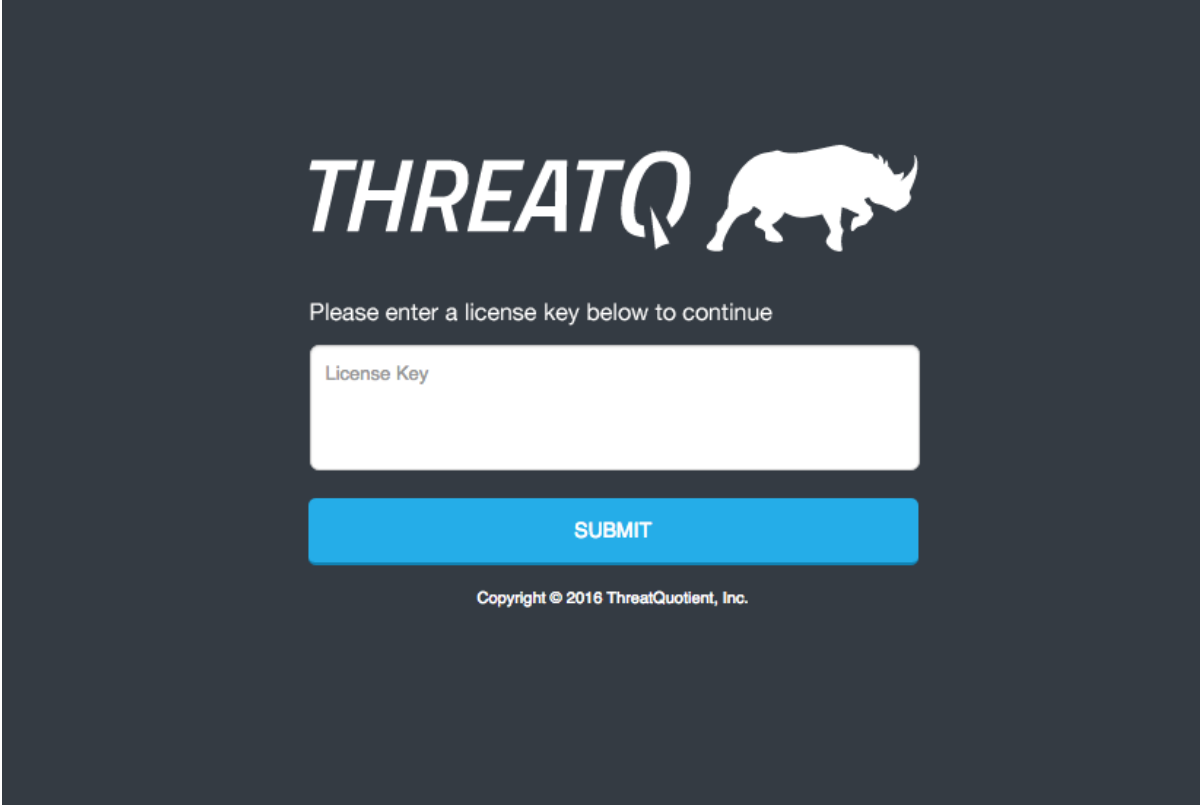
Confirm your password

Confirm Password

Save Credentials and Reboot

3. Wait approximately ten minutes for the server to reboot and navigate to the IP address you created for ThreatQ. You are redirected to the License Key screen which prompts you to

enter the license key included in your Welcome Letter.

The image shows a dark gray login screen for ThreatQ. At the top, the ThreatQ logo (the word 'THREATQ' in white, italicized, sans-serif font, followed by a white silhouette of a rhinoceros) is centered. Below the logo, the text 'Please enter a license key below to continue' is displayed in a smaller white font. Underneath this text is a large, white rectangular input field with the placeholder text 'License Key' in a light gray font. Below the input field is a bright blue rectangular button with the word 'SUBMIT' in white, uppercase, sans-serif font. At the bottom of the screen, the copyright notice 'Copyright © 2016 ThreatQuotient, Inc.' is written in a small white font.

4. Enter your license key and click the **Submit** button.
 5. Log in with the credentials you created in Step 2.
 6. Accept the End User License Agreement (EULA).
 7. Opt in/out for Product Analytics and then click the **Submit** button.
- Congratulations, you have now completed the installation of ThreatQ!

What to Do Next

Visit the [Help Center](#) for information on configuring ThreatQ imports from external feeds, or internal integrations with existing infrastructure.

Configuring Network Connectivity

Caution: The following steps must be performed as the root user or via sudo.

Configuring network connectivity for your ThreatQ environment may include some or all of the following processes:

- [Converting to a Static IP Address](#)
- Configuring chrony as a Network Timing Protocol (NTP) Client
- [Checking Connectivity to ThreatQ Servers](#)
- [Setting Up Your Proxy Server](#)

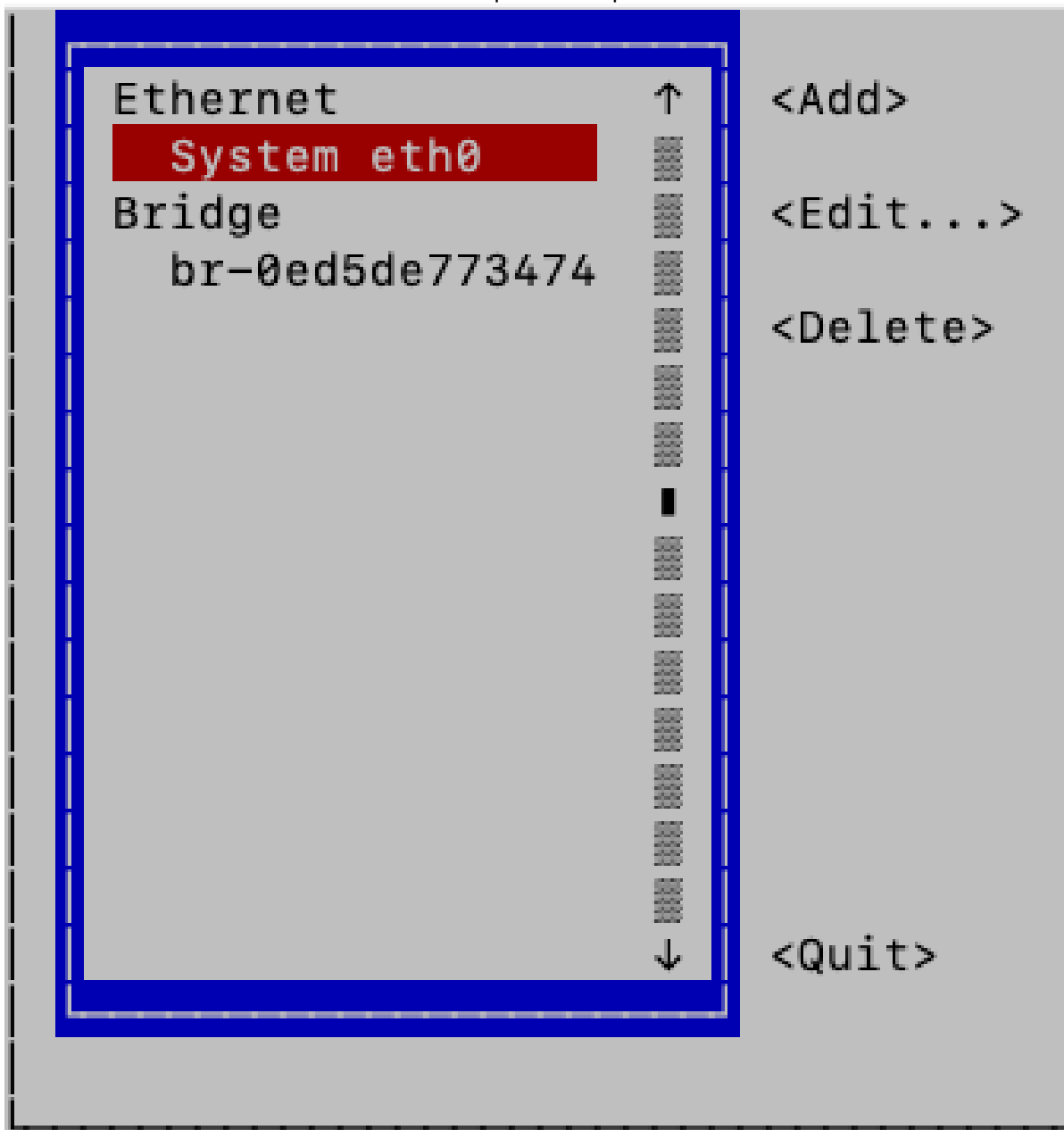
Converting to a Static IP Address

1. Run the network configuration utility from the command line:

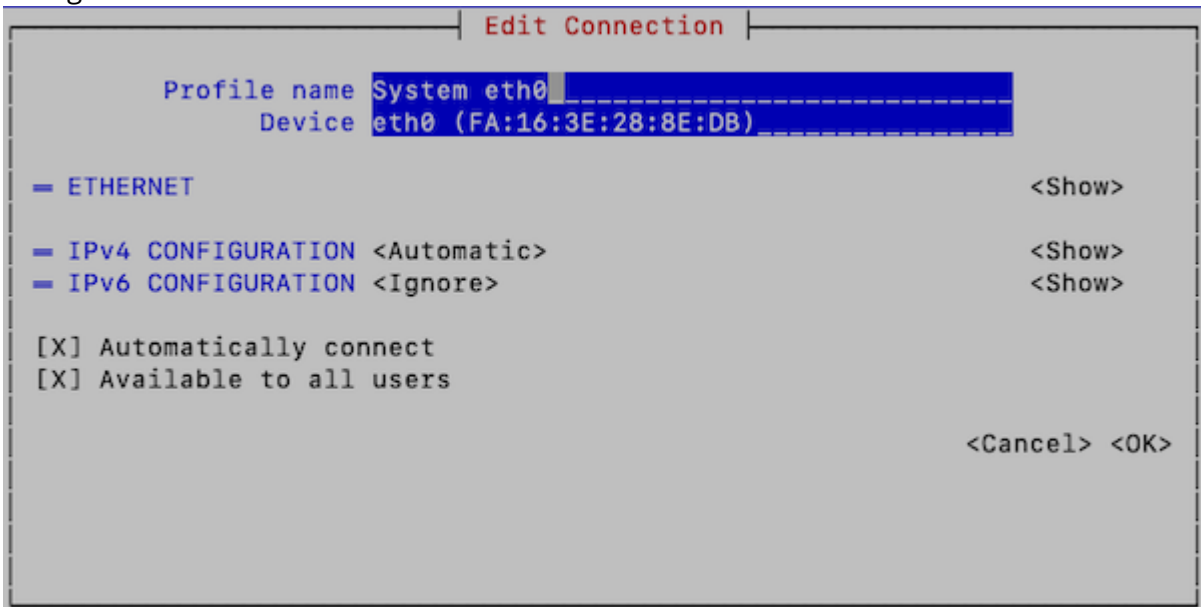
```
# nmtui-edit
```

2. Select the appropriate network interface in the left column.

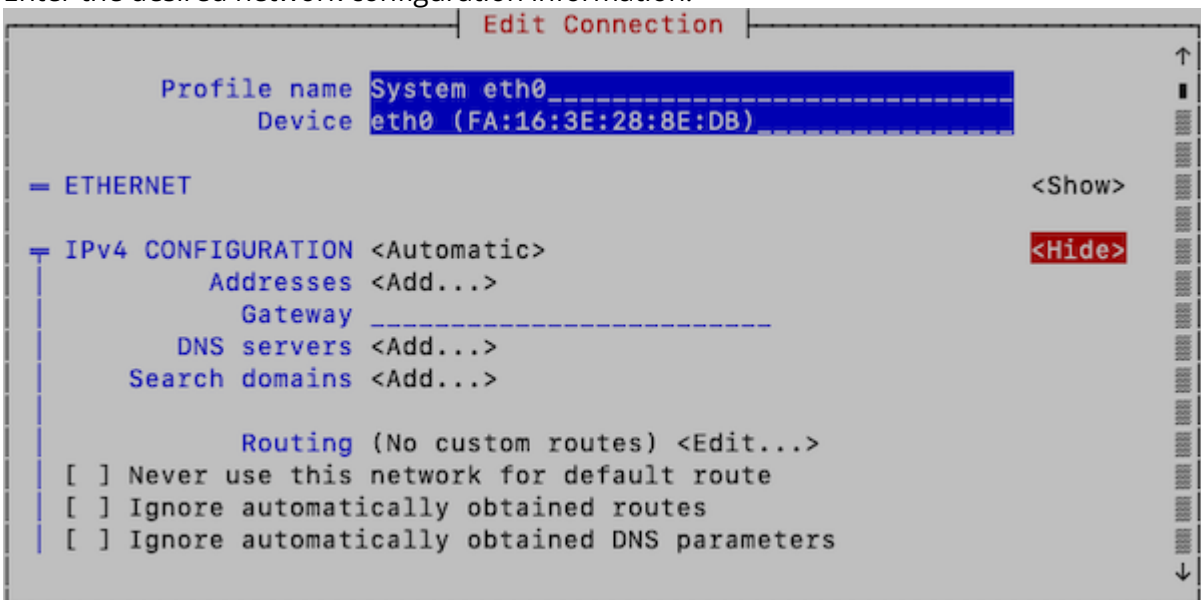
3. Press Tab to move the cursor to the **Edit** option and press Enter.



4. Press Tab to move the cursor to **<Show>** for the protocol (IPv4 or IPv6) that you wish to configure:



5. Enter the desired network configuration information.



6. Tab to **<OK>** and press Enter.
This returns you to the main page.
7. Tab to **<Quit>** to close the tool.
8. Enter the following command to restart networking:

```
# systemctl restart network
```

Networking configuration should now be complete. You can verify network configuration by running the `ip addr` command.

Checking Connectivity to ThreatQ Servers

To test your connection to the ThreatQ RPM servers, enter the following commands:

```
$ curl -Ihttps://rpm.threatq.com
HTTP/1.1 401 Unauthorized
Date: Tue, 19 Jul 2016 19:50:13 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.6.14
WWW-Authenticate: Basic realm="Restricted Access"
Content-Type: text/html; charset=iso-8859-1
```

```
$ curl -Ihttps://system-updates.threatq.com
HTTP/1.1 403 Forbidden
Date: Tue, 19 Jul 2016 19:53:19 GMT
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips
Last-Modified: Thu, 16 Oct 2014 13:20:58 GMT
ETag: "1321-5058a1e728280"
Accept-Ranges: bytes
Content-Length: 4897
Content-Type: text/html; charset=UTF-8
```

Setting Up Your Proxy Server

1. SSH into your ThreatQ instance.
2. Open the environment file using the vi command:

```
vi /etc/environment
```

3. Press the i character to enter insert mode. Enter your following entry into the file while replacing the placeholders with your information. These settings are case-sensitive so you must include both the lowercase, ex: http, and uppercase, ex: HTTP, versions.



You can add exceptions to the no_proxy strings to prevent specific entries that should not be forwarded to the proxy. The minimal value for no_proxy should be the loopback IP address and "localhost" plus the TQ entry for itself "threatq". Do not use CIDR notation or wildcards with no_proxy entries as they are not accepted formats. In that situation, list the IP addresses.

If Proxy Server Requires a Password

```
http_proxy=http://<username>:<password>@<Proxy IP>:<Proxy Port>
HTTP_PROXY=http://<username>:<password>@<Proxy IP>:<Proxy Port>
https_proxy=http://<username>:<password>@<Proxy IP>:<Proxy Port>
HTTPS_PROXY=http://<username>:<password>@<Proxy IP>:<Proxy Port>
```

```
no_proxy=localhost,127.0.0.1,threatq,<ThreatQ IP>, <ThreatQ Hostname>
NO_PROXY=localhost,127.0.0.1,threatq,<ThreatQ IP>, <ThreatQ Hostname>
```

If Proxy Server Does Not Require a Password

```
http_proxy=http://<Proxy IP>:<Proxy Port>
HTTP_PROXY=http://<Proxy IP>:<Proxy Port>
https_proxy=http://<Proxy IP>:<Proxy Port>
HTTPS_PROXY=http://<Proxy IP>:<Proxy Port>
no_proxy=localhost,127.0.0.1,threatq,<ThreatQ IP>, <ThreatQ Hostname>
NO_PROXY=localhost,127.0.0.1,threatq,<ThreatQ IP>, <ThreatQ Hostname>
```

4. Press the **ESC** key and enter the following command to close the editor:

```
:wq <Enter Key>
```

The next several steps will show you how to ensure that custom connector CRON jobs are able to use the proxy settings. This is achieved by sourcing the environment script so that it is available to all child sessions and applications.

5. Open the proxy.sh file using the vi command:

```
vi /etc/profile.d/proxy.sh
```

6. Press the **i** key to enter Insert mode and enter the following lines:

```
set -a
source /etc/environment
set +a
```

This will ensure the automatic export of any variables created.

7. Press the **ESC** key and enter the following command to close the editor:

```
:wq <Enter Key>
```

8. Log out of your session and then log back in.
9. Run the following command to confirm your settings:

```
printenv | grep -i proxy
```

10. Remove any other proxy-related files from the `/etc/profile.d` directory.

Hosting Services

ThreatQuotient offers a robust, hosted solution for your ThreatQ applications. The following table outlines key operational/maintenance events and specifies whether the customer or ThreatQuotient handles the tasks associated with them:

EVENT	TASK	CUSTOMER	THREATQUOTIENT
Back-End Service Failure			✓
	Platform Maintenance and Upgrades		
	Request a platform upgrade	✓*	
	Performing platform upgrades and maintenance		✓
	Detecting and fixing failed upgrades		✓
	Security patching		✓
	Backup		✓
Network Configuration	Disaster recovery		✓*
	Creating user accounts	✓	

Resetting passwords for users	✓
General Configuration	
Enabling MFA	✓
SAML/LDAP	✓
Integration Upgrades/ Installs	
CDFs	✓
Operations	✓
Custom connectors	✓*
Integration Configuration	
API keys and credentials	✓
Monitoring feed failures (via email alerts)	✓
App configuration (e.g. Splunk)	✓
Customer Support Requests	✓*

*Open a Help Desk ticket with ThreatQuotient Support via phone, [email](#), or the [ThreatQuotient Support Portal](#).

FIPS 140-2 Compliance

The Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules was issued by the National Institute of Standards and Technology (NIST) in May, 2001, and is the Federal standard for proper cryptography for computer systems purchased by the government and was issued. The standard specifies the security requirements for cryptographic modules utilized within a security system that protects sensitive or valuable data.

Utilizing the FIPS 140-2 validated crypto module ensures that the crypto algorithms used are deemed appropriate and perform the encrypt/decrypt/hash functions in accordance to the NIST standard. The requirements can be found in the following documents:

- [Security Requirements for Cryptographic Modules](#)
- [Annex A: Approved Security Functions for FIPS PUB 140-2, Security Requirements for Cryptographic Modules](#)

ThreatQ FIPS 140-2 Compliance

ThreatQuotient complies with FIPS 140-2, which defines the technical requirements to be used by Federal Agencies when these organizations specify cryptographic-based security systems for protection of sensitive or valuable data.

The compliance of ThreatQ with FIPS 140-2 is ensured by:

- Integrating validated and NIST-certified third party cryptographic module(s), and using the module(s) as the only provider(s) of cryptographic services;
- Using FIPS-approved cryptographic functions;
- Using FIPS-approved and NIST-validated technologies applicable for ThreatQ design, implementation and operation.

Modes of Operation

The ThreatQ platform operates in one of two modes, as determined by the OS configuration.

MODE	DETAILS
FIPS-Compliant Mode	This mode supports FIPS 140-2 compliant cryptographic functions. In this mode, all cryptographic functions, default algorithms, and key lengths are bound to those allowed by FIPS 140-2.
Standard Mode	This mode is non-FIPS 140-2 compliant mode which utilizes all existing ThreatQ cryptography functions.

TLS

All the ThreatQ platform communications can be secured with FIPS-compliant Transport Layer Security TLS1.2 or higher, which relies on FIPS 140-2 approved hash algorithms and ciphers.

- TLS handshake, key negotiation and authentication provides data integrity and uses secure hash and FIPS 140-2 approved cryptography and digital signature.
- TLS encryption of data in transit provides confidentiality and makes use of FIPS 140-2 approved cryptography.

Enabling FIPS Mode

ThreatQ conforms with FIPS 140-2 Level 1 compliance by dynamically linking to the FIPS 140-2 approved OpenSSL cryptographic module provided by the Operating System, which is currently the **Red Hat Enterprise Linux 7 OpenSSL Module**.

The ThreatQ platform can be configured to operate in **FIPS-Compliant Mode** to ensure its functions and procedures that require cryptography (secure hash, encryption, digital signatures etc.), such as SSL/TLS connections, makes use of the crypto services provided by Red Hat Enterprise 7 OpenSSL Module v3.0, which is validated for FIPS 140-2.



The assurance that ThreatQ is using the right FIPS 140-2 encryption modules is managed at the operating system level by CentOS implementation.

ThreatQ checks the OS level flag setting `/proc/sys/crypto/fips_enabled` to kick off ThreatQ's FIPS mode installation.

You can enable FIPS Mode in your ThreatQ environment manually or via script. Links to both methods can be found below.

METHOD

STEPS REFERENCE

Manual
Configuration

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/chap-federal_standards_and_regulations#sec-Enabling-FIPS-Mode

enableFIPS
Script

<https://access.redhat.com/discussions/3487481>

Change Log



Version numbers assigned to the change log entries below indicate document versions and not ThreatQ platform versions.

- **Version 1.0.9**
 - Updated [Downloading and Running TQAdmin](#).
- **Version 1.0.8**
 - Updated [Downloading and Running TQAdmin](#).
- **Version 1.0.7**
 - Updated [ThreatQ on your own device BYOD](#).
- **Version 1.0.6**
 - Updated the Proxy setting commands.
- **Version 1.0.5**
 - Updated [ThreatQ on your own device BYOD](#).
- **Version 1.0.4**
 - Updated [Configuring Network Connectivity](#).
- **Version 1.0.3**
 - Updated [BYOD Partitioning requirements](#).
- **Version 1.0.2**
 - Updated the process for Setting the Network Timing Protocol.
- **Version 1.0.1**
 - Updated the [AWS guidelines](#) for Virtual and BYOD deployments.
- **Version 1.0.0**
 - Initial Release