ThreatQuotient

ThreatQ Version 5 Air Gapped Installation Guide

Version 1.0.4

July 03, 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

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.

ThreatQ in an Air Gapped Environment

ThreatQuotient supports the deployment of ThreatQ version 5 on an air gapped device. An air gapped device can be defined as a device situated in a location with no or limited public network access.

The standard steps for installing ThreatQ require network access to the ThreatQ repositories to download and install the platform. In an air gapped instance, where the device cannot make that connection, you must download required files from a network-connected device and then transfer those files to the targeted air gapped device. The process is the same when it comes to upgrading an air gapped device.

This document will provide you with the requirements, recommended settings, and the steps for installing a new instance of ThreatQ version 5 on a device in an air gapped environment.

> Throughout this guide, you will see commands with $ and # characters. $ identifies commands that can be run as any user while # identifies commands that must be run as root.

Warnings

ThreatQuotient supports bring your own device (BYOD) air gapped installations of ThreatQ.

Review the following warnings to ensure the success of your installation and to 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.

Prerequisites

Review the following requirements before attempting to install the ThreatQ platform on your air gapped device.

Recommended Settings per Deployment Size

Your system must meet the following requirements:

DEPLOYMENT SIZE	TYPICAL USAGE	RECOMMENDED SETTINGS
< 2M indicators	Development or PoC (Small)	• 4- 8 Core CPUs • 64 GB of RAM • 800 GB of hard disk provisioned size
2 - 10M indicators	Medium Production	• 8 - 16 Core CPUs • 128 GB of RAM • 800 GB of hard disk provisioned size
> 10M indicators	Large Production	• 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.

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.

Before you begin, confirm that you have the following:

- A functional CentOS/RHEL 7.2 or later minimal install (7.2 to 7.9 minimal)
- ThreatQ version 5 tarball package - steps to download this package are included in the Installation chapter.
- ThreatQuotient 5 install script (tqadmin) - steps to download this package are included in the Installation chapter.
- Customer configuration (RPM username and password)

- 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 Recommended Settings per Deployment Size .

Partitioning

The following is recommend for your 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

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.

Root Password Requirements

You need to load your configuration into the environment prior to installing ThreatQ.

```
# export CUSTOMER_USERNAME='your username'

# export CUSTOMER_PASSWORD='your password'
```

Air Gapped Installation

The following steps will walk you through how to download all necessary files and install ThreatQ on an air gapped device.

1. Log into https://install.threatq.com/ using your YUM credentials.
2. Locate and download the appropriate ThreatQ install tarball.

   File Name Format:
   <version>-platform.tar.gz

   Example:
   5.6.1-platform.tar.gz

   You can also download the tarball using a curl command:

   ```
   curl https://<YUM_USER>:<YUM_PASSWORD>@install.threatq.com/<version>-platform.tar.gz -o
   <version>-platform.tar.gz
   ```
3. Open the CLI of the device you will install ThreatQ on and copy the install tarball to `/root/` using the SCP client of your choice.
4. Return to the CLI of the device and confirm that the install tarball is present.
5. Use the following curl command to download dependencies for the TQAdmin yum package:

   ```
   # curl https://vault.centos.org/7.9.2009/os/x86_64/Packages/bash-completion-2.1-8.el7.noarch.rpm -o
   bash-completion-2.1-8.el7.noarch.rpm
   ```
6. Log into https://download.threatq.com/ using your YUM credentials.
7. Download the `tqadmin.rpm` file.

   You can also download the rpm using a curl command:

   ```
   curl https://download.threatq.com/tqadmin.rpm -o tqadmin.rpm
   ```
8. Open the CLI of the device you will install ThreatQ on and copy the `tqadmin.rpm` file to `/root/` using the SCP client of your choice.
9. Run the following command to install TQAdmin on the air gapped device:

   ```
   yum localinstall <path to tqadmin rpm>
   ```
10. Log into the air gapped device as a root user.
11. Run the following command to install ThreatQ on the air gapped device:

    ```
    tqadmin platform install -v <release number> -z
    ```

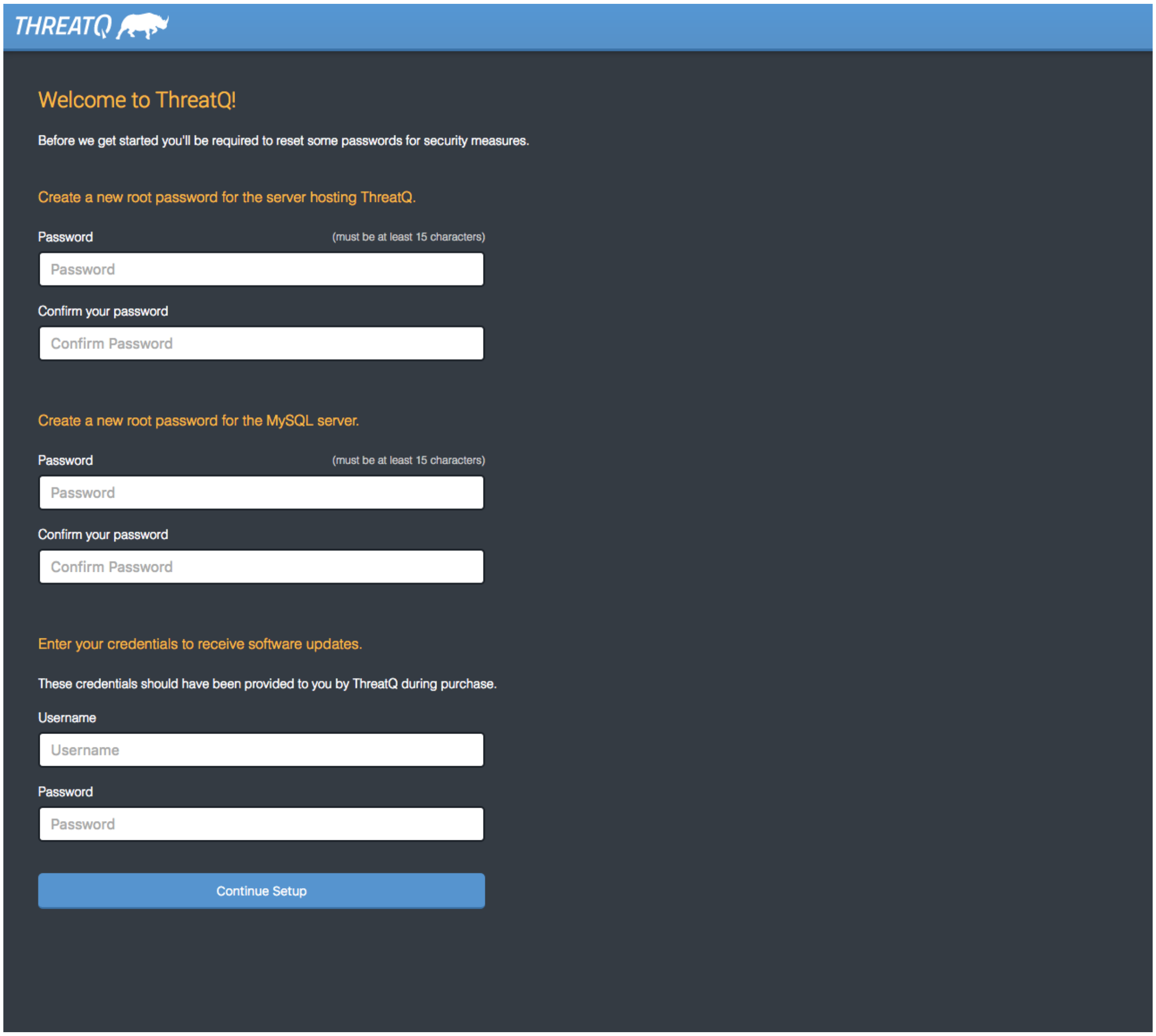
    Example:

    > tqadmin platform install -v 5.6.1 -z

The install process will look for the install tarball in the /root/ location. If the file is not in that location, you are prompted to enter the absolute path of the tarball.

12. Navigate to your instance in a web browser after the install process has completed.

    The Welcome ThreatQ page will load.



Welcome to ThreatQ!

Before we get started you'll be required to reset some passwords for security measures.

Create a new root password for the server hosting ThreatQ.

Password (must be at least 15 characters)

Confirm your password

Create a new root password for the MySQL server.

Password (must be at least 15 characters)

Confirm your password

Enter your credentials to receive software updates.

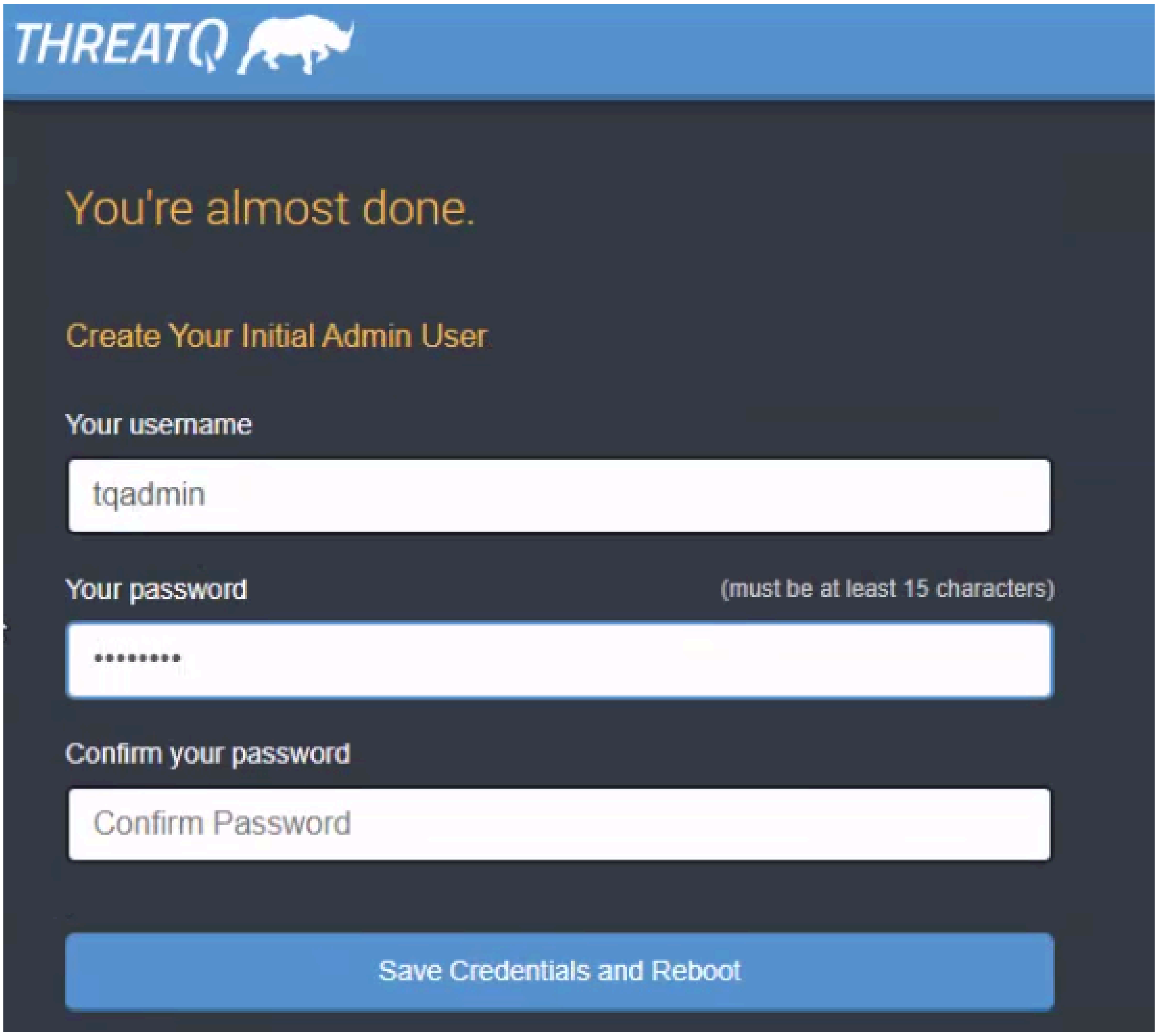
These credentials should have been provided to you by ThreatQ during purchase.

Username

Password

13. Create a new **Password** for the server hosting ThreatQ.
14. Create a new **Password** for the MySQL server.
15. Enter your YUM credentials (username and password).
16. Click on **Continue Setup**.

The Initial Admin User page will load.



You're almost done.

Create Your Initial Admin User

Your username

tqadmin

Your password (must be at least 15 characters)

•••••••••

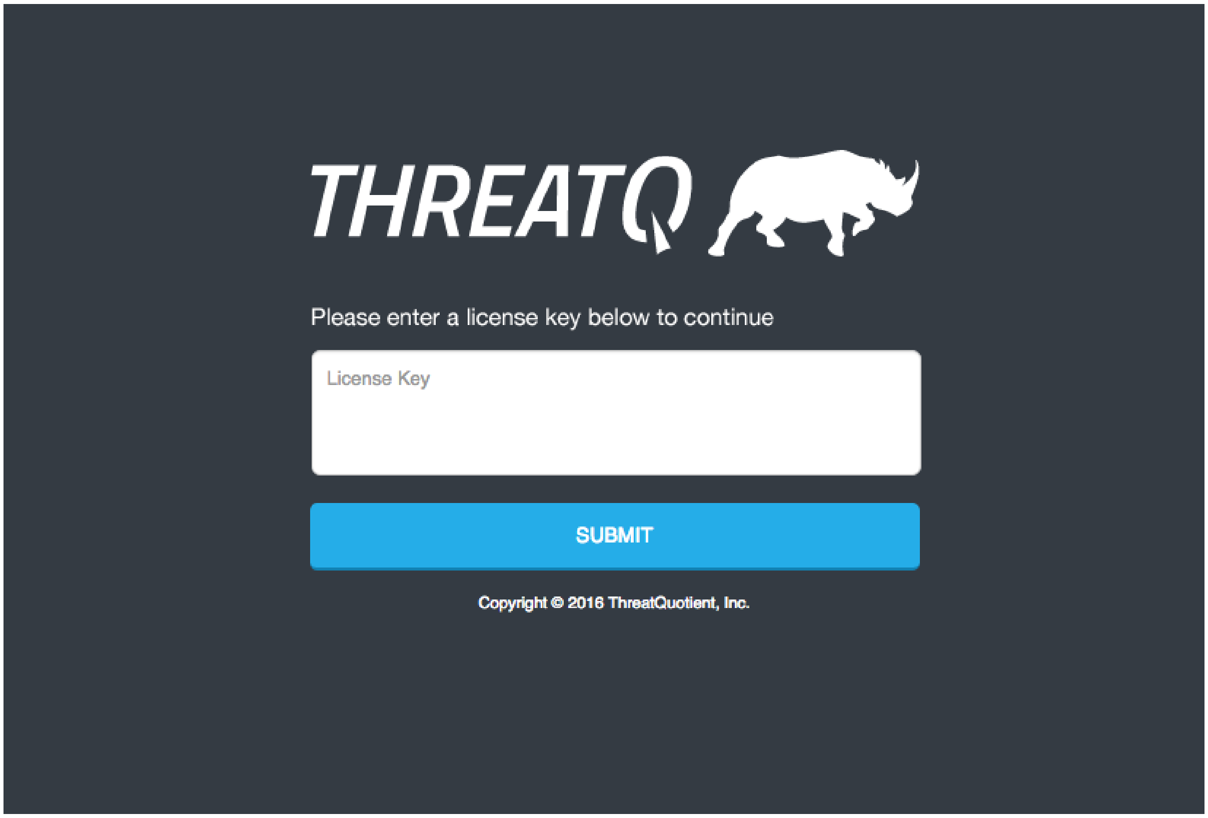
Confirm your password

Confirm Password

17. Create your initial Admin account for the ThreatQ platform by providing a email address and password. This account will serve as your Maintenance account.
18. Click on **Save Credentials and Reboot ThreatQ**.

> The server will reboot. It may take up to 10 minutes for the server to complete this process.

19. Refresh the page or navigate back to the ThreatQ instance after the reboot process has completed. You will be prompted for a license key.


Please enter a license key below to continue

20. Enter your **License Key** and click on **Submit**.

> Your license key is included in your Welcome Letter from ThreatQ Support.

21. Log in with the credentials you created in step 16.
22. Accept the End User License Agreement (EULA).
23. Opt in/out for Product Analytics and then click the **Submit** button.

Configuring Network Connectivity

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

- Converting to a Static IP Address
- Setting the Network Timing Protocol (NTP)
- Setting Up Your Proxy Server

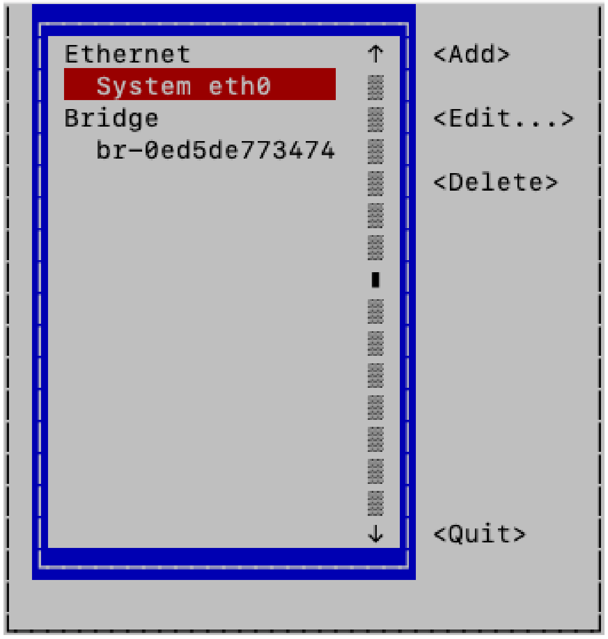
> ⚠ The following steps must be performed as the root user or via sudo.

Converting to a Static IP Address

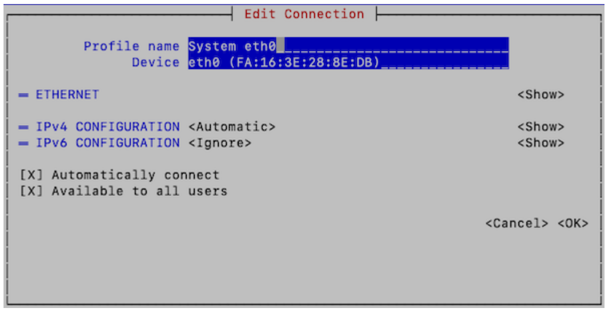
1. Run the network configuration utility from the command line:

```
# 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.

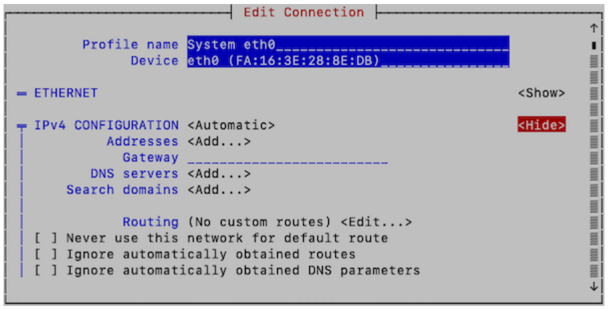


4. Press Tab to move the cursor to **<Show>** for the protocol (IPv4 or IPv6) that you wish to configure:



```
                         Edit Connection

          Profile name System eth0
                Device eth0 (FA:16:3E:28:8E:DB)

═ ETHERNET                                              <Show>

═ IPv4 CONFIGURATION <Automatic>                        <Show>
═ IPv6 CONFIGURATION <Ignore>                           <Show>

[X] Automatically connect
[X] Available to all users

                                                  <Cancel> <OK>
```

5. Enter the desired network configuration information.



```
                         Edit Connection

          Profile name System eth0
                Device eth0 (FA:16:3E:28:8E:DB)

═ ETHERNET                                              <Show>

╤ IPv4 CONFIGURATION <Automatic>                        <Hide>
│          Addresses <Add...>
│            Gateway _________________________
│        DNS servers <Add...>
│     Search domains <Add...>
│
│            Routing (No custom routes) <Edit...>
│ [ ] Never use this network for default route
│ [ ] Ignore automatically obtained routes
│ [ ] Ignore automatically obtained DNS parameters
```

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.

Configuring chrony as a Network Timing Protocol (NTP) Client

In Linux systems, the chronyd daemon provided by the chrony package is the default NTP client. By default, chronyd uses an NTP.org pool as the time source. You can update the `server` or `pool` option in the `/etc/chrony.conf` file to specify a single NTP (`server`) or pool of NTP servers (`pool`) as the time source.

1. Enter the following command to access the NTP configuration file:

   ```
   vi /etc/chrony.conf
   ```

2. To specify a single NTP sever as your time source, add the following lines to the chrony configuration file, replacing *<ntp server>* with your preferred NTP server.

   ```
   server <NTP server> iburst
   ```

   To specify a pool of NTP servers as your time source, add the following lines to the chrony configuration file, replacing *<ntp server pool>* with your preferred NTP server pool.

```
pool <NTP server pool> iburst
```

3. Save your changes.
4. For your changes to take affect you must reboot or use the following command to restart chronyd:

```
systemctl restart chronyd
```

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.

Upgrading

Perform the following steps to upgrade an air gapped ThreatQ instance.

1. Log into https://install.threatq.com/ using your YUM credentials.
2. Locate and download the appropriate air gap upgrade file.

   File Name Format:
   <version>-platform.tar.gz

   Example:
   5.6.1-platform.tar.gz

   You can also download the upgrade tarball using a curl command:

   ```
   curl https:// : @install.threatq.com/ <version>-platform.tar.gz -o <version>-platform.tar.gz
   ```
3. Open the CLI of the device to upgrade and copy the upgrade file to `/root/` using the SCP client of your choice.
4. Return to the CLI of the device and confirm that the upgrade file is present.
5. Log into the air gapped box as a root user.
6. Run the following command to upgrade the air gapped box:

   ```
   tqadmin platform upgrade -v <release number> -z
   ```

   Example:

   EX tqadmin platform upgrade -v 5.6.1 -z

   The upgrade process will look for the upgrade tarball in the `/root/` location. If the file is not in that location, you are prompted to enter the absolute path of the tarball.

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 Crytographic 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 1.04.**
  - Added instructions for adding dependencies for TQAdmin.
- **Version 1.0.3**
  - Updated Time standard requirements.
- **Version 1.0.2**
  - Updated the Proxy setup commands.
- **Version 1.0.1**
  - Updated the **Setting Up Your Proxy Server** chapter.
  - Updated the **Setting the Network Timing Protocol (NTP)** chapter.
- **Version 1.0.0**
  - Initial Release