

# ThreatQuotient



## ThreatQ Version 6 Air Gapped Installation Guide

Version 1.3.3

May 09, 2025

### ThreatQuotient

20130 Lakeview Center Plaza Suite 400  
Ashburn, VA 20147

### Support

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [support.threatq.com](http://support.threatq.com)

Phone: 703.574.9893

# Contents

<b>Warning and Disclaimer .....</b>	<b>3</b>
<b>ThreatQ 6x Air Gapped Installation .....</b>	<b>4</b>
Operating System and Kubernetes Distribution Maintenance .....	4
Supported Hardening Standards by Operating System.....	4
Security Technical Implementation Guide (STIG) Installs.....	5
Prerequisites.....	5
System Requirements.....	5
ThreatQ v6 BYOD Partitioning Overview .....	6
Specific Sizes Overview .....	6
Specific Size Breakdown .....	8
Dedicated Mount /opt .....	9
Before You Begin .....	9
Set up Your Ubuntu or RHEL Environment .....	9
Pin Your RHEL 9 Version .....	10
Pin Your Ubuntu 22.04 Version.....	11
Configure Internal Networking .....	11
Prepare the RKE2 Configuration File .....	12
Change the Kubernetes Subnet (Optional) .....	13
Set Up kubectl .....	13
Verify Your RKE2 Installation .....	14
Air Gapped Installation .....	14
Access Your New ThreatQ 6x Instance .....	17
Next Steps .....	17
<b>Change Log .....</b>	<b>18</b>

# 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 © 2025 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 6x Air Gapped Installation

ThreatQuotient supports the deployment of ThreatQ version 6 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 6 on a device in an air gapped environment.



ThreatQuotient recommends you install the most recent version of ThreatQ 6x for your upgrade.

## Operating System and Kubernetes Distribution Maintenance

After upgrading to ThreatQ 6x, customers are responsible for maintaining their RHEL or Ubuntu operating system as well as the RKE2 Kubernetes distribution.

ThreatQ currently supports RHEL 8.10 or 9.4, Ubuntu 22.04 LTS, and the latest, stable RKE2 version. Before updating to a different version, please contact ThreatQuotient Support to confirm compatibility.

## Supported Hardening Standards by Operating System

ThreatQ v6 supports the following hardening standards for RHEL 8.10, RHEL 9.4, and Ubuntu 22.04 LTS:

	RHEL 8.10	RHEL 9.4	UBUNTU 22.04 LTS
CIS Level 1	X	✓	X
CIS Level 2	X	✓	X
STIG	✓	✓	X

See the ThreatQ v6 RHEL v9 Hardening guide for more information on implementing CIS Level 1, CIS Level 2, and STIG hardening standards in a RHEL 9.4 environment.

## Security Technical Implementation Guide (STIG) Installs

This installation guide includes STIG Install Notes to assist customers performing a STIG install of ThreatQ 6x on RHEL 8.10 or 9.4 instances.

## Prerequisites

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

## System Requirements

**⚠** Before you begin a ThreatQ install, you must disable any security endpoint tools running on your VM as this may cause the installation to fail.

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.

- Ubuntu 22.04 LTS or Red Hat Enterprise Linux (RHEL) 8.10 or 9.4 instance that meets ThreatQ System Requirements and is configured to use UTC as the time zone standard.
- The latest stable RKE2 version. See the steps below for information on installing and configuring RKE2.
- The following packages must be installed on your system: bash-completion, curl, gnupg, python3, tmux, wget, and zstd. In addition, software-properties-common is required for Ubuntu. The container-selinux and iptables packages are required for RHEL.
- Your ThreatQ license key.
- Your ThreatQ YUM credentials.
- A static IP address assigned to the new Ubuntu or RHEL instance.
- Firewall access to the following ports:

### ThreatQ Appliance Ports

SOURCE	DESTINATION	PORT	PORT USE
All of the workstations that will be used by security analysts	ThreatQ	443	Open for ThreatQ UI (HTTPS / TLS)

SOURCE	DESTINATION	PORT	PORT USE
Workstations that will access remotely ThreatQ	ThreatQ	22	Secure shell access. Open for shell access by administrators
All of the workstations that will be used by security analysts	ThreatQ	80	Redirects to 443 to ensure TLS is used
TAXII Clients	ThreatQ	5910	Used by the embedded TAXII server
Other TQX subscribers	ThreatQ Publisher	8883	Used by ThreatQ Exchange (TQX) Broker (opendxl-broker). The port is used for TQX communication. This is the subscriber's incoming connection port

## ThreatQ v6 BYOD Partitioning Overview

For BYOD 6x installations, we require the following partition scheme to obtain the best ThreatQ experience.

### Specific Sizes Overview

Use the following in the event that your organization requires specific sizes:

FILE SYSTEM	SIZE	NOTES
/	50GB	N/A
/var	120GB/ 200GB	200GB is the recommended size if there are no other partitions under <b>/var</b> . 120GB is the recommended size if there are separate log and tmp partitions under <b>/var</b> . Images are stored in <b>/var</b> in addition to the locations listed below.

FILE SYSTEM	SIZE	NOTES
		See the breakdown of the individual locations within <b>/var</b> in the Specific Size Breakdown table below.
/opt	>=600GB	The majority of resources should be dedicated to this location. MYSQL and SOLR utilize this mount point. A minimum of 600GB to several TBs is required for optimal performance.

## Specific Size Breakdown

The following is a more detailed break down of specific sizes (listed on the overview table above):

FILE SYSTEM	SIZE	NOTES
/boot	1GB	N/A
/home	20GB	N/A
/tmp	20GB	N/A
/var/tmp	5GB	<ul style="list-style-type: none"> <li>If your <b>/var</b> size is 200GB, the <b>/var/tmp</b> size is included in the overall recommended <b>/var</b> file system size of 200GB.</li> <li>If your <b>/var</b> size is 120GB, the <b>/var/tmp</b> size is not included in the overall recommended <b>/var</b> size of 120GB.</li> </ul>
/var/log	50GB	<p>All container logs are written to this location. You can increase the size if needed.</p> <ul style="list-style-type: none"> <li>If your <b>/var</b> size is 200GB, the <b>/var/log</b> size is included in the overall recommended <b>/var</b> file system size of 200GB.</li> <li>If your <b>/var</b> size is 120GB, the <b>/var/log</b> size is not included in the overall recommended <b>/var</b> size of 120GB.</li> </ul>
/var/log/audit	20GB	<ul style="list-style-type: none"> <li>If your <b>/var</b> size is 200GB, the <b>/var/log/audit</b> size is included in the overall recommended <b>/var</b> file system size of 200GB.</li> <li>If your <b>/var</b> size is 120GB, the <b>/var/log/audit</b> size is not included in the overall recommended <b>/var</b> size of 120GB.</li> </ul>
/	>=680GB	All remaining resources should be dedicated to this location.



## Dedicated Mount /opt


Use the following sizing, in addition to the Specific Size Breakdown table, if you are required to create a dedicated mount for /opt.

FILE SYSTEM	SIZE	NOTES
/	250GB	N/A
/opt	>=600GB	The majority of resources should be dedicated to this location. A minimum of 600GB to several TBs is required for optimal performance.

## Before You Begin

Before setting up your new environment, installing ThreatQ 6x, and migrating your ThreatQ 5x data, we recommend the following preparation:

- Create a non-root user for the new ThreatQ 6x environment.
- Determine if you want to use the default IP range for K8s on the new 6x instance or a custom IP range.
- Make sure your YUM credentials are easily accessible. If you do not have them, please reach out to [ThreatQ Support](#).

 The following install steps must be completed using a non-root user account.

## Set up Your Ubuntu or RHEL Environment

1. Provision a new amd64 Ubuntu 22.04 LTS or RHEL 8.10 or 9.4 instance that meets ThreatQ system requirements.

DEPLOYMENT SIZE	TYPICAL USAGE	REQUIRED HARDWARE SPECIFICATIONS	MINIMUM INSTANCE SIZE FOR AWS DEPLOYMENT
<2M Indicators	Development or PoC (small)	<ul style="list-style-type: none"> <li>• 4-8 Core CPUs</li> <li>• 64GB RAM</li> <li>• 800GB of provisioned storage</li> </ul>	r6i.2xlarge
2 - 10M Indicators	Medium Production	<ul style="list-style-type: none"> <li>• 8-16 Core CPUs</li> <li>• 128GB RAM</li> <li>• 800GB of provisioned storage</li> </ul>	r6i.4xlarge
>10M Indicators	Large Production	<ul style="list-style-type: none"> <li>• 16-32 Core CPUs</li> <li>• 256GB RAM</li> <li>• 2TB of provisioned storage</li> </ul>	r6i.8xlarge

- Run the following command to set the maximum number of inotify instances for the installing user to 300.



If the inotify instance maximum is already configured for your system, this command will overwrite any existing value with a value of 300.

```
sudo sed -i '/^fs\.inotify\.max_user_instances/d' /etc/sysctl.conf &&
printf "fs.inotify.max_user_instances = 300\n" | sudo tee -a /etc/
sysctl.conf >/dev/null && sudo sysctl -p
```

## Pin Your RHEL 9 Version

The following steps allow you to pin your current RHEL 9 release so that you cannot inadvertently upgrade your RHEL 9 environment to an unsupported release. See the Red Hat Enterprise Linux 9 Support section for more information on currently supported RHEL 9 versions.



Run the following commands as root or prefix them with sudo.

- Set release to minor version:

```
subscription-manager release --set=<release number>
```

2. Clean repositories:

```
yum clean all
```

3. Check which release is set locally:

```
subscription-manager release --show
```

## Pin Your Ubuntu 22.04 Version

ThreatQ recommends you update the **release-upgrades** file to disable manual Ubuntu upgrades so that you cannot inadvertently upgrade your Ubuntu 22.04 environment to an unsupported release.

1. Use a text editor, such as vi, to access `/etc/update-manager/release-upgrades`.
2. Change the `Prompt=` setting to `Prompt=never`.
3. Save your changes and exit the file.

## Configure Internal Networking



With the default configuration, changing the hostname or external IP address of a Kubernetes system can cause unrecoverable errors that require a complete reinstall to resolve. All these commands must be run with root permissions.

3. Create a virtual network interface using an IP address that does not exist on a local subnet.

**For Ubuntu:**

```
sudo tee /etc/netplan/99-k8s-dummy.yaml <<EOF > /dev/null
network:
  version: 2
  bridges:
    dummy0:
      interfaces: []
      addresses: [ "<dummy IP>/32" ]
EOF
sudo chmod 0600 /etc/netplan/*.yaml
sudo netplan apply
```



You may receive a warning message. You can ignore this message and proceed to the next step.

**For RHEL:**

```
sudo nmcli connection add type dummy ifname dummy0 ipv4.method manual
ipv4.addresses <dummy IP>/32 ipv6.method disabled
```

4. Add an entry to the /etc/hosts file mapping the IP address of the dummy network interface to a simple hostname like "node".

Example:

```
echo '<dummy IP> node' | sudo tee -a /etc/hosts
```

## Prepare the RKE2 Configuration File

5. Add a configuration file for RKE2 **before** installing it so it takes effect when building the initial configuration. This will force the system to use the dummy IP address and hostname for the Kubernetes node, leaving you free to change your system's external IP address and hostname.

```
sudo mkdir -p /etc/rancher/rke2
sudo tee /etc/rancher/rke2/config.yaml <<EOF > /dev/null
node-name: node
node-ip: <dummy IP>
node-external-ip: <dummy IP>
EOF
```

Example:

```
sudo mkdir -p /etc/rancher/rke2
sudo tee /etc/rancher/rke2/config.yaml <<EOF > /dev/null
node-name: node
node-ip: 192.168.199.1
node-external-ip: 192.168.199.1
EOF
```



Further steps require additional changes to the configuration file, so be careful not to overwrite the file if it already exists.

6. **For RHEL only**, enable SELinux in the rke2 config file:

```
echo "selinux: true" | sudo tee -a /etc/rancher/rke2/config.yaml > /dev/null
```

7. You **must** configure RKE2 to disable the default ingress module **before** installing in an air gapped environment. Failure to do so will result in the ThreatQ installation hanging later.

```
sudo tee -a /etc/rancher/rke2/config.yaml <<EOF> /dev/null
disable:
- rke2-ingress-nginx
```

```
EOF
```

## Change the Kubernetes Subnet (Optional)



By default, RKE2 uses the 10.42.0.0/15 subnet for container and service networking. If that subnet is used for your local network, you may want to configure RKE2 to use a different subnet.

See the [RKE2 server configuration options](#) for cluster-cidr, service-cidr, and cluster-dns.optional.

## Set Up kubectl

8. Run the following command to add RKE2 and associated utilities:

```
sudo tee /etc/profile.d/rke2.sh <<EOF > /dev/null
export PATH="\$PATH:/var/lib/rancher/rke2/bin"
EOF
source /etc/profile.d/rke2.sh
```



During the installation of RKE2, restart the host system right after you enable the rke2-server.service and before you start it.

9. Install RKE2 as a Server Node on a systemd-based system using the steps in the [RKE2 Air-Gap Install guide](#).



If you are using RKE2 on a RHEL system with SELinux enabled you **MUST** install the [rke2-selinux package](#) prior to starting the rke2-server service. This is done automatically if RKE2 is installed via RPM but **NOT** if it is installed via tarball.

## Verify Your RKE2 Installation



The following steps must be completed using a non-root user account.

- After the RKE2 installation is complete, copy the RKE2 kubeconfig file to your home directory and set the appropriate permissions. This enhances security by restricting access to the kubeconfig file.

**Example:**

```
mkdir -p ~/.kube
sudo cp /etc/rancher/rke2/rke2.yaml ~/.kube/config
sudo chmod 600 ~/.kube/config
sudo chown <non-root username>:<non-root username> ~/.kube/config
```

- Run the following command to check the status of your pods:

```
kubectl get pods -A
```

**Example - Successful Output:**

NAMESPACE	NAME	READY	STATUS	RESTARTS	AGE
kube-system	cloud-controller-manager-node	1/1	Running	3 (23m ago)	34m
kube-system	etcd-node	1/1	Running	0	34m
kube-system	helm-install-rke2-canal-hfgqz	0/1	Completed	0	35m
kube-system	helm-install-rke2-coredns-58ssq	0/1	Completed	0	35m
kube-system	helm-install-rke2-ingress-nginx-8w876	0/1	Completed	0	35m
kube-system	helm-install-rke2-metrics-server-csrnh	0/1	Completed	0	35m
kube-system	helm-install-rke2-snapshot-controller-crd-tcpsx	0/1	Completed	0	35m
kube-system	helm-install-rke2-snapshot-controller-t9x67	0/1	Completed	1	35m
kube-system	helm-install-rke2-snapshot-validation-webhook-qwsxp	0/1	Completed	0	35m
kube-system	kube-apiserver-node	1/1	Running	0	34m
kube-system	kube-controller-manager-node	1/1	Running	3 (23m ago)	35m
kube-system	kube-proxy-node	1/1	Running	0	34m
kube-system	kube-scheduler-node	1/1	Running	3 (23m ago)	34m
kube-system	rke2-canal-g7mfc	2/2	Running	0	34m
kube-system	rke2-coredns-rke2-coredns-84b9cb946c-r79rv	1/1	Running	0	34m
kube-system	rke2-coredns-rke2-coredns-autoscaler-b49765765-8d6k8	1/1	Running	0	34m
kube-system	rke2-ingress-nginx-controller-tph5x	1/1	Running	0	32m
kube-system	rke2-metrics-server-655477f655-glq7m	1/1	Running	0	33m
kube-system	rke2-snapshot-controller-59cc9cd8f4-s262d	1/1	Running	2 (23m ago)	33m
kube-system	rke2-snapshot-validation-webhook-54c5989b65-mw5hf	1/1	Running	0	33m

root@dc01-threatq-v6-01:~#

## Air Gapped Installation

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

- Use the following link format to download the appropriate ThreatQ install tarball:



You will be prompted to enter your YUM credentials.



**STIG Install Note:**

Download ThreatQ from another system. FIPS will not allow you to download ThreatQ. After you download ThreatQ from another system, copy it to the /root/ directory.

```
https://install-v6.threatq.com/<version>-platform.tar.gz
```

You can also download the tarball using a curl command:

```
curl https://<YUM_USER>:<YUM_PASSWORD>@install-v6.threatq.com/
<version>-platform.tar.gz -O
```

13. Download the tqadmin file.



#### STIG Install Note:

Download TQAdmin from another system. FIPS will not allow you to download TQAdmin. After you download TQAdmin from another system, copy it to the /root/ directory.

Ubuntu:

```
curl -fO -u <YUM_USER> https://install-v6.threatq.com/tqadmin.deb
```

RHEL:

```
curl -fO -u <YUM_USER> https://install-v6.threatq.com/tqadmin.rpm
```

14. Open the CLI of the device you will install ThreatQ on and copy the install tarball and tqadmin package to /root using the SCP client of your choice.
15. Return to the CLI of the device and confirm that the install tarball and tqadmin package are present.
16. Install TQAdmin:



#### STIG and RHEL 8.10 Install Note:

For STIG installs and for non-STIG RHEL 8.10 installs, append --nodigest to the end of the TQAdmin install command.

Ubuntu:

```
sudo dpkg -i tqadmin.deb
```

RHEL:

```
sudo rpm -Uvh tqadmin.rpm
```

17. For RHEL installs, run the following command to install iptables:

RHEL:

```
sudo dnf install iptables-nft
```

18. Run the following command to provision your deployment:

```
sudo /usr/local/bin/tqadmin configure
```

PROMPT	DESCRIPTION
Do you want to enable OpenDXL (TQX)? (yes/no)	Enter yes to enable ThreatQ Data Exchange's OpenDXL functionality. Enter no to disable this functionality.
Do you want to enable the embedded TAXII server? (yes/no)	Enter yes to enable ThreatQ Data Exchange's TAXII server functionality. Enter no to disable this functionality.
Do you want to use your own SSL certificate? (yes/no)	Enter yes to configure a custom SSL certification (not self-signed).
Enter the file path for your certificate	Enter the path for your SSL certificate. <b>example:</b> /etc/threatq-certs/mycert.pem
Enter the file path for your private key	Enter the path for the SSL certificate's private key. <b>example:</b> /etc/threatq-certs/mykey.pem
Do you want to enable CAC/mTLS? (yes/no)	Enter yes to configure SSL Client Certificate Authentication.
Enter the file path for your certificate	Enter the path for your CA Certificate. <b>example:</b> /etc/threatq-certs/mycert.pem
Enter the FQDN of the server	Enter the FQDN of the server. <b>example:</b> myserver.threatq.com



#### STIG Install Notes:

Running the `tqadmin platform install` command may take longer than fifteen minutes and as such may trigger the timeout interval required by STIG. To prevent process interruption, a user will need to press the spacebar prior to each timeout. If this is not an option, you can use the following command to increase the timeout interval:

**RHEL 9.4:** `sudo sed -i 's/=600/=60000/g' /etc/profile.d/tmout.sh`

#### RHEL 8.10:

`sudo sed -i 's/600/60000/g' /etc/ssh/sshd_config`

`sudo systemctl restart sshd.service`

After you run this command, you must log out and log back in. After you complete the install process, run the following command to reinstate the timeout interval:



```
RHEL 9.4: sudo sed -i 's/=60000/=600/g' /etc/profile.d/tmout.sh
RHEL 8.10:
sudo sed -i 's/60000/600/g' /etc/ssh/sshd_config
sudo systemctl restart sshd.service
```

19. Run the following command to Install ThreatQ. You will be prompted for the location of the platform bundle if it is not in **/root**.

```
sudo /usr/local/bin/tqadmin platform install -v <ThreatQ version> -z
```



#### STIG Install Note:

If you disabled the fifteen minute timeout, after the TQAdmin install completes, run the following command to reinstate the timeout interval:

```
RHEL 9.4: sudo sed -i 's/=60000/=600/g' /etc/profile.d/tmout.sh
RHEL 8.10:
sudo sed -i 's/60000/600/g' /etc/ssh/sshd_config
sudo systemctl restart sshd.service
```

20. Run the following command to generate the initial password for the ThreatQ Admin user (username = admin):

```
sudo /usr/local/bin/tqadmin password
```

21. To verify your ThreatQ installation, check the status of the pods and services in your Kubernetes cluster.

```
kubectl get pods -A
kubectl get svc -A
```

22. List the ThreatQ pods:

```
kubectl get pods -n threatq
```

## Access Your New ThreatQ 6x Instance

23. Connect to the ThreatQ web interface, using the IP/hostname given during the installation.
24. Add the license key provided by ThreatQ Support.
25. Use the username admin and the password you generated.
26. Accept the EULA.
27. Opt in or out of sending analytics.

## Next Steps

See the Air Gapped Data Sync section of the Help Center for information on exporting data from your source ThreatQ 6x installation and importing it to your Target installation.

# Change Log



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

- **Version 1.3.3**
  - Added **Pin Your Ubuntu 22.04** Version section.
- **Version 1.3.2**
  - Added iptables as a prerequisite for RHEL installs.
- **Version 1.3.1**
  - Updated the curl command for downloading TQAdmin.
- **Version 1.3.0**
  - Updated the curl command for downloading TQAdmin.
  - Updated the command for configuring RKE2 to disable the default ingress module.
- **Version 1.2.0**
  - Added **Pin Your RHEL 9** Version section.
- **Version 1.1.0**
  - Updated the RHEL 8.10 command for enabling the timeout interval.
- **Version 1.0.9**
  - Minor update to code snippet format in the **Configure Internal Networking** section.
- **Version 1.0.8**
  - Added the **Supported Hardening Standards by Operating System** section.
- **Version 1.0.7**
  - Increased the / size listed in the **Dedicated Mount /opt** section.
- **Version 1.0.6**
  - Added security endpoint warning to prerequisites.
- **Version 1.0.5**
  - Updated partitioning requirements.
  - Updated SSL Certificate file path examples.
- **Version 1.0.4**
  - Updated partitioning recommendations.
  - Added timeout extension command for STIG install of RHEL 8.10.
- **Version 1.0.3**
  - Added support for STIG installs in RHEL 8.10 instances.
- **Version 1.0.2**
  - Added python3 dependency.
- **Version 1.0.1**
  - Added support for install in a RHEL 8.10 instance.
- **Version 1.0.0**
  - Initial Release