# ThreatConnect® Upgrade Guide: Containerized Deployment

## Software Version 7.7

### Technical Guide

September 25, 2024

10033-06 EN Rev. B

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 | F: 703.229.4489
www.ThreatConnect.com

# Table of Contents

# Overview

This guide describes how to upgrade ThreatConnect® on a ThreatConnect instance that is running in a containerized solution using Docker®.

**Important**: The containerized deployment was tested on AlmaLinux OS™ and is the preferred deployment method for all production and non-production systems starting with ThreatConnect version 7.5. For instructions on how to upgrade ThreatConnect and keep it running directly on an operating system (OS), see *ThreatConnect Upgrade Guide: Operating System*.

# Upgrade Steps

## Step 1: Restore Your Environment File

**Note**: You must complete this step on all hosts that run ThreatConnect or some component of ThreatConnect.

Restore your ThreatConnect Docker `.env` file (replace the placeholder `<//secure location>` value):

```
Unset
scp <//secure location>/.env /opt/threatconnect-docker/.env
```

## Step 2: Update the TC_VERSION Variable

**Note**: You must complete this step on all hosts that run ThreatConnect or some component of ThreatConnect.

Update `TC_VERSION` to the latest ThreatConnect version in your `.env` file (replace the `<version number>` placeholder value with the version number for the ThreatConnect version to which you are upgrading):

```
Unset
TC_VERSION=v<version number>
```

## Step 3: Add New Environment Variables

**Note**: You must complete this step on all hosts that run ThreatConnect or some component of ThreatConnect.

Add and configure the following variables in your `.env` file:

```
Unset
# TC Logs folder. Set an absolute path, create if not exist, owned by user 1000
TC_MON_LOGS=/opt/threatconnect-docker/logs/tc-mon
TC_APP_LOGS=/opt/threatconnect-docker/logs/tc-app
TC_JOB_LOGS=/opt/threatconnect-docker/logs/tc-job
# TC Memory Limits.
TC_MON_MEM=12G
TC_APP_MEM=6G
TC_JOB_MEM=12G
# OpenSearch Java Options. Xms (initial) and Xmx (maximum) must be equal.
OPENSEARCH_JAVA_OPTS=-Xms6g -Xmx6g
# Redis server arguments
REDIS_ARGS=--maxmemory 6G --maxmemory-policy allkeys-lru --maxmemory-samples 5
```

# Step 4: Upgrade Docker Files

**Note**: You must complete this step on all hosts that run ThreatConnect or some component of ThreatConnect.

Upgrade the ThreatConnect Docker ZIP file to the latest version (replace the `<version number>` placeholder value with the version number for the ThreatConnect version to which you are upgrading). Note that you should let the `unzip` command replace everything except for `nginx.conf`, `opensearch_internal_users.yml` and `postgres.conf`, as you may have local changes to those files.

```
Unset
cd /opt
unzip /tmp/threatconnect-docker-v<version number>.zip
```

# Step 5: Fix Shell Scripts

**Note**: You must complete this step on all hosts that run ThreatConnect or some component of ThreatConnect.

Reformat and change permissions on shell scripts:

```
Unset
cd /opt/threatconnect-docker
sed -i 's/\r$//' load_schema.sh
chmod 755 load_schema.sh
sed -i 's/\r$//' docker-entrypoint.d/00_init.sh
chmod 755 docker-entrypoint.d/00_init.sh
sed -i 's/\r$//' docker-entrypoint.d/98_custom_ca.sh
chmod 755 docker-entrypoint.d/98_custom_ca.sh
sed -i 's/\r$//' docker-entrypoint.d/99_deploy.sh
chmod 755 docker-entrypoint.d/99_deploy.sh
```

## Step 6: Log Into ThreatConnect's ECR

Log into ThreatConnect's Elastic® Container Registry (ECR). If located in Europe, replace `us-east-1` with `eu-central-1` before running the following commands:

```
Unset
docker login \
  -u AWS \
  -p $(/usr/local/bin/aws ecr get-login-password --region us-east-1) \
  373319941383.dkr.ecr.us-east-1.amazonaws.com
```

## Step 7: Stop and Remove Containers

Run the following command to stop and remove the service containers:

```
Unset
docker-compose rm -fs redis opensearch tc-mon tc-app tc-job
```

## Step 8: Start OpenSearch

**Note**: You must complete this step on the host that runs OpenSearch.

1. Start OpenSearch:

```
Unset
docker-compose up -d opensearch
```

2. Test the installation (replace the `<opensearch password>` placeholder value):

```
Unset
curl -sku admin:<opensearch password>
https://localhost:9200/_cat/indices/orgs?v
```

# Step 9: Start ThreatConnect

Start each of the following services in the following order: **tc-mon** → **tc-app** → **tc-job**. After starting each service, make sure to perform the following actions:

- Run `docker-compose logs --tail=10 --follow` to verify the service starts up before moving on to the next.
- Press **Ctrl+C** once the service is started.

## Start tc-mon

**Note**: You must complete this step on the host that runs the ThreatConnect messaging server.

Run the following command to start **tc-mon**:

```
Unset
docker-compose up -d redis tc-mon
```

## Start tc-app

**Note**: You must complete this step on the host that runs the ThreatConnect application server.

Run the following command to start **tc-app**. Note that `nginx` is required only if you are on a host other than **tc-mon**.

```
Unset
docker-compose up -d tc-app
```

## Start tc-job

**Note**: You must complete this step on the host that runs the ThreatConnect Playbooks server.

Run the following command to start **tc-job**:

```
Unset
docker-compose up -d tc-job
```

# Step 10: Monitor ThreatConnect

Follow these steps to restart and monitor the ThreatConnect containers without an `.env` file in place:

1. Move your `.env` file to a secure location (e.g., a server where passwords are stored).
2. Docker Compose commands cannot be run without an `.env` file in place. Therefore, run the following command to check the status of the ThreatConnect containers. Note that the container names are in the first column.

```
Unset
docker ps --format "table {{.Names}}\t{{.Image}}\t{{.Status}}"
```

3. Restart the ThreatConnect containers (replace all `<container name>` placeholder values):

```
Unset
docker restart <container name> <container name>
```

4. Tail monitor the ThreatConnect logs:

```
Unset
docker ps --format "table {{.Names}}" | grep -e "mon\|app\|job" | xargs -L 1 -P
`docker ps | wc -l` docker logs --since 15m -f
```

# Step 11: Re-Create Search Index

1. Log into ThreatConnect with a System Administrator account.
2. Hover over **Settings** on the top navigation bar and select **System Settings**.
3. Click **CREATE SEARCH INDEX** at the top right of the **Settings** tab.
4. On the **Setup** tab of the **Search Index Configuration** window, select the **Perform search indexing on database source** and **Load file contents into search index** checkboxes, and then click **INITIALIZE**.

   **Note**: The **Perform search indexing on database source** checkbox determines whether to index objects that exist in the ThreatConnect database, and the **Load file contents into search index** checkbox determines whether to index objects that exist in document storage.