How to Install Track on Premise (ToP) - Step-by-Step Guide

safectory GmbH

1 Foreword **2**

2 Virtual Machine Setup for Track On Premise (Debian/Ubuntu) **2**
- 2.1 Prerequisites for VM Setup . . . 2
- 2.2 Step 1: Create the Virtual Machine in VirtualBox . . . 2
- 2.3 Step 2: Configure Hardware (Adhering to Server Requirements) . . . 3
- 2.4 Step 3: Create Virtual Hard Disk . . . 3
- 2.5 Step 4: Configure Network (Bridged Adapter for Direct Network Access) . . . 4
- 2.6 Step 5: Boot and Install Debian/Ubuntu Server . . . 5
- 2.7 Step 6: Initial Server Configuration & SSH Access . . . 6
- 2.8 Step 7: Setup Uncomplicated Firewall (ufw) . . . 6

3 Installing Safectory "Track on Premise" Software **8**
- 3.1 Installation Checklist . . . 8
- 3.2 Prerequisites for ToP Installation . . . 9
- 3.3 Step 1: Download and Run the Installer . . . 9
  - 3.3.1 Option 1: Simplified one-liner (Recommended): . . . 9
  - 3.3.2 Option 2: Download directly from Nexus and install: . . . 10
  - 3.3.3 Option 3: If you already have the installation package (`install_track_on_premise.tar.gz`) on the server: . . . 11
- 3.4 Step 2: Follow On-Screen Prompts from the Installer . . . 11
- 3.5 Step 3: Test Your Installation . . . 12
- 3.6 Step 4: Certificate Management . . . 12

4 Updating Safectory "Track on Premise" **13**
- 4.1 Update Checklist . . . 13
- 4.2 Step 1: Navigate to the directory where the script is located (typically `/root/`) and execute it: . . . 13
- 4.3 Step 2: The update script will present several prompts: . . . 14
- 4.4 Step 3: Once the update process is complete, the script will confirm. . . . 14

5 Managing Safectory "Track on Premise" **14**
- 5.1 Backups and Database Restore . . . 14
- 5.2 Uninstalling Safectory "Track on Premise" . . . 15
- 5.3 Troubleshooting . . . 16
- 5.4 Need Help? . . . 17

1 Foreword

This documentation provides comprehensive information on how to set up the Safectory Track on Premise (ToP) solution. It covers creating a suitable virtual machine (VM) based on Safectory's Track On Premise Server Requirements documentation, and the subsequent installation of the ToP software.

Important Notes:

- While this guide focuses on a Virtual Machine setup, the ToP solution can also be installed on a *physical server* running a compatible Linux distribution (Debian/Ubuntu). The OS installation and ToP software installation steps will be largely similar.
- The ToP installer expects a supported system (see Safectory's Track On Premise Server Requirements documentation) in **minimal configuration**, that is, **no additional packages** and **no other services** installed other than the ones provided by the base operating system.

2 Virtual Machine Setup for Track On Premise (Debian/Ubuntu)

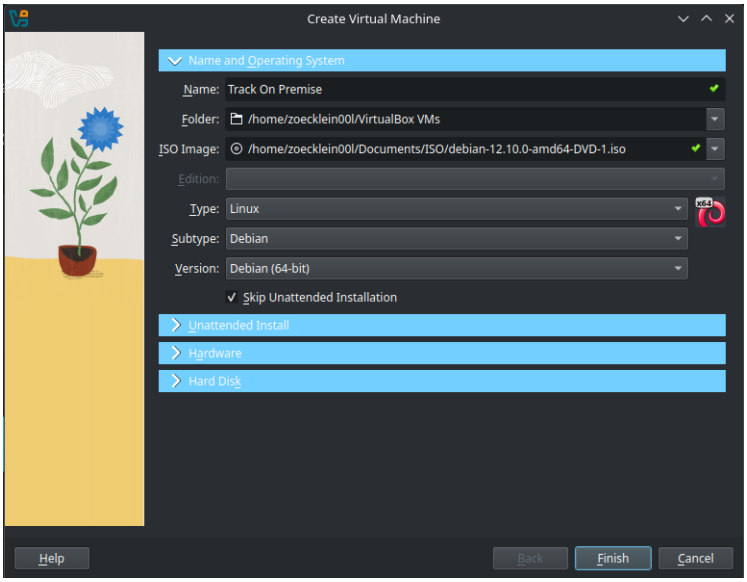
This section walks you through configuring a Debian-based or Ubuntu-based Oracle VirtualBox virtual machine, optimized for **Track On Premise**. This includes hardware allocation, networking, and initial OS setup.

2.1 Prerequisites for VM Setup

- **VirtualBox**: Ensure you have the latest version of Oracle VirtualBox installed on your host machine.
- **Debian or Ubuntu Server ISO**:
  - Debian: `debian-12.10.0-amd64-DVD-1.iso` (or a newer stable version).
  - Ubuntu Server: `ubuntu-24.04.2-live-server-amd64.iso` (or a newer LTS version).
- **Disk Space**: At least 50GB of free disk space on your host machine for the VM's virtual hard disk.
- **Familiarity**: Basic understanding of VM creation and Linux installation is beneficial. For beginners, refer to the official VirtualBox and Debian/Ubuntu installation guides.

2.2 Step 1: Create the Virtual Machine in VirtualBox

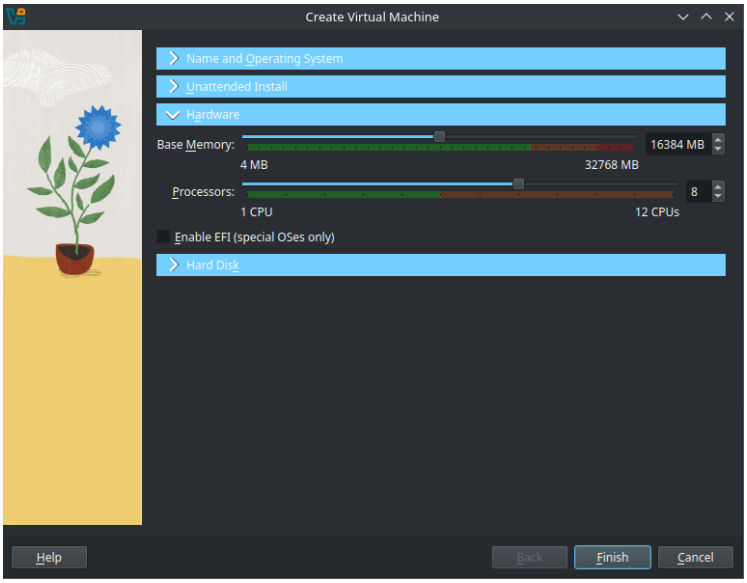
1. Open VirtualBox and click **New**.
2. Fill in the VM details:
   - **Name**: `Track On Premise` (or a name of your choice)
   - **Folder**: Choose your preferred storage location for VM files.
   - **ISO Image**: Select the downloaded Debian or Ubuntu Server ISO file.
   - **Type**: `Linux`
   - **Version**: `Debian (64-bit)` or `Ubuntu (64-bit)` (VirtualBox often auto-detects this from the ISO).
   - Check **Skip Unattended Installation** to have full control over the setup process.



2.3 Step 2: Configure Hardware (Adhering to Server Requirements)

1. **Memory (RAM)**: Allocate **16384 MB (16 GB)**.
2. **Processors**: Assign **8 CPUs**.

   Note: These are recommended minimums. Adjust based on your specific load and the official server requirements.

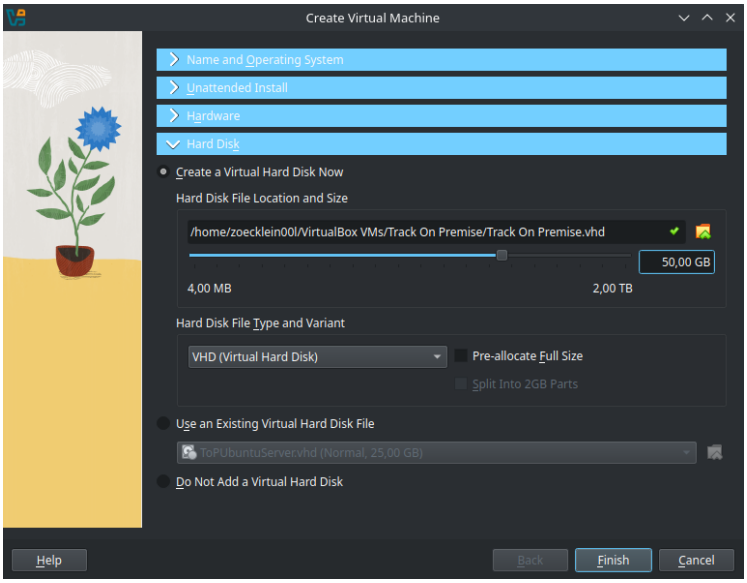


2.4 Step 3: Create Virtual Hard Disk

1. Select `Create a Virtual Hard Disk Now`.
2. Configure the virtual hard disk:
   - **Location**: Default is usually fine (e.g., `~/VirtualBox VMs/Track On Premise/Track On Premise.vdi`).
   - **File Size**: **50.00 GB** (or more, as per server requirements and expected data volume). This refers to the size of the virtual disk for the VM, not just free space on the host.
   - **Hard disk file type**: `VHD (Virtual Hard Disk)` is generally recommended, `VDI (VirtualBox Disk Image)` but is also acceptable.

- **Storage on physical hard disk**: `Dynamically allocated` is usually fine for flexibility, or `Fixed size` (Pre-allocate full size) for potentially better performance.

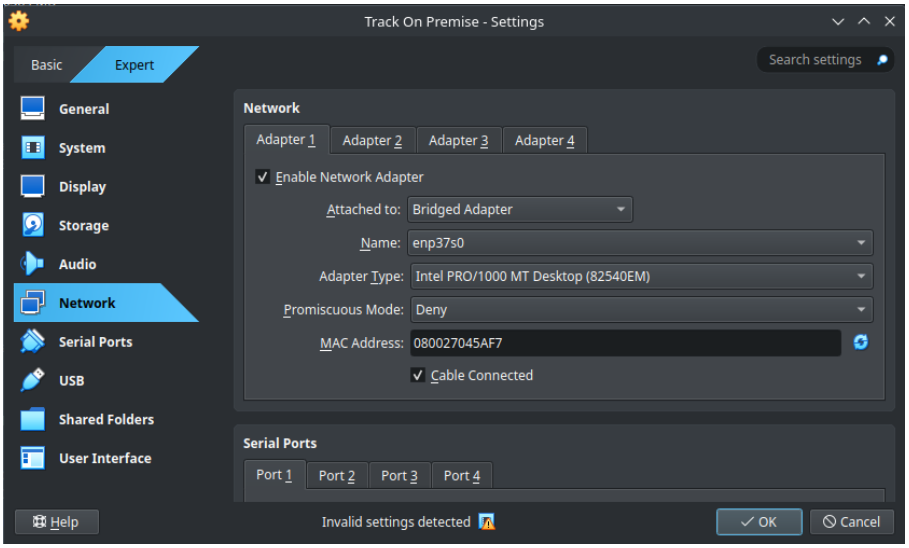
3. Click **Finish**.



2.5 Step 4: Configure Network (Bridged Adapter for Direct Network Access)

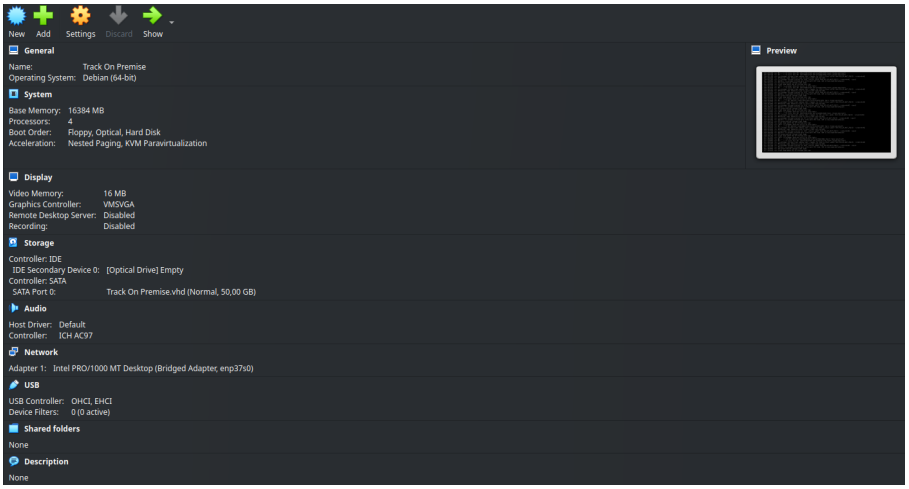
For the VM to be accessible on your local network (e.g., for SSH and ToP services), a bridged adapter is recommended.

1. With the `Track On Premise` VM selected, go to **Settings** > **Network**.
2. **Adapter 1**:
   - Enable Network Adapter.
   - **Attached to**: Select `Bridged Adapter`.
   - **Name**: Choose your host machine's active network interface (e.g., `enp37s0` on Linux, `Ethernet` on Windows/macOS).
     - *To find your host interface name on Linux, you can use `ip addr` or `nmcli device status` in a terminal. On Windows, check Network Connections. On macOS, check Network System Preferences.*
   - **Adapter Type**: `Intel PRO/1000 MT Desktop (82540EM)` (or a compatible default).
   - Under **Advanced**:
     - Ensure **Cable Connected** is checked.
3. Click **OK**.



2.6 Step 5: Boot and Install Debian/Ubuntu Server

1. Start the `Track On Premise` VM. It should boot from the selected ISO image.
2. Follow the on-screen instructions to install Debian or Ubuntu Server:
   - **Language, Location, Keyboard**: Select your preferences.
   - **Hostname**: e.g., `top-server`.
   - **Domain Name**: (Optional, can be left blank if not applicable).
   - **User Setup**: Create a non-root user and a strong password.
   - **Partitioning**:
     - Choose **Guided - use entire disk** (or "Guided - use entire disk and set up LVM" for more flexibility if you're comfortable with it). This is generally the simplest for a dedicated VM.
     - Confirm partitioning scheme.
   - **Software Selection**:
     - For Debian: Deselect any desktop environment. Ensure **SSH server** and **standard system utilities** are selected.
     - For Ubuntu Server: Choose the default server profile. OpenSSH server should be installed by default or offered as an option.
   - **GRUB Bootloader**: Install GRUB to the master boot record (usually the primary virtual disk).
3. Once the installation is complete, the system will reboot. Remove the ISO from the virtual CD/DVD drive if prompted or through VM settings to boot from the virtual hard disk.

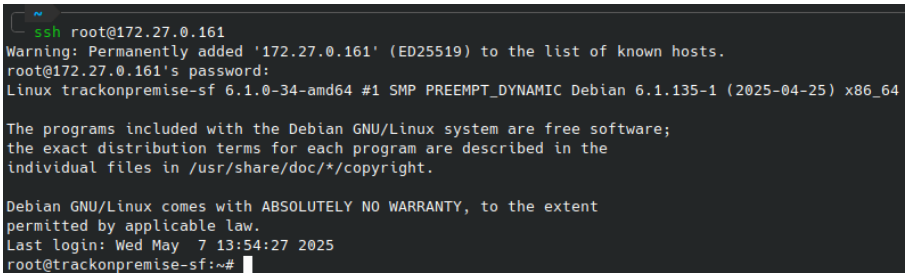


2.7 Step 6: Initial Server Configuration & SSH Access

1. Log in to the VM console using the credentials you created during installation.
2. **Obtain IP Address**: Find your VM's IP address using the command `ip a`. Look for an IP address associated with your primary network interface (e.g., `enp0s3` or `eth0`). It should be an IP address from your local network (e.g., `192.168.1.X` or `172.27.0.161`). *Note: The interface name inside the VM (e.g., `enp0s3`) might differ from your host's interface name (e.g., `enp37s0`). This is normal.*

3. **Test SSH from Host**: From your host machine's terminal (not the VM console), SSH into the server:

```
ssh root@<VM_IP_ADDRESS>
```



4. **(Optional but Highly Recommended) Enable Root SSH Login (Temporarily for Setup if Needed) & Key-Based Authentication**:
   - While direct root SSH login is generally discouraged for security, it might be required by some installation scripts or for initial setup convenience. If you need to enable it temporarily:

     ```
     sudo nano /etc/ssh/sshd_config
     ```

     Change `PermitRootLogin prohibit-password` or `#PermitRootLogin prohibit-password` to `PermitRootLogin yes`. Save and exit. Then restart SSH & SSHD: `systemctl restart ssh`, `systemctl restart sshd`.
   - **Security Best Practice**: For long-term secure access, set up SSH key-based authentication and disable password authentication (including for root). This is more secure than using passwords.

2.8 Step 7: Setup Uncomplicated Firewall (ufw)

Execute the following commands as `root` or using `sudo`.

1. **Install `ufw`** (if not already installed):

```
sudo apt install ufw -y
```

2. **Set Default Policies**: Deny all incoming traffic by default and allow all outgoing traffic by default (a common starting point).

```
sudo ufw default deny incoming
sudo ufw default allow outgoing # Allows server to initiate connections (e.g., for updates)
```

3. **Add Specific Allow Rules**: You need to allow traffic for SSH, the ToP application (HTTP/HTTPS), and any other necessary services like Nexus.

   - **SSH Access** (replace `<your_client_IP_or_network>` with the specific IP or network range that needs SSH access, or `any` if access from any IP is acceptable but less secure):

   ```
   sudo ufw allow from <your_client_IP_or_network> to any port 22 \
     proto tcp comment 'Allow SSH access'
   ```

     – Example for a specific IP:

   ```
   sudo ufw allow from 192.168.1.100 to any port 22 proto tcp comment 'Allow SSH from my workstation'
   ```

     – Example for a local network:

   ```
   sudo ufw allow from 192.168.1.0/24 to any port 22 proto tcp comment 'Allow SSH from local network'
   ```

     – If you only need SSH from any IP (less secure):

   ```
   sudo ufw allow 22/tcp comment 'Allow SSH access'
   ```

   - **Track on Premise Frontend Access (HTTP & HTTPS)** (replace `<your_client_IP_or_network>` with the IP/network that should access the ToP frontend, or `any` if it should be publicly accessible):

   ```
   sudo ufw allow from <your_client_IP_or_network> to any port 80 \
     proto tcp comment 'Allow HTTP for ToP'
   sudo ufw allow from <your_client_IP_or_network> to any port 443 \
     proto tcp comment 'Allow HTTPS for ToP'
   ```

     – If ToP should be accessible from any IP:*

   ```
   sudo ufw allow 80/tcp comment 'Allow HTTP for ToP'
   sudo ufw allow 443/tcp comment 'Allow HTTPS for ToP'
   ```

   - **Track on Premise Additional Ports**:

   ```
   # sudo ufw allow out to any port 6555 proto tcp comment 'ToP BLE Data Input'
   # sudo ufw allow out to any port 6556 proto tcp comment 'ToP BLE Data Input'
   ```

   - **Outbound Access to Safectory Nexus Repository**: The ToP installer needs to download packages from `nexus.safectory.com` (IP: `91.250.82.47`) on port `8443`.

   ```
   sudo ufw allow out to 91.250.82.47 port 8443 \
     proto tcp comment 'Allow outbound to Safectory Nexus'
   ```

   - **Outbound DNS Access**

   ```
   sudo ufw allow out 53/udp comment 'Allow outbound DNS (UDP)'
   sudo ufw allow out 53/tcp comment 'Allow outbound DNS (TCP)'
   ```

4. **Enable Firewall**:

   ```
   sudo ufw enable
   ```

   Confirm with `y` when prompted.

5. **Check Status**:

   ```
   sudo ufw status numbered
   sudo ufw status verbose
   ```

Make sure your SSH port rule is active before enabling, or you might lock yourself out if connecting remotely!

3 Installing Safectory “Track on Premise” Software

3.1 Installation Checklist

- **Prerequisites**
  - **Pre-installation materials received**:
    - ☐ Installation script.
    - ☐ Installation guide: `ToP_manual.md`.
    - ☐ Server requirement documentation.
  - **Server Setup**:
    - ☐ Server configured with a minimal OS installation (Debian/Ubuntu).
    - ☐ No additional packages or services other than the base OS ones are installed.
    - ☐ Refer to the appropriate system-requirements table for the estimated size:
      - ☐ Allocate sufficient CPU cores according to the selected size.
      - ☐ Allocate sufficient RAM [GB] according to the selected size.
      - ☐ Allocate sufficient SSD [GB] according to the selected size.
  - **Network and Access**:
    - ☐ Server has internet access, especially to Safectory’s Nexus repository.
    - ☐ Domain name or static IP address determined for ToP instance.
    - ☐ BLE gateways are configured with the correct domain name or IP address.
    - ☐ Nexus username and password provided by Safectory.
    - ☐ Root access is available, and `su -` is used for proper `PATH` environment information.
    - ☐ **bash** is the current shell.
    - ☐ All required ports are open and not occupied:
      - Internal: 6555, 6556.
      - Inbound: 443, 80.
      - Outbound: 8443.
      - Outbound (for PostgreSQL installation):

      `deb http://apt.postgresql.org/pub/repos/apt $(lsb_release -cs)-pgdg main`.

- **Installation Process**
  - ☐ **Option 1 (Simplified one-liner - Recommended)**:
    - ☐ Execute `wget -O - https://safectory.com/top | bash` as `root`.
    - ☐ Provide Nexus credentials if prompted (skipped if already in `/etc/track.config`).
  - ☐ **Option 2 (Download from Nexus)**:
    - ☐ Execute the one-liner command as `root`.
    - ☐ Provide Nexus username and password when prompted.
  - ☐ **Option 3 (Package is on server)**:
    - ☐ Run `tar -xzvf install_track_on_premise.tar.gz -C /`.
    - ☐ Change to the `/root` directory.
    - ☐ Run `chmod +x install_track_on_premise.sh`.
    - ☐ Execute the script with `./install_track_on_premise.sh`.
  - ☐ **Installer Prompts**:
    - ☐ Re-enter Nexus credentials (if not already provided).
    - ☐ Enter the domain name or IP address for the ToP instance.
    - ☐ Select the application use case (e.g., “asset-tracking” or “tamper-safe beacon”).
    - ☐ Select the installation size (e.g., “Tiny”, “Small”).
    - ☐ Log in to TrackUI with `admin` / `changeme` and immediately set a new admin password before productive use.

- **Post-Installation Verification**

- ☐ **Test with `curl`**:
  - ☐ Run `curl -k https://your_top_domain_or_IP` from the server.
  - ☐ Expect HTML output.
- ☐ **Test with a web browser**:
  - ☐ Navigate to `https://your_top_domain_or_IP`.
  - ☐ Expect to see the ToP login page.
  - ☐ (If using a non-public domain) Add the virtual machine's IP address and domain name to your local machine's `hosts` file.
- ☐ **Check service status**:
  - ☐ Check Track service:
    - `systemctl status prodtrac.service`
    - expected: `Active: active (running)`
  - ☐ Check NGINX/OpenResty service:
    - `systemctl status nginx.service` (Debian) or
    - `systemctl status openresty.service` (Ubuntu)
    - expected: `Active: active (running)`
  - ☐ Check PostgreSQL service:
    - `systemctl status postgresql@15-main.service`
    - expected: `Active: active (running)`

3.2 Prerequisites for ToP Installation

- **Configured Server**: A Debian/Ubuntu server (physical or VM) meeting the system requirements.
- **Network Access**: The server must have internet access, particularly to Safectory's Nexus repository.
- **Domain Name or IP Address**: The domain name (e.g., `https://top.yourcompany.com`) or static IP address that will be used to access your ToP instance. You will either need a resolving domain name (resolving in the configured DNS of the server and the BLE gateways) or an IP address for Track-on-Premise to use. This domain name or the IP address must be configured on the BLE gateways to send the data as well.
- **Certificate**: Self-signed certificates are supported and must be provided in the webserver Nginx configuration. After running the ToP installer, this can be controlled via the ssl_certificate and the ssl_certificate_key directives in the server context of file `/etc/nginx/sites-enabled/001-trac-ssl`.
- **Nexus Credentials**: A username and password for Safectory's Nexus repository, provided by Safectory.
- **Root Access**: The installation script typically requires root privileges.

3.3 Step 1: Download and Run the Installer

Log in to your server as `root` or a user with `sudo` privileges. If not root, prepend `sudo` to the commands or use `sudo -i`.

If your environment requires a proxy, configure it with variables before running installer commands: `TOP_NO_PROXY` is a comma-separated bypass list (e.g., `localhost,127.0.0.1,.internal.example.com,10.0.0.0/8`), so those targets are reached directly while everything else uses `TOP_PROXY_URL`.

3.3.1 Option 1: Simplified one-liner (Recommended):

This is the simplest installation method. Run this single command as **root**:

```
wget -O - https://safectory.com/top | bash
```

Proxy variant (optional):

```
TOP_PROXY_URL="http://<proxy-host>:<proxy-port>" \
TOP_NO_PROXY="localhost,127.0.0.1,<internal-hosts>" \
bash -c 'wget -O - https://safectory.com/top | bash'
```

- **How it works**:
  - Downloads and executes a jump script that handles the entire installation process
  - Automatically checks for existing Nexus credentials in `/etc/track.config` and only prompts for Nexus credentials if not found
  - Downloads the installer package and runs it with all interactive prompts as usual

3.3.2 Option 2: Download directly from Nexus and install:

Use this option if `safectory.com` is unreachable or if you need to download from a specific Nexus repository.

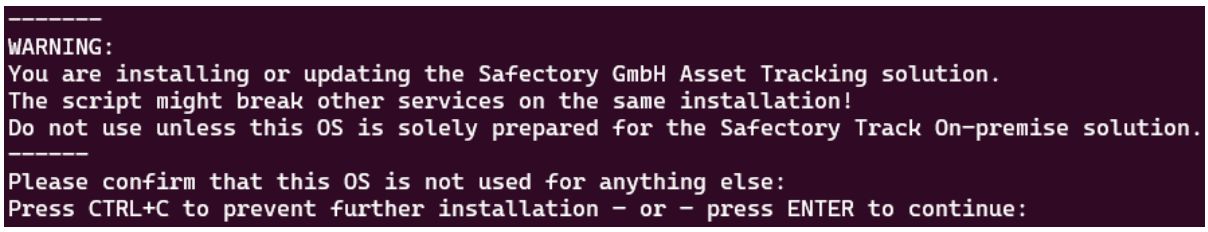
Run this one-liner command as **root** (or adapt for `sudo`):

```
TAR_GZ_URL="https://nexus.beamzone.net:8443/repository/\
safectory_on_premise/install_track_on_premise.tar.gz" \
  && apt-get -y install curl \
  && read -p "Enter Nexus username: " username \
  && read -s -p "Enter Nexus password: " password && echo \
  && curl -u "$username:$password" -L -o /root/install_track_on_premise.tar.gz "$TAR_GZ_URL" \
  && tar -xzvf /root/install_track_on_premise.tar.gz -C / \
  && cd /root && chmod +x install_track_on_premise.sh \
  && bash install_track_on_premise.sh
```

Proxy variant (optional):

```
TOP_PROXY_URL="http://<proxy-host>:<proxy-port>" \
TOP_NO_PROXY="localhost,127.0.0.1,<internal-hosts>" \
bash -c '
TAR_GZ_URL="https://nexus.beamzone.net:8443/repository/\
safectory_on_premise/install_track_on_premise.tar.gz" \
  && apt-get -y install curl \
  && read -p "Enter Nexus username: " username \
  && read -s -p "Enter Nexus password: " password && echo \
  && curl -u "$username:$password" -L -o /root/install_track_on_premise.tar.gz "$TAR_GZ_URL" \
  && tar -xzvf /root/install_track_on_premise.tar.gz -C / \
  && cd /root && chmod +x install_track_on_premise.sh \
  && bash install_track_on_premise.sh'
```

After executing this, the following lines may appear, indicating the script is about to run. Proceed by pressing `Enter` if prompted by a confirmation like the one shown:



- **Note**:
  - This script requires Bash version 2.0 or higher, which is standard on modern Linux distributions.*
  - The script first attempts to install `curl` if not present. Then, it prompts for your Nexus username and password to download the installer package.

    ```
    Enter Nexus username:
    Enter Nexus password:
    ```

  - If you encounter errors during installation, please refer to section Troubleshooting.

3.3.3 Option 3: If you already have the installation package (`install_track_on_premise.tar.gz`) on the server:

1. Navigate to the directory containing the package.
2. Extract and run the installer:

```
tar -xzvf install_track_on_premise.tar.gz -C /
cd /root # The scripts are typically extracted here
chmod +x install_track_on_premise.sh uninstall_track_on_premise.sh
bash install_track_on_premise.sh
```

3. The same package also contains `uninstall_track_on_premise.sh` for complete removal of a ToP installation.

3.4 Step 2: Follow On-Screen Prompts from the Installer

Once `install_track_on_premise.sh` is running, it will guide you through the installation process with several prompts.

- You will be prompted to enter your **Nexus credentials** again. These are used by the installer script itself.

```
Configuration file /etc/track.config not found, will ask questions during installation...
Please enter the customer's Nexus user (example: company name) and press ENTER:

Please enter the customer's Nexus password and press ENTER:
```

- You will need to enter your **domain name** for the ToP instance (e.g., `https://top.yourcompany.com` or `https://subdomain.example.com`).

```
Please enter the report URL including the protocol (example: https://track.safectory.com):
```

- The installer will ask for other configuration details, such as the **application use case** and the **installation size**. Read prompts carefully and select the appropriate option based on your server's resources and expected load. Example when picking the **"tamper-safe beacon"** application use case and the **tiny** installations size:

```
Please select the application type for this installation:
  * asset-tracking [1] (= default)
  * tamper-safe-beacons [2]
2
```

```
Please enter the size for this installation:
  * demo [1]
  * tiny [2] (= default; up to 100 devices and 8 GiB of RAM)
  * small [3]
  * medium [4]
  * large [5]
2
```

  - *Note: Please refer to the Server Requirements Documentation for detailed information about choosing the correct installation size.*

- At the end of a successful installation, the initial TrackUI admin password is set to `changeme`. **Change this password before switching to productive use.**

```
Setting admin (TracUI user) password...
IMPORTANT: The initial admin password is 'changeme'.
Change it before switching to productive use.

Installation finished.
```

3.5 Step 3: Test Your Installation

1. **Using `curl` (from server or another machine on the network):** Replace `your_top_domain_or_IP` with the domain name or IP address you configured.

   ```
   curl -k https://your_top_domain_or_IP
   ```

   - The `-k` (or `--insecure`) flag for `curl` tells it to allow connections to SSL sites without verifying the certificate. This is useful if the installation uses a self-signed certificate initially. You should see HTML output if the server is responding.

2. **Using a Web Browser:** Open a web browser on a machine that can access the server and navigate to:

   ```
   https://your_top_domain_or_IP
   ```

   You should see the ToP login page. You might get a browser warning about an untrusted certificate if it's self-signed or not yet configured with a valid CA certificate.

   DNS / Hosts File Note: If you are using a domain name that is not yet publicly resolvable via DNS (or for testing purposes), you might need to add an entry to your local machine's `hosts` file to point the domain name to your ToP server's IP address.

   - **Linux/macOS**: Edit `/etc/hosts`
   - **Windows**: Edit `C:\Windows\System32\drivers\etc\hosts` (requires administrator privileges)
   - Example entry:

     ```
     <VM_IP_ADDRESS> your_top_domain.com
     ```

     (e.g., `192.168.1.123 https://top.yourcompany.com`)

3.6 Step 4: Certificate Management

To properly allow HTTPS requests between clients and the backend, one needs to make sure that Nginx/OpenResty is aware of the SSL certificate and its corresponding secret key (both in PEM format). This can be controlled via the `ssl_certificate` and the `ssl_certificate_key` directives in the `server` context of file:

- *Debian*: `/etc/nginx/sites-enabled/001-trac-ssl`
- *Ubuntu*: `/usr/local/openresty/nginx/conf/sites-enabled/001-trac-ssl`

An example for those two directives may look as follows:

```
server {
    ...
    ssl_certificate     /etc/ssl/certs/crt.pem;
    ssl_certificate_key /etc/ssl/private/key.pem;
    ...
}
```

Note that the paths (e.g., `/etc/ssl/certs/crt.pem`) can be freely adjusted, and the secret-key file should not be readable by anyone else (`chmod 600`). After adjusting the Nginx/OpenResty config (and testing it with `nginx -t`/`openresty -t`), an Nginx/OpenResty reload is necessary via `systemctl reload nginx` on Debian or via `systemctl reload openresty` on Ubuntu. It is also recommended to test HTTPS afterwards, for example, by simply opening Track UI in a browser and checking if it was able to establish a secure connection.

Note: When **replacing a certificate** with another one (e.g., due to renewing an expired or soon-to-expire certificate), Nginx/OpenResty also has to be reloaded, even if the paths to the certificate and secret-key files do not change.

4 Updating Safectory “Track on Premise”

To update your ToP instance to the latest version, re-run the same `install_track_on_premise.sh` script. You can re-download it using *Option 2* from “*Step 1: Download and Run the Installer*” to ensure you have the **newest** installer script.

4.1 Update Checklist

- **Standard Update Process**
  - ☐ Re-run the `install_track_on_premise.sh` script.
  - ☐ Confirm backup creation when prompted (`yes` recommended).
  - ☐ Load existing configuration values when prompted (`yes` recommended).
  - ☐ Do NOT drop the existing database (default is `no`).
  - ☐ Acknowledge downtime confirmation by pressing `Enter`.

- **Manual Backup and Database Restore**
  - ☐ **Prepare for restore**:
    - ☐ (Optional, for new machine) Manually back up floorplan files from `/opt/prodtrac/media/floorplans`.
    - ☐ Stop Track service: `systemctl stop prodtrac`.
    - ☐ Switch to `postgres` user: `su postgres`.
    - ☐ (Optional) Create a backup of the current database:
    `pg_dump -Fc -Z 9 -d prodtrac --file=${HOSTNAME}_$(date +%F_%H-%M-%S).pgdump`.
  - ☐ **Restore steps**:
    - ☐ Drop existing database: `psql -c "DROP DATABASE prodtrac;"`.
    - ☐ Re-create database: `psql -c "CREATE DATABASE prodtrac;"`.
    - ☐ Restore database: `pg_restore -j 8 -v -d prodtrac /home/psql_backups/<timestamp>_prodtrac.pgdump`.
  - ☐ **Finalize**:
    - ☐ (Optional, for new machine) Copy old floorplans to `/opt/prodtrac/media/floorplans`.
    - ☐ Switch back to `root` user: `exit`.
    - ☐ Start the Track service: `systemctl start prodtrac`.

- **Troubleshooting**
  - ☐ **`apt-get` mirror sync errors**:
    - ☐ Please first try re-running the installation script.
    - ☐ If the error persists, execute `rm -rf /var/lib/apt/lists/*` (followed by `apt-get update`) as **root**.
    - ☐ Re-execute the installation script once again.

4.2 Step 1: Navigate to the directory where the script is located (typically `/root/`) and execute it:

```
cd /root
bash install_track_on_premise.sh
```

The script will detect an existing installation and guide you through the update process.

```
-------
WARNING:
You are installing or updating the Safectory GmbH Asset Tracking solution.
The script might break other services on the same installation!
Do not use unless this OS is solely prepared for the Safectory Track On-premise solution.
------
Please confirm that this OS is not used for anything else:
Press CTRL+C to prevent further installation - or - press ENTER to continue:

OK. Beginning installation/updating process...
ToP version to be installed and installed version match (1.25.5, ef1ef313). Do you want to reinstall (= yes) or abort (= no; default)? [yes/no]
```

4.3 Step 2: The update script will present several prompts:

- **Backup Creation**: The script prompts you to create a backup of the current *Track on Premise* installation. It is highly recommended to back up all existing files to prevent data loss in case of errors. The default option is `yes`.

```
Do you want to create a backup of all ToP files (= yes; default) or skip backup generation (= no)? [yes/no]
```

- **Existing Configuration**: You'll be asked if you want to load existing configuration values. It's generally recommended to load existing values (`yes`) unless you intend to reconfigure.

```
Configuration file /etc/track.config already exists. Do you want to load all existing config values (= yes; default) or start over (= no)? [yes/no]:
```

- **Database**: You may be asked if you want to drop and recreate the existing database (e.g., `prodtrac`). For a standard update, you typically do **not** want to drop the database (default is `no`). Dropping the database will result in data loss unless you have a separate backup you intend to restore.

```
Database 'prodtrac' exists. Do you want to drop and recreate it (default: no)? [yes/no]:
```

- **Downtime Confirmation**: The script will inform you about a short downtime required to stop and restart services. Press `Enter` to continue.

```
Changing Nginx to use generic certificates...
Adjusting permissions of Nginx/Openresty logrotate file...
Done with transferring data. The last steps require to stop and restart all services, which will create a *DOWNTIME* of a short duration.
Please press ENTER to continue
```

4.4 Step 3: Once the update process is complete, the script will confirm.

```
Determining new config options...
Updated ssl_certificate and ssl_certificate_key in /etc/nginx/sites-enabled/001-trac-ssl
Restarting all services...
Waiting for services to start...
Skipped setting a new admin (TrackUI user) password...
If you need to reset the admin password, you can use the following PSQL query ('su postgres', then 'psql -d prodtrac') to set it to "password" and change it via TrackUI afterwards:
UPDATE users SET hashedpassword = 'e5d9f0ae86ff45d4a6092ffd66f631c094d0900b1857a183', salt = '9923a2e79931dc687dc73f949955a4fc4d3dfcb7c5ed7dc3' WHERE email='admin';

Installation finished.
All configuration files have been adjusted.
Please verify all configuration settings in /opt/prodtrac/config and /etc/nginx.
(Backups of all config files can be found in /root/backups/cur_configs___2025-05-14_14-58-36.)
```

The script is designed to:

- Fetch the latest version of the ToP software (if a newer version is available than what the script itself contains).
- Ask if you want to back up current data (this prompt might appear depending on the script version and specific update path).
- Retain existing settings by default when prompted about the configuration file.

5 Managing Safectory "Track on Premise"

5.1 Backups and Database Restore

- **Automatic Backups**: The ToP system is typically configured to perform daily automatic backups of its database. These are usually saved in a directory like `/home/psql_backups/` on the server.

- **Manual Restore**: The following lines explain how to restore the database from a nightly backup manually.

  1) Optional (when moving to a new / fresh machine):

     By default, floorplan files are stored in `/opt/prodtrac/media/floorplans` (cf. value of `media.baseDir` in `/opt/prodtrac/config/custom.xml`) and are currently not included in the database dump created by the backup script. Hence, they need to be backed up and restored manually when moving to a new or fresh machine. In this step, please make sure to manually save the content of the mentioned directory from the "old" installation so that they can later be copied to the new installation.

  2) Stop the Track service as `root` and switch to user `postgres` (for the next steps):

     ```
     systemctl stop prodtrac
     su postgres
     ```

  3) If necessary, create a backup of the current database (make sure to first switch to a directory with write permissions; e.g., type `cd` to switch to `postgres`'s home directory):

     ```
     pg_dump -Fc -Z 9 -d prodtrac --file=${HOSTNAME}_$(date +%F_%H-%M-%S).pgdump
     ```

  4) Drop the existing database:

     ```
     psql -c "DROP DATABASE prodtrac;"
     ```

  5) Re-create the database (still as `postgres` user):

     ```
     psql -c "CREATE DATABASE prodtrac;"
     ```

  6) Proceed with executing the `pg_restore` as follows:

     ```
     pg_restore -j 8 -v -d prodtrac /home/psql_backups/2020-05-13-0035-01_prodtrac.pgdump
     ```

     Note: You need to replace `2020-05-13-0035-01` with the timestamp of the backup file you want to actually restore from `/home/psql_backups/`.

  7) Optional (when moving to a new or fresh machine): Copy any existent floorplans from the old installation to the `/opt/prodtrac/media/floorplans` directory (in case there is no such directory yet, create one). Otherwise, be aware that paths to floorplan images in the database will be nulled on backend startup if the respective image is missing.

  8) Start the Track service again (after switching back to user `root`):

     ```
     exit # = switch from user postgres to root
     systemctl start prodtrac
     ```

5.2 Uninstalling Safectory "Track on Premise"

Use `/root/uninstall_track_on_premise.sh` to remove a ToP installation from a server.

1. Run the uninstall script as `root`:

```
cd /root
bash uninstall_track_on_premise.sh
```

2. Confirm prompts:
   - `Do you really want to uninstall all ToP components ...` (default: `no`)
   - `Do you want to create a backup of all ToP data before uninstall ...` (default: `yes`)
3. The script stops and disables ToP-related services before file cleanup, removes ToP runtime artifacts, drops ToP DB/user (`prodtrac`/`trac`/`track`), and attempts to purge installer runtime packages (with warnings if package purge is only partially possible).

4. After uninstall, verify that ToP services are no longer active and ToP directories/files are removed.

5.3 Troubleshooting

- **Issue**: Cannot connect via SSH.
  - **Solution**: Check VM network settings (Bridged Adapter), VM IP address, host firewall, VM firewall (ufw) rules for port 22.
- **Issue**: ToP web interface not loading.
  - **Solution**: Check ToP service status on server, ufw rules for ports 80/443, DNS resolution for the domain, `/etc/hosts` file if applicable. Check ToP logs for errors.
- **Issue**: Various package fetch errors during installation such as shown below (the actual packages and versions may differ):
  - Example 1:

```
Err:1 http://deb.debian.org/debian bookworm/main arm64 nginx-common all 1.22.1-9+deb12u1
404  Not Found [IP: 199.232.190.132 80]
Err:2 http://deb.debian.org/debian bookworm/main arm64 nginx arm64 1.22.1-9+deb12u1
404  Not Found [IP: 199.232.190.132 80]
E: Failed to fetch
 ↪  http://deb.debian.org/debian/pool/main/n/nginx/nginx-common_1.22.1-9%2bdeb12u1_all.deb
 ↪  404  Not Found [IP: 199.232.190.132 80]
E: Failed to fetch
 ↪  http://deb.debian.org/debian/pool/main/n/nginx/nginx_1.22.1-9%2bdeb12u1_arm64.deb  404
 ↪  Not Found [IP: 199.232.190.132 80]
E: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
```

  - Example 2:

```
Get:23 http://deb.debian.org/debian bookworm/main arm64 libxt-dev arm64 1:1.2.1-1.1 [402 kB]
Err:23 http://deb.debian.org/debian bookworm/main arm64 libxt-dev arm64 1:1.2.1-1.1
File has unexpected size (817724 != 401664). Mirror sync in progress? [IP: 199.232.190.132
 ↪  80]
Hashes of expected file:
  - SHA256:88d22c70c2b936f6d6c4d825a9bb8c3a9a99460244a77940c85e98accd9289ca
  - MD5Sum:82ea8cbba36ecc7af2a753a2e18c08b3 [weak]
  - Filesize:401664 [weak]
    Fetched 118 MB in 13s (9,311 kB/s)
    E: Failed to fetch
     ↪  http://deb.debian.org/debian/pool/main/libx/libxt/libxt-dev_1.2.1-1.1_arm64.deb  File
     ↪  has unexpected size (817724 != 401664). Mirror sync in progress? [IP: 199.232.190.132
     ↪  80]
    Hashes of expected file:
  - SHA256:88d22c70c2b936f6d6c4d825a9bb8c3a9a99460244a77940c85e98accd9289ca
  - MD5Sum:82ea8cbba36ecc7af2a753a2e18c08b3 [weak]
  - Filesize:401664 [weak]
    E: Unable to fetch some archives, maybe run apt-get update or try with --fix-missing?
    Installation incomplete, reason: install default-jdk
```

  - **Solution**: Please first try re-running the installation script. If the error persists, please execute command `rm -rf /var/lib/apt/lists/*` (followed by `apt-get update`) as **root** and re-execute the installation script once again.
- **Issue**: Nexus returns `HTTP 404` for `current_master` (or similar `current_<branch>` path).
  - **Cause**: A `404` means Nexus on port `8443` was reached, but the requested path or file was not found (for example wrong repository/branch, missing `current_<branch>` file, or wrong Nexus endpoint). If port `8443` is blocked, you usually see timeout/connection errors instead of `404`.

  - **Solution**: Verify outbound access to `nexus.safectory.com:8443`, then verify repository and branch/version inputs. You can test that using valid credentials with:

    ```
    curl -k -I https://nexus.safectory.com:8443/repository/<repo>/current_<branch>
    ```

- **Issue**: ToP bundle download aborts.
  - **Cause**: It aborts because of errors such as:
    * `Installation incomplete, reason: ERROR: Downloading Track service files failed`
    * `curl: (3) URL using bad/illegal format or missing URL`
  - **Solution**: Re-run the installer first. If prompted because the local tarball differs from Nexus, choose to re-download. If the issue persists, remove the affected local tarball from `/root/nexus/` and run again, or specify branch/version explicitly (`bash install_track_on_premise.sh <branch> <version> [repo]`) to bypass `current_<branch>` lookup issues. Also verify free disk space and Nexus connectivity.
- **Issue**: Installer script fails for other reasons.
  - **Solution**: Check for error messages in the script output. Ensure all prerequisites are met (Nexus access, disk space, dependencies like `curl`). Check the installation log.
- **Issue**: Password reset functionality is not working.
  - **Cause**: The system is currently unable to send password reset emails due to a missing or unconfigured SMTP server.
  - **Solution**: To enable password reset emails, configure an SMTP server and ensure valid credentials are stored in the configuration file located at: `/opt/prodtrac/config/mail.xml`. Once configured, password reset requests will be delivered via email.
  - **Alternative Solution**: An administrator with full access to the server needs to reset the password via a PSQL query: `su postgres` → `psql -d prodtrac` →

    ```
    UPDATE users
    SET hashedpassword = 'e5d9f0ae86ff45d4a6092ffd66f631c094d0900b1857a183',
        salt = '9923a2e79931dc687dc73f949955a4fc4d3dfcb7c5ed7dc3'
    WHERE email='[USER_TO_RESET_PASSWORD]';
    ```

    This resets the password to `password` and can then be changed in TrackUI afterwards.

5.4 Need Help?

If you encounter issues during installation or operation, please gather the following information before contacting support:

- The installation log file (usually located at `/root/top_install-latest.log` or a similar path indicated by the installer).
- Details about your server setup (OS version, VM or physical, network configuration).
- Steps you've already tried to resolve the issue.

Email Safectory support at **support@safectory.com**.