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

safectory GmbH

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)

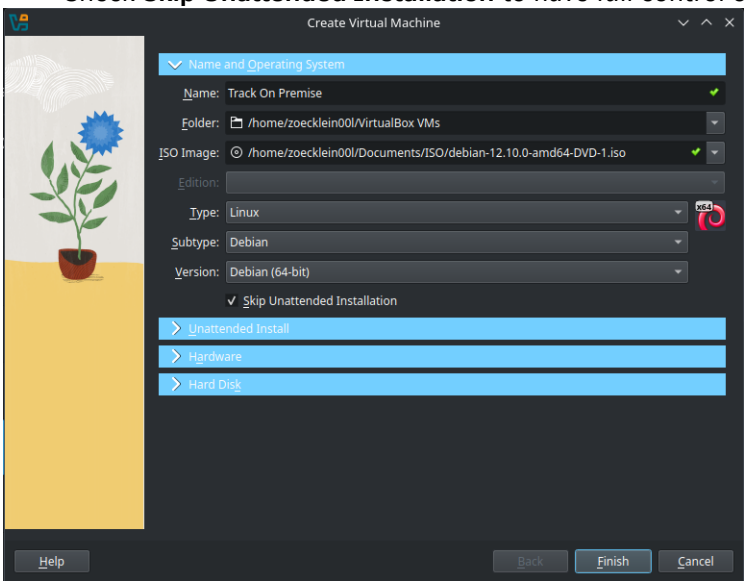
This section walks you through configuring a Debian-based or Ubuntu-based Oracle VirtualBox virtual machine, optimized for **Track On Premise**. This includes hardware allocation, networking, and initial OS setup.

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

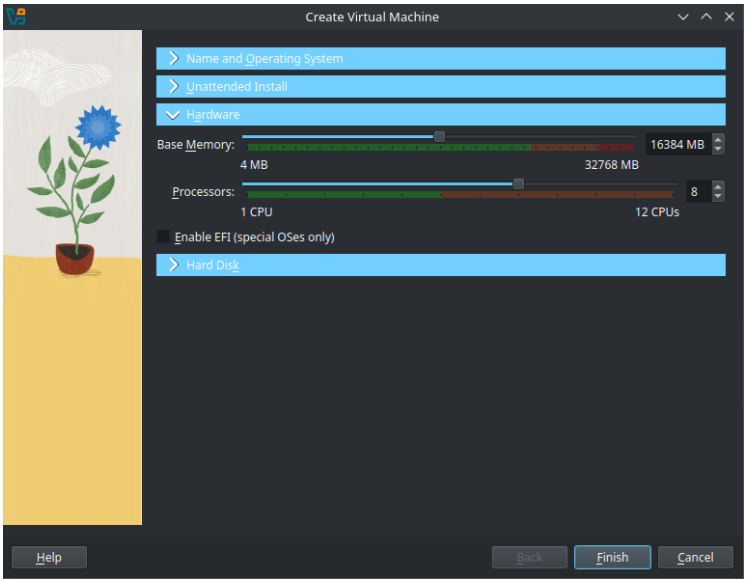
1. Open VirtualBox and click **New**.
2. Fill in the VM details:
   - **Name**: `Track On Premise` (or a name of your choice)
   - **Folder**: Choose your preferred storage location for VM files.
   - **ISO Image**: Select the downloaded Debian or Ubuntu Server ISO file.
   - **Type**: `Linux`
   - **Version**: `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)

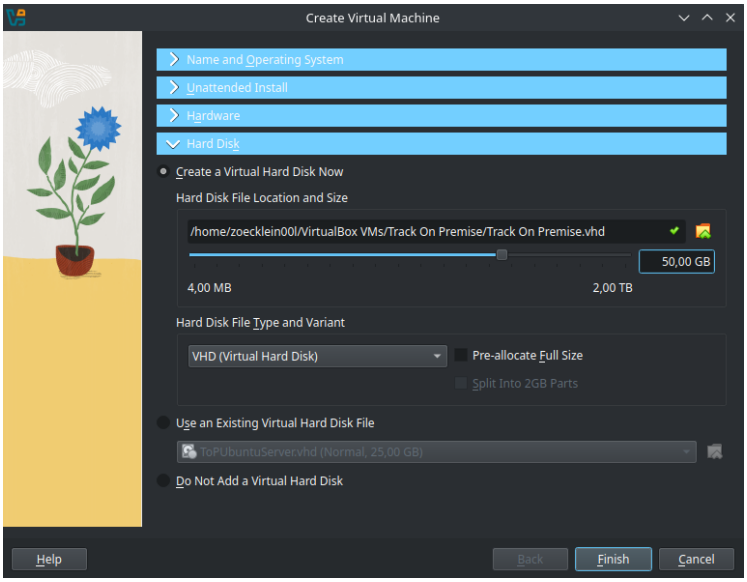
1. **Memory (RAM)**: Allocate **16384 MB (16 GB)**.
2. **Processors**: Assign **8 CPUs**.

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



2.4 Step 3: Create Virtual Hard Disk

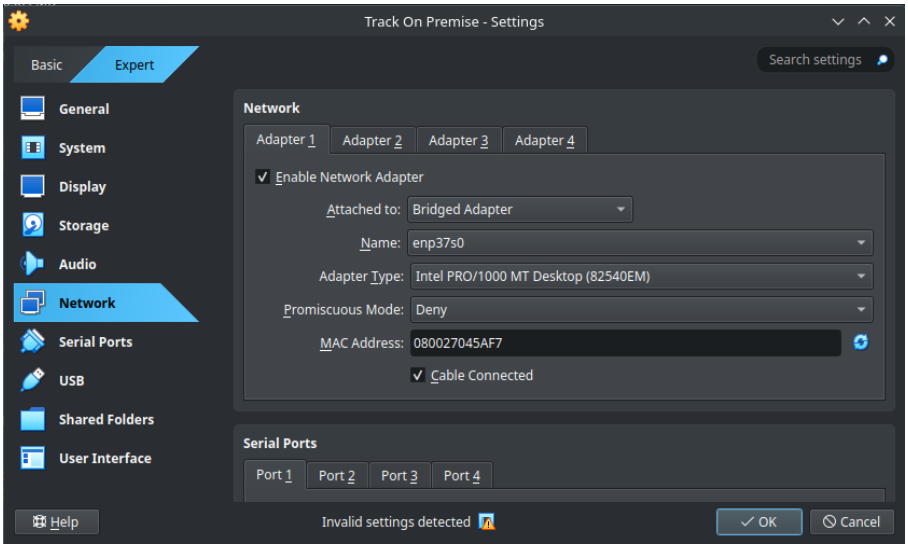
1. Select `Create a Virtual Hard Disk Now`.
2. Configure the virtual hard disk:
   - **Location**: Default is usually fine (e.g., `~/VirtualBox VMs/Track On Premise/Track On Premise.vdi`).
   - **File Size**: **50.00 GB** (or more, as per server requirements and expected data volume). This refers to 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.

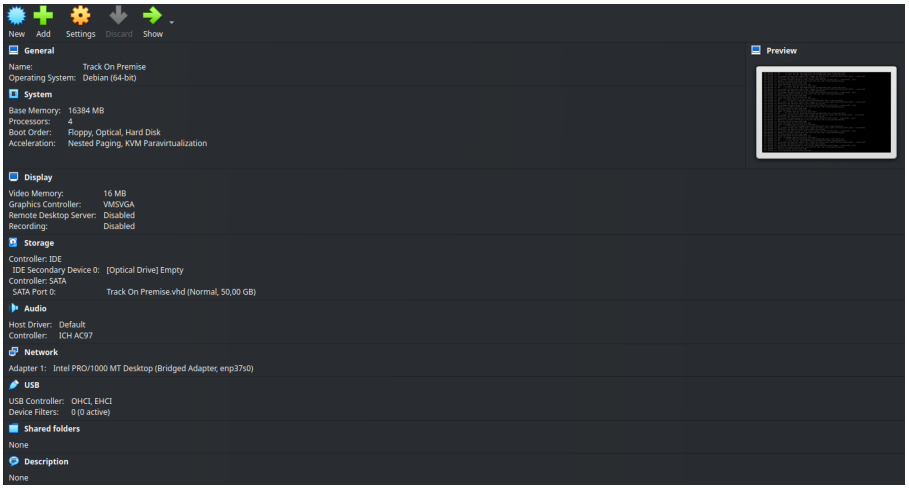
1. With the `Track On Premise` VM selected, go to **Settings** > **Network**.
2. **Adapter 1**:
   - Enable Network Adapter.
   - **Attached to**: Select `Bridged Adapter`.
   - **Name**: Choose your host machine's active network interface (e.g., `enp37s0` on Linux, `Ethernet` on Windows/macOS).
     - *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.*

```
root@trackonpremise-sf:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:04:5a:f7 brd ff:ff:ff:ff:ff:ff
    inet 172.27.0.161/21 brd 172.27.7.255 scope global dynamic enp0s3
       valid_lft 2881sec preferred_lft 2881sec
    inet6 fe80::a00:27ff:fe04:5af7/64 scope link
       valid_lft forever preferred_lft forever
root@trackonpremise-sf:~#
```

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

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

```
~
ssh root@172.27.0.161
Warning: Permanently added '172.27.0.161' (ED25519) to the list of known hosts.
root@172.27.0.161's password:
Linux trackonpremise-sf 6.1.0-34-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.135-1 (2025-04-25) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed May  7 13:54:27 2025
root@trackonpremise-sf:~#
```

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 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.

3.2 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`.

3.2.1 Option 1: 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 script is typically extracted here
chmod +x install_track_on_premise.sh
bash install_track_on_premise.sh
```

3.2.2 Option 2: Download directly from Nexus and install (Recommended for latest version):

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
```

```
root@topdebian:~# 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 "https://nexus.beamzone.net:8443/repository/safectory_on_premise/install_track_on_premise.tar.gz" \
&& 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:

```
-------
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:
```

- *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:
```

3.3 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 **installation size**. Read prompts carefully and select the appropriate option based on your server's resources and expected load.

```
Please enter the size for this installation:
  * demo[1]
  * tiny[2]
  * small[3]
  * medium[4]
  * large[5]
Default value is the tiny installation, option 2 (e.g., to expect when having 100 devices and 16 GiB of RAM)
```

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

- At the end of a successful installation, you should receive a **randomly generated admin password** for accessing the TrackUI. **Store this password securely.**

```
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   601  100   556  100    45   3737    302 --:--:-- --:--:-- --:--:--  4033
NEW track admin password is SEJiyhsZydAnUDDUgNcI

Installation finished.
```

3.4 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`)

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.

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]
   ```

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
```

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

```
systemctl stop prodtrac
su postgres
```

2) If necessary, create a backup of the current database:

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

3) Drop the existing database:

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

4) Re-create the database by typing `psql` (still as `postgres` user) and then:

```
postgres=# CREATE DATABASE prodtrac;
CREATE DATABASE
postgres=# exit
```

5) 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/`.

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

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

5.2 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**: Installer script fails.
  - **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.

5.3 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**.