Server Requirements for Safectory Track on Premise

safectory GmbH

1 Linux Server Requirements

1.1 Server Hardware and Installation Size

The service can run on physical hardware or in a virtualized environment. The installation script will ask what installation size to use. The following table serves as orientation:

Size	Tags	High average of events per tag and 8h activity per day	Total estimate of events	CPU threads	RAM [GB]	SSD [GB]
Large	15000	1920	28,800,000	24	128	1000
Medium	1000	1920	1,920,000	16	64	500
Small	500	1920	192,000	8	32	250
Tiny	100	1920	96,000	8	16	250
Demo	15	1920	28,800	4	4	100

1.2 Supported Linux Distributions

Distribution	Codename	EOL
Debian 11	bullseye	2026-08-31
Debian 12	bookworm	2028-06-30
Ubuntu 22.04 LTS	jammy	April 2027
Ubuntu 24.04 LTS	noble	April 2029

Operating systems not listed above are currently unsupported. If support for a different OS is required, please contact us to discuss a custom support agreement.

1.3 Network

Network has to provide DNS, NTP, and routing information.

1.4 Firewall and Port Requirements

Please make sure that the following firewall-related requirements are met. The table below summarizes the necessary port configurations.

1.4.1 Port List Table

Legend:
`trusted_net` = your trusted IP address or network in CIDR format (e.g., `203.0.113.0/24`)

Port	Protocol	Direction	Service	Source IP / Network	Destination IP / Network	Notes
22	TCP	In	SSH access	`trusted_net`	Server IP	Replace `trusted_net` with your allowed IP or network range.
80	TCP	In	ToP frontend access (HTTP)	`trusted_net`	Server IP	Also required for BLE gateway access. If ToP is public, allow 80/tcp.
443	TCP	In	ToP frontend access (HTTPS)	`trusted_net`	Server IP	Also required for BLE gateway access. If ToP is public, allow 443/tcp.
123	UDP	Out	NTP access	Server IP	NTP server(s)	For system time synchronization.

Port	Protocol	Direction	Service	Source IP / Network	Destination IP / Network	Notes
6555	TCP	Local	Track backend API	Nginx (local)	Backend service	Internal-only port for REST API. Externally exposed via Nginx reverse proxy on 443.
6556	TCP	Local	ToP BLE data input	Nginx (local)	Backend service	Internal-only port for BLE data input. Externally exposed via Nginx reverse proxy on 443.
8443	TCP	Out	Safectory Nexus access	Server IP	91.250.82.47	Required for downloading ToP installation files from `nexus.safectory.com`.
53	UDP	Out	DNS access	Server IP	DNS server(s)	For DNS resolution.
53	TCP	Out	DNS access	Server IP	DNS server(s)	For DNS resolution (TCP fallback).

1.4.2 Additional Firewall Notes:

- The installation script must be able to install packages from the configured Debian/Ubuntu Server repositories. This typically means allowing outbound HTTP (80/tcp) and HTTPS (443/tcp) to the repository mirrors.
- The system can be used without internet connection after installation.
- Temporary internet connection (Debian/Ubuntu Server repositories and safectory's Nexus) is required for updates.

1.5 NTP

An NTP client has to be available on the Debian/Ubuntu Server system to provide accurate timing information for the Track Service. This usually means allowing outbound NTP (123/udp).

1.6 Debian Repository

For `apt-mirror`, **`/etc/apt/sources.list`** repository location needs to be configured before executing the installation script.

1.7 Language

Supported:

- `de_DE.utf-8`
- `en_GB.utf-8`

Other default installation languages might work but are unsupported.

1.8 Root Access

Root access needs to include the `PATH` environment information. Use `su -` to elevate permissions.

2 Safectory Repository Account (Nexus)

Your username and password for the Safectory Nexus repository is needed during installation to download the installation files.
This access is via HTTPS on port 8443 to `nexus.safectory.com` (IP: `91.250.82.47`).

3 BLE Gateway Access to the ToP Service

Installed BLE gateways need to connect to the ToP service via HTTP Port 80 and Port 443.

4 Mandatory Processes

4.1 Process Definition

Processes mandatory for Track to work properly:

- Track Java application
- Nginx webserver/proxy
- PostgreSQL database

4.2 Check Process Status

If the ToP instance was set up with the provided SF installation script on a Debian/Ubuntu Server system, then one can check the process statuses as follows with Systemd (`Active: active (running)` is always the expected state):

- Track: `systemctl status prodtrac.service`
- Nginx: `systemctl status nginx.service`
- PostgreSQL: `systemctl status postgresql@13-main.service` (note that `@13-main` depends on the PSQL version actually installed)

Example output for a healthy Track service:

```
$ systemctl status prodtrac.service
• prodtrac.service - Safectory Track
   Loaded: loaded (/etc/systemd/system/prodtrac.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2024-07-15 13:36:45 CEST; 1 months 11 days ago
 Main PID: 32294 (java)
    Tasks: 308 (limit: 4915)
   Memory: 11.9G
   CGroup: /system.slice/prodtrac.service
           └─32294 /usr/bin/java
             ↪  -agentlib:jdwp=transport=dt_socket,server=y,suspend=n,address=*:6000
             ↪  -Djava.rmi.server.hostname=localhost -Dcom.sun.management.jmxremote.port=8091
             ↪  -Dcom.sun.management.jmxremote.rmi.port=8091 -Dcom.sun.managem...
```

4.3 Output Analysis

Limit values are specific to each system due to configurations and use cases and should be individually agreed with Safectory.

4.4 Basic Ping Check

For Track, one can additionally send periodic requests (e.g., via cronjob) to the `/api/ping` endpoint and verify that the backend is always responding with `pong`. If it does not respond consecutively a few times as expected, it is recommended to restart the backend as a first measure and investigate log files shortly afterwards.

5 Standard Configuration

5.1 General

- **Offline Mode**: `false` – Map is visible, system requires Internet access.

5.2 Network

- **Default Service Ports**: `6555, 6556` – BLE data input and API communication.
- **Proxy-Server Management**: `snake-oil certificate` – For fully secured connections, a custom certificate may be required. This certificate is expected to be issued by the client's IT department.
- **HTTP Session Timeout**: `1800` – In seconds, applies to both TrackUI and API session timeouts.

5.3 Performance Options

- **General**: `performance` – Default values optimized for performance.
- **Position Deduplication**: `true` – Default values prevent duplicate positions and improve performance.
- **Beacon Last Seen Update Limitation**: `3600` – In seconds, updates beacon information, enhanced performance.

5.4 Data Management

- **Data Maintenance and Automatic Deletion**: `24` – In hours, periodic position and metadata cleanups.
- **Startup Device-Check Method**: `true` – Sanity check on backend-startup.
- **Database Indexing**: `true` – Backend generates indexes every night, which improves performance.

5.5 Integrations

- **BLE Counters Statistics**: `disabled`
- **Third-Party Gateways**:
  - **gRPC and JWT Backend Configuration Options**: `disabled`
  - **Aruba Access Points**: `disabled`
- **MQTT Integration**: `disabled`

5.6 Add-Ons

- **Fidelio**: `disabled`
- **Manufacturer Data**: `disabled`