Server Requirements for Safectory Track on Premise

safectory GmbH

1 Linux Server Requirements **2**
- 1.1 Server Hardware and Installation Size . . . 2
  - 1.1.1 Reference CPU . . . 2
  - 1.1.2 System-Requirements Tables . . . 2
- 1.2 Supported Linux Distributions . . . 3
- 1.3 Network and Certificate . . . 3
- 1.4 Firewall and Port Requirements . . . 3
  - 1.4.1 Port List Table . . . 3
  - 1.4.2 Additional Firewall Notes: . . . 5
- 1.5 NTP . . . 6
- 1.6 Debian/Ubuntu Repository Access Requirements . . . 6
  - 1.6.1 Default Diagnostic Tools . . . 6
- 1.7 Language . . . 7
- 1.8 Root Access . . . 7

2 Safectory Repository Account (Nexus) **7**

3 BLE Gateway Access to the ToP Service **7**

4 Mandatory Processes **7**
- 4.1 Process Definition . . . 7
- 4.2 Check Process Status . . . 7
- 4.3 Output Analysis . . . 8
- 4.4 Basic Ping Check . . . 8

5 Standard Configuration **8**
- 5.1 General . . . 8
- 5.2 Network . . . 8
- 5.3 Performance Options . . . 8
- 5.4 Data Management . . . 8
- 5.5 Integrations . . . 8
- 5.6 Add-Ons . . . 9

6 Appendix **9**
- 6.1 Appendix: Services and Connection Overview . . . 9

1 Linux Server Requirements

This requirements sheet informs the on-site IT staff about system prerequisites, required network access, and components/packages that are installed for ToP installation and operation. Installation must only start after this requirements sheet has been reviewed and approved by the on-site IT staff.

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.

1.1.1 Reference CPU

The following CPU specifications serve as reference for the suggested number of cores in the tables below:

- CPU model: Intel Core i7-8700 @ 3.20GHz
- Geekbench scores (version: `Geekbench 6.4.0 Build 603514 (rosedale-main-build eb7eea2a40)`):
  - Single-core: **1645**
  - Multi-core: **6443**
- Sysbench results (version: `sysbench 1.0.20`):
  - 1 thread: ~**1550 events/sec**
  - 16 threads: ~**13150 events/sec**

1.1.2 System-Requirements Tables

The following two system-requirements tables serve as orientation for the asset-tracking and “tamper-safe beacon” use cases. For the requirements we assume a supported operating system (see section Supported Linux Distributions) in minimal configuration, that is, no additional packages and no other services installed other than the ones provided by the base operating system. For Safectory-led operations/troubleshooting, diagnostic tooling is part of the default installation scope (see Default Diagnostic Tools).

Further assumptions:

- The numbers are based on measurements with Track version 1.26. (Other versions may have different performance requirements.)
- On average, each tag generates about 2 × 0.067 requests/sec (or 1 × 0.067 requests/sec per beacon), forwarded by 5 gateways in range.
- The estimates include headroom for background tasks such as cleanup jobs, indexing, and backups.
- These estimates assume no high volume of periodic `/api` requests (e.g., route reports). If you plan to trigger a large number of such requests, please request a more detailed capacity assessment in advance.

Asset-Tracking Case

Size	Tags	CPU Cores	RAM [GB]	SSD [GB]
Large (approximated)	4000	32	128	1024
Medium	1000	8	64	512
Small	500	4	32	256
Tiny	100	2	16	128
Demo	15	1	4	64

Tamper-Safe–Beacon Case

Size	Beacons	CPU Cores	RAM [GB]	SSD [GB]
Large (approximated)	4000	16	64	1024
Medium	1000	4	32	512
Small	500	2	16	256
Tiny	100	1	8	128
Demo	15	1	4	64

Notes on disk space / partitioning:

- Although the tables above specify the total disk space required for each system size, it's essential to ensure that space is properly allocated across the server's partitions. For example, database files are typically stored under `/var/lib/postgresql`. If the `/var` partition lacks sufficient space, the system may run out of disk space even if other partitions have available capacity.
- **Recommendation:** When configuring the server, allocate sufficient space to the partition containing the database data directory, or mount it separately. Likewise, ensure that partitions used for logs (e.g., `/var/log`, `/opt/prodtrac/logs`) have enough capacity to prevent operational issues.

1.2 Supported Linux Distributions

Distribution	Codename	Supported Until (LTS)
Debian 12	bookworm	2028-06-30
Debian 13	trixie	2030-06-30
Ubuntu 22.04 LTS	jammy	April 2027
Ubuntu 24.04 LTS	noble	April 2029
Ubuntu 26.04 LTS	resolute	April 2031

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 and Certificate

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

For fully secured connections, a **custom certificate** may be required. This certificate is expected to be issued by the client's IT department. Detailed information can be found in the ToP manual ("Certificate Management").

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

Overview:

For a detailed overview of services and connection points, see Appendix: Services and Connection Overview.

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	Only required for backend maintenance tasks (e.g., Track updates).
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.
67	UDP	Out	DHCP client requests	Server IP	DHCP server(s)	Required only if the ToP server gets its network configuration via DHCP.
68	UDP	In	DHCP client replies	DHCP server(s)	Server IP	Required only if the ToP server gets its network configuration via DHCP.
6555	TCP	Local	Track backend API	NGINX/OpenResty (local)	Backend service	Internal-only port for REST API. Externally exposed via reverse proxy on port 443.
6556	TCP	Local	ToP BLE data input	NGINX/OpenResty (local)	Backend service	Internal-only port for BLE data input. Externally exposed via reverse proxy on port 443.
8443	TCP	Out	Safectory Nexus access	Server IP	91.250.82.47	Required for downloading ToP installation files from `nexus.safectory.com`.
80	TCP	Out	APT repository access (HTTP)	Server IP	Debian/Ubuntu APT repositories	Required during installation and updates for package downloads.
443	TCP	Out	APT repository access (HTTPS)	Server IP	Debian/Ubuntu APT repositories	Required during installation and updates for package downloads and key retrieval.
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).

Ports needed when third-party gateways (i.e., Aruba, Cisco, Extreme Networks) are involved:

Aruba:

Port	Protocol	Direction	Service	Source IP / Network	Destination IP / Network	Notes
443	TCP	In	BLE data (HTTPS/Web-Socket)	Aruba AP / WLC	Backend service	Regular port for HTTPS.
6555	TCP	In	BLE data (HTTP/Web-Socket)	Aruba AP / WLC	Backend service	Only required if HTTP needs to be enforced; must match the internal Track backend API port (see main table).

Cisco:

Port	Protocol	Direction	Service	Source IP / Network	Destination IP / Network	Notes
443	TCP	In	Control & authentica-tion (HTTPS)	Cisco AP / WLC	Backend service	Used for auth, health checks, and control API calls.
57501	TCP	In	BLE data (gRPC)	Cisco AP / WLC	Backend service	Default port for Cisco's gRPC BLE streaming endpoint.

Extreme Networks:

Port	Protocol	Direction	Service	Source IP / Network	Destina-tion IP / Network	Notes
6978	UDP	In	BLE data	Extreme Con-troller	Backend service	Default for controller-based deployments; AP sends raw UDP payloads.
6979	TCP	In	BLE data	Extreme APs	Backend service	Default for AP-direct deployments; AP sends raw TCP payloads.

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/Ubuntu Repository Access Requirements

The installation script automatically configures the required APT repositories for PostgreSQL and OpenResty (NGINX replacement on Ubuntu). No manual changes to `/etc/apt/sources.list` or related files are needed.

However, please ensure that the following external repositories are reachable from the machine prior to running the script:

- **PostgreSQL APT repository**:
  `http://apt.postgresql.org/pub/repos/apt`
- **OpenResty APT repository** (architecture-dependent):
  - x86_64: `http://openresty.org/package/ubuntu`
  - aarch64: `http://openresty.org/package/arm64/ubuntu`

Also, ensure the machine can download the required APT repository signing keys:

- **PostgreSQL signing key**:
  `https://www.postgresql.org/media/keys/ACCC4CF8.asc`
- **OpenResty signing key**:
  `https://openresty.org/package/pubkey.gpg`

If your environment restricts outbound HTTP/HTTPS traffic (e.g., via firewalls or proxy settings), make sure appropriate exceptions are configured.

> **Tip:** You can test connectivity with `curl -I <URL>` or `wget --spider <URL>`.

1.6.1 Default Diagnostic Tools

As part of the regular ToP installation, the following packages are installed by default:

- `screen`
- `tcpdump`
- `net-tools` (e.g., `arp`, `route`, `netstat`)
- `htop`
- `sysstat` (e.g., `iostat`, `sar`)
- `dnsutils` (e.g., `dig`, `nslookup`)
- `iputils-ping`
- `traceroute`
- `nmap`
- `ethtool`
- `lsof`

Network-safety notes:

- Installing these packages does not open additional inbound ports and does not create persistent outbound connections by itself.
- Some tools generate network traffic when actively used (for example `nmap`, `ping`, and `traceroute`).
- Some commands can also trigger DNS/reverse-DNS or ARP neighbor lookups even in diagnostics mode.
- For low-impact analysis, numeric-output flags (`-n`, `-nn`) are preferred where available, and active scans should be coordinated with on-site IT security policies.

These tools are typically available from the standard Debian/Ubuntu repositories and do not require additional third-party APT repositories in common setups.

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/OpenResty 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/OpenResty: `systemctl status nginx.service` (Debian) / `systemctl status openresty.service` (Ubuntu)
- 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` – OS-provided (can be replaced with custom one, see section Network and Certificate)
- **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

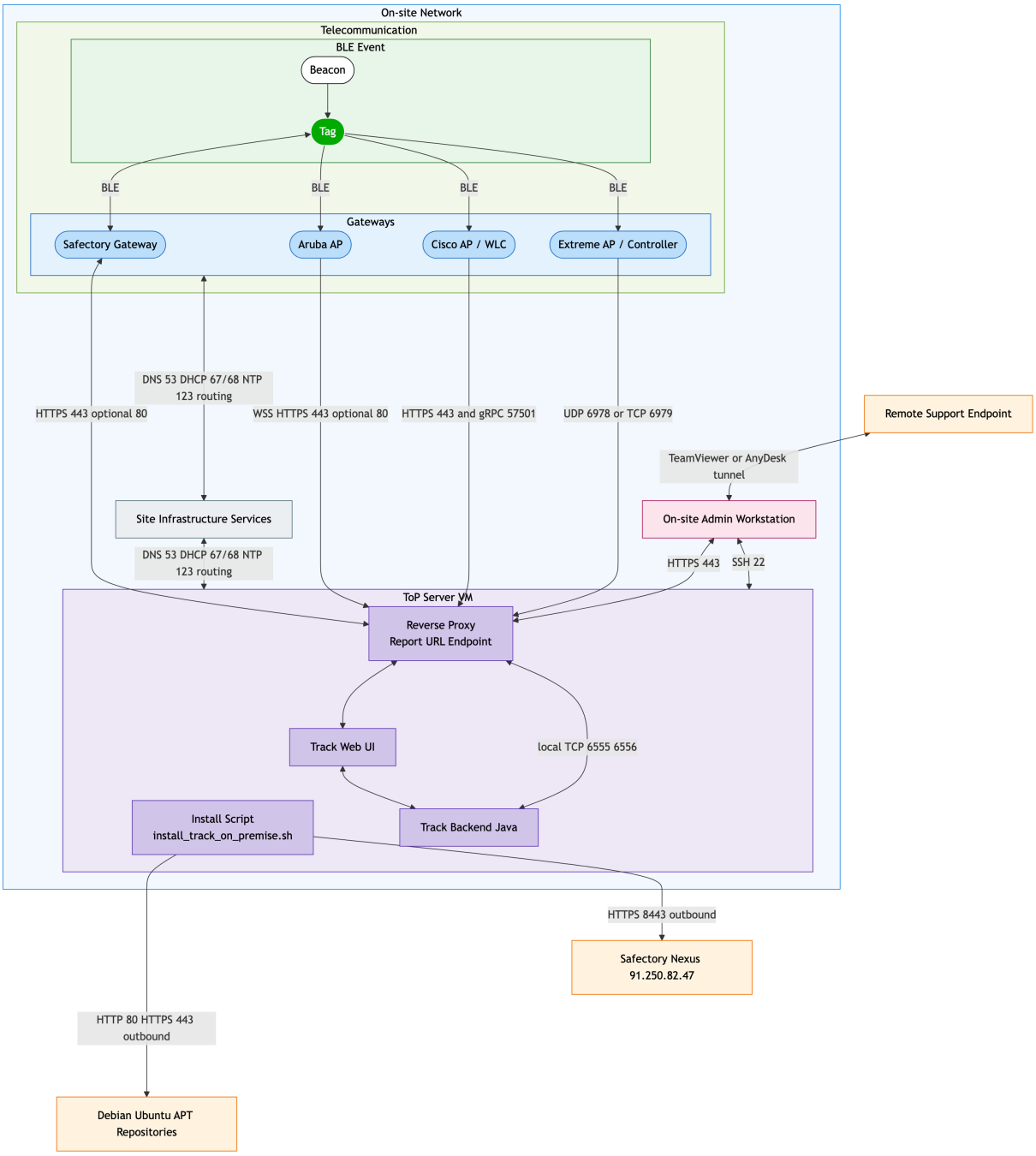
- **Data Maintenance and Automatic Deletion**: `24` – In hours, periodic position and metadata cleanups.
- **Startup Device-Check Method**: `true` – Sanity check on backend-startup.
- **Database Indexing**: `true` – Backend generates indexes every night, which improves performance.

5.5 Integrations

- **BLE Counters Statistics**: `disabled`
- **Third-Party Gateways**:
  - **gRPC and JWT Backend Configuration Options**: `disabled`
  - **Aruba Access Points**: `disabled`
  - **Gateway Auto-Add Access Point Devices and Beacons**: `enabled`
- **MQTT Integration**: `disabled`

5.6 Add-Ons

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

6 Appendix

6.1 Appendix: Services and Connection Overview