INSTALLATION GUIDE · CERT.GT

T-Pot community sensor

Version 1.0 · Reviewed Oct 11, 2026 · TLP:CLEAR · For: anyone who administers a Linux server

This guide takes you from an empty server to a sensor that reports attacks to the cert.gt network. You install T-Pot in Sensor mode; the cert.gt team then links it to the central node (Hive). The sensor is a decoy: it only records whoever attacks it, never your traffic.

How it works

- Your sensor exposes fake services (SSH, web, databases) that attract automated attacks.
- Every attempt is logged and sent, encrypted, to the cert.gt central node.
- The data is published in aggregate on the live map and in the statistics; your IP and exact location are never shown.

Before you start

- A dedicated server or virtual machine: do not install T-Pot on a machine that is already used for something else.
- Resources recommended by T-Pot for the Sensor type: 8 GB of RAM and 128 GB of disk. Check the current values in the official documentation.
- A freshly installed operating system supported by T-Pot (Debian or Ubuntu Server, among others).
- A dedicated public IP, or an isolated DMZ. Never place it inside your internal network.
- Outbound internet access and a user with sudo privileges.

Step 1 · Install T-Pot in Sensor mode

Log in to your server as a regular user (not root) and run:

```
git clone https://github.com/telekom-security/tpotce.git
cd tpotce/
./install.sh
```

- When the installer asks for the type, choose **Sensor** (option **S**).
- When it finishes, reboot the server:

```
sudo reboot
```

Important: after the reboot, the management SSH service is no longer on port 22; it moves to port **64295**. Port 22 is now answered by the decoy. To log back in:

```
ssh -p 64295 your_user@your_sensor_ip
```

Step 2 · Request linking

- Fill in the form at **cert.gt/en/sensor** with the sensor's public IP, the department where it is located and a contact email.
- The cert.gt team replies with the central node's SSH public key and the destination your sensor will send its events to.
- Do not send passwords through the form or by email.

Step 3 · Authorize the central node

The central node configures your sensor automatically (Ansible) over SSH. To allow this, add the public key we sent you to the sensor's management user:

```
mkdir -p ~/.ssh && chmod 700 ~/.ssh
echo "PUBLIC_KEY_WE_SENT_YOU" >> ~/.ssh/authorized_keys
chmod 600 ~/.ssh/authorized_keys
```

- If you have a firewall, allow port 64295 only from the central node IP we give you.
- During deployment we will ask you, over an agreed channel, to type the sudo password yourself, or to enable temporary sudo for that user.

Step 4 · Verify

- The cert.gt team runs the deployment from the central node and confirms once the sensor is registered.
- Reboot the sensor once more when we tell you to.
- Within a few minutes your events start appearing on the live map, aggregated by department.

To check the status of the services on your sensor:

```
sudo systemctl status tpot
sudo docker ps
```

Keep it secure

- Do not store any of your own data on the sensor, and do not reuse passwords from other systems on it.
- Block outbound traffic from the sensor to your internal network; it only needs to reach the internet and the central node.
- Apply T-Pot updates when we notify you.
- If you are going to decommission it, write to us so we can remove it from the central node.

If something goes wrong

- You cannot log in over SSH: remember to use port 64295.
- The installer stops: check that the system is freshly installed and meets the minimum resources.
- The sensor does not appear on the map: confirm with us that linking has finished and that your firewall allows outbound traffic.
- Any questions: write to incidentes@cert.gt with the subject “Sensor”.

cert.gt is a private, community-driven initiative of Devel Group.

cert.gt · devel.group · Report an incident at cert.gt/en/reportar or email incidentes@cert.gt

T-Pot is an open-source project by Telekom Security (github.com/telekom-security/tpotce). By installing the sensor you agree that the decoy's data may be published in aggregate form. This guide is not a document from a government entity.