



1. AI Sensor

The AI EdgeLabs Sensor is a proprietary network telemetry and monitoring agent that continuously scans and reports network and Edge/IoT Gateway performance and configuration. It holds an AI-powered model set that continuously checks traffic behavior through pre-trained algorithms.

With AI EdgeLabs Sensor, infrastructure teams can locate application performance problems faster, reduce time-to-diagnosis, and accelerate time-to-repair without additional efforts for deployment and integration thanks to plug-and-play capabilities.

2. Ways to install AI Sensor

During its first deployment, the AI EdgeLabs Sensor runs a configurable set of security checks and topology research to collect the initial context of the environment. Data from these collections is analyzed by the AI EdgeLabs Platform.

The AI EdgeLabs Platform provides a set of AI-based models which are pre-trained in the existing knowledge base of threat patterns and attack signatures; this pre-training is always done centrally on our platform by running these collections from a fleet of well-distributed/placed EdgeLabs Sensors.



There are couple ways to install AI Sensor to Edge from customer side:

- Docker-based installation
- Kubernetes-based installation
- Edge-Orchestration platform installation
- OpenShift-based installation

The general idea of Sensor installation for all variations is the same — it requires Docker runtime for NDR/EDR — considering the fact that there are different container platforms like Kubernetes or similar, the variations of this installation would slightly differ too.

3. Tenant activation flow

Tenant — is the organization entity that is directly mapped to billing and coordinated by tenant admin user.

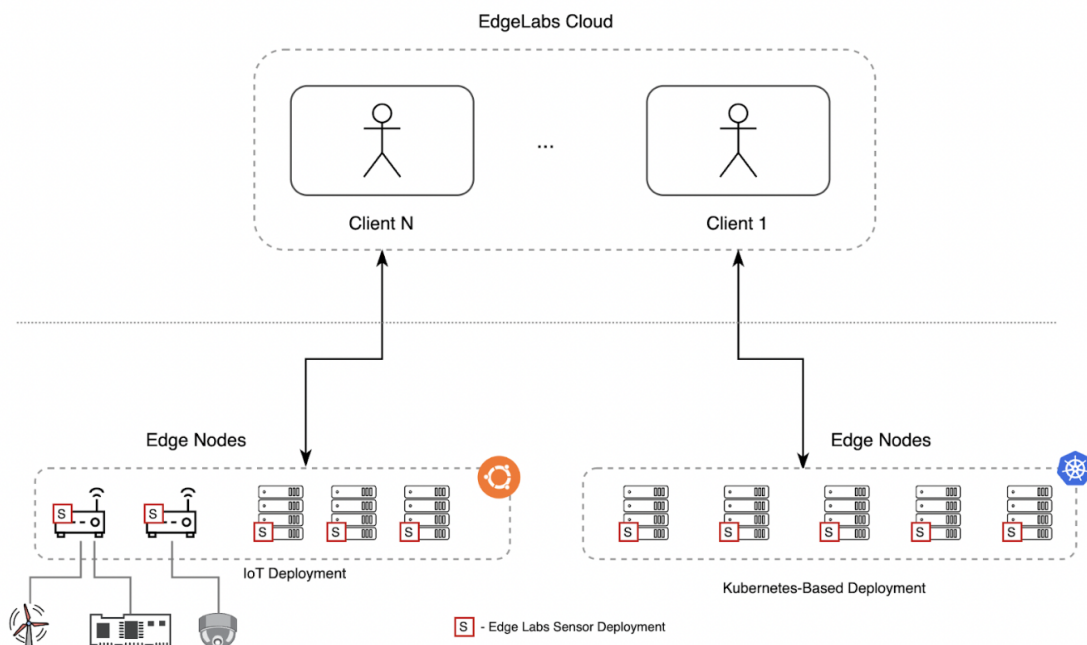
Client (or tenant) activation flow usually happens after email invitation from EdgeLabs team, where invite to tenant activation will be sent. As a result future tenant admin will get email with tenant activation and will be asked to activate credentials for SOC Center (dashboard) access.

So tenant creation and activation flow usually have following steps:



AI **E D G E** LABS

1. AI EdgeLabs customer success team creates tenant and send invite for registration to particular email address of client.
2. Client sees “AI EdgeLabs Activation” email and activates tenant, creates password for Dashboard access. That user will be tenant administrator and will have maximum permissions inside of this organization. (Users get admin permissions inside the tenant).
3. Sensor API_KEY will be available on the Dashboard > Settings > API section after tenant activation and login to the platform.



4. Docker-based Installation

One of the classic cases of AI-Sensor installation is the Docker-based installation which usually looks like a standard container run. This type of installation requires Docker runtime to be installed

1. Install Docker on a specified machine (this step is optional — if no Docker installed):

```
sudo apt update && sudo apt install docker.io
```

2. Setup registry and login into AI EdgeLabs registry for access. AI EdgeLabs uses a private container registry, so REGISTRY_LOGIN and REGISTRY_PASS will be provided after tenant activation from AI EdgeLabs side.

```
docker login -u '<REGISTRY_LOGIN>' -p '<REGISTRY_PASS>' registry.edgelabs.ai
```

3. Pull the installation packet from the Private registry with the following command:

For **x86_64**:

```
docker pull registry.edgelabs.ai/ai-sensor/ai-sensor:latest
```

for **arm64**:

```
docker pull registry.edgelabs.ai/ai-sensor/ai-sensor-arm:latest
```

4. Run the installation to Docker with the following command:

In order to run Sensor installation, we need to setup Registry and AI EdgeLabs credentials in the commands below.

SENSOR_KEY - API Key data which is available at EdgeLabs Dashboard > Settings > Sensor Integration



AI **E D G E** LABS

section. That, API_KEY is generated upon tenant registration. It's required for secure communicator registration with API

REGISTRY_LOGIN - Registry username private key for access to the Private Registry.
REGISTRY_PASS - Password for access to the Private Registry.

Note about `privileged` access: this flag is required in order to have EDR-based capabilities of the AI Sensor. For example for malware detection, process and host-data verification. If we not set this flag - this malware detection and prevention

For **x86_64**:

```
docker run -d --name ai-sensor -e HOST_PATH=/host --pid=host --privileged \
-v /:/host/ --network=host --restart unless-stopped \
--cap-add=NET_ADMIN \
--env API_KEY='<SENSOR_KEY>' \
registry.edgelabs.ai/ai-sensor/ai-sensor:latest
```

For **arm64**:

```
docker run -d --name ai-sensor -e HOST_PATH=/host --pid=host --privileged \
-v /:/host/ --network=host --restart unless-stopped \
--cap-add=NET_ADMIN \
--env API_KEY='<SENSOR_KEY>' \
registry.edgelabs.ai/ai-sensor/ai-sensor-arm:latest
```

For **multiplatform** (arm64 + x86_64):

```
docker run -d --name ai-sensor -e HOST_PATH=/host --pid=host --privileged \
-v /:/host/ --network=host --restart unless-stopped \
--cap-add=NET_ADMIN \
--env API_KEY='<SENSOR_KEY>' \
registry.edgelabs.ai/ai-sensor/ai-sensor-multiarch
```

5. Verify installation:

```
docker ps
docker logs ai-sensor
```

6. Update installation:

```
docker stop ai-sensor
docker rm ai-sensor
docker pull registry.edgelabs.ai/ai-sensor/ai-sensor:latest
```





or

```
docker pull registry.edgelabs.ai/ai-sensor/ai-sensor-arm:latest (for arm64)
docker pull registry.edgelabs.ai/ai-sensor/ai-sensor-arm:latest (for
multiplatform)
docker run ... (from step 4 depending arch)
```

5. Installation to Kubernetes (Helm)

Add the *ai-sensor* repo to your environment with kubectl and helm:

Step 1:

```
helm repo add --username='<REGISTRY_LOGIN>' --password='<REGISTRY_PASS>'
ai-sensor https://registry.edgelabs.ai/chartrepo/ai-sensor
```

Step 2:

Update repo:

```
helm repo update
```

Step 3:

Add docker registry credentials:

```
kubectl create secret docker-registry regcred \
--docker-server=registry.edgelabs.ai \
--docker-username='<REGISTRY_LOGIN>' \
--docker-password='<REGISTRY_PASS>'
```

Step 4:

Install the chart from the repo:

```
helm install ai-sensor ai-sensor/ai-sensor --set api.key='<SENSOR_KEY>'
```



A I **E D G E** L A B S

SENSOR_KEY - Sensor API key can be taken from Settings -> Sensor Integration in SOC dashboard;

REGISTRY_LOGIN - Registry username private key for access to the Private Registry;

REGISTRY_PASS - Password for access to the Private Registry

