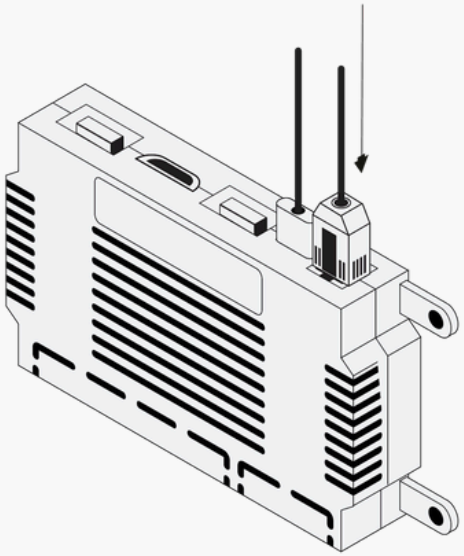
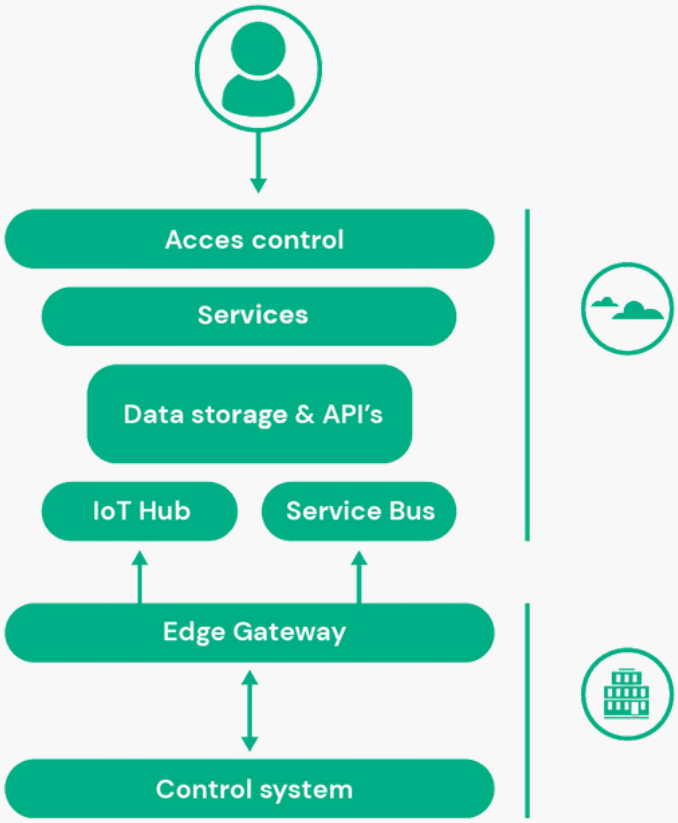
Security Policy Statement

Energy Management System (all models)



An overview of the security

The EMS, and the infrastructure behind it, can be divided into multiple security layers. The local EMS connects to the cloud. In the cloud, data is stored, and services are hosted. This is also where users gain access to their services. The security of each of these components will be discussed below.



The gateway

- To utilize cloud services, a connection needs to be established with the internet. Therefore, the EMS is utilized to provide a secure interface between the controlled device(s) and the internet. It is a closed system that can only be configured and used for Eniris services, and non-Eniris software cannot be executed on it.
- The communication between the EMS and the cloud takes place via the HTTPS protocol to ensure the integrity, confidentiality, and authenticity of the data.

Network ports for outbound connections

The EMS requires that outbound connections in the network firewall are allowed on the following ports:

- TCP port 80 & 443: General Internet connection port. Without this port, the EMS cannot function. Some monitored & controlled devices use port 80 locally for communication, but this port is not generally used for internet communication.
- TCP port 1194: Remote service connection port for updates, diagnostic services and remote support. The EMS can function without this port, but may not receive updates, and remote support is not possible. It is recommended to enable this port. You can change this port in the EMS configuration to port 1192 or any port in the range 35000 to 40000 if needed.
- TCP port 1883 and 8883: Used for MQTT; required in case the EMS must be able to receive live control signals (e.g. when coupled to the imbalance / FCR energy markets!)
- UDP port 123: NTP Port (Clock). Without this port, the EMS cannot update its internal clock. This is important for proper communication.

Network ports for inbound connections

The EMS does not require opening any network ports for inbound connections.

It is strongly discouraged and NOT necessary to configure your firewall to port forward or allow incoming TCP and UDP connections on the listed ports above! This is a serious security risk.

Domain whitelist

To avoid connectivity issues after future updates, it is recommended to whitelist all the eniris.be and eniris.io domains with a wildcard:
***.eniris.be**
***.eniris.io**

At least the following Eniris domains are used at present by the EMS:

- api.eniris.be - (telemetry & energy measurements) - TCP port 443:
- authentication.eniris.be - (authentication) - TCP port 443
- public-health.eniris.be - (device health monitoring system) - TCP port 443
- mender.eniris.be - (device update system) - TCP port 443
- mqtt.eniris.be - (MQTT) - TCP ports 1883 & 8883
- neoregistry.eniris.be - (device update system) - TCP port 443
- vpn.eniris.be - (remote support) - TCP & UDP ports 1192-1194 and 35000-40000

Encryption method of VPN remote support

Cyphers:
ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:ECDH+3DES:DH+3DES:RSA+AESGCM:RSA+AES:RSA+3DES:!aNULL:!MD5:!DSS
TLS: Minimaal TLS 1..2

Q&A

- How does the authentication of the gateway take place (against IoThub and service bus)?

Our device implements a security mechanism by utilizing refresh and access tokens, enabling automatic rotation of credentials to ensure continuous protection.

- How do we assure separation from other customer assets?

via VLAN

- Will an inventory of EMS devices be maintained? If so, where and how will it be kept up-to-date?

Yes, we use Mender to update and maintain our devices. Updates are announced via email, and if you prefer not to enable auto-updates, you can disable them locally on your EMS.