

Access credentials and sign-in

Access to the MANDÍK air handling unit visualisation

Every MANDÍK unit has its **own login credentials**, tied to a specific order. Access to the visualisation is through the unit's built-in web server – it is therefore part of the network wiring described on the following pages. Keep this sheet together with the unit documentation.

Your unit

Item	Value
Username	—
Password – user level	—
Password – service level	—
Visualisation address – ETH0 (factory default)	192.168.1.101/hmi
Visualisation address – ETH1 (factory default)	192.168.131.101/hmi
Remote access (cloud)	climan.online

The username and both passwords are filled in per order (generated in the visualisation at /hmi/credentials, or computed according to authLocal.js).

Use the service password prudently

The service level allows changes to the unit configuration – it is intended for **experienced users**. Make changes at the service level after consulting the MANDÍK service department; incorrect settings can take the unit out of operation.

How to sign in

- **From the local network:** on a computer, tablet or phone connected to the same network as the unit, enter one of the addresses listed above into the browser. The ETH0 interface can be reconfigured to a different static IP address or to DHCP – the network settings are described in detail on page 2.
- **From the touchscreen** (if supplied): the visualisation is available directly, with no further setup.
- **Remotely via the cloud:** if the unit is connected to the cloud, sign in at `climan.online` – you will see the unit from anywhere. *The network preparation for the connection is described on page 2 of this sheet – hand it over to your IT.*

Access levels

- **User** – everyday operation of the unit: mode selection, setpoint temperatures, time programs, year calendar, alarm overview.
- **Service** – unit configuration and service interventions (see the notice above).

Loss of access credentials

If you lose the credentials, contact MANDÍK technical support – access to your unit can be restored at any time. Do not pass the credentials on to third parties.

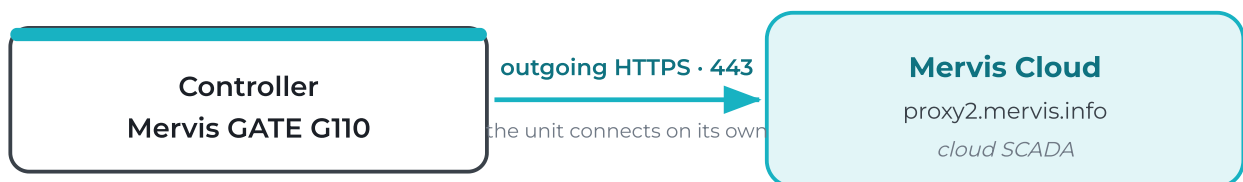
Cloud connection

Procedure for local IT – how to connect the Mandík controller to the network so that it connects to the cloud (Mervis Proxy Service)

The Mandík controller is a **Mervis GATE G110** type and has two ethernet ports – ETH0 and ETH1 (network wiring for multiple units is on pages 3–5). It connects to the cloud **on its own** – it establishes an outgoing connection to the `proxy2.mervis.info` server. The proxy address is set in the unit by Mandík during commissioning. The local IT's only task is to **connect the unit to a network with internet access** – a public IP address, VPN or port forwarding are not needed.

Connection procedure

- 1. Connect the unit to the network.** Plug the Mandík unit's ethernet cable into a network (outlet / switch / VLAN) that has internet access.
- 2. Check the unit's network settings.** From the factory the unit is set to static IP addresses: **ETH0** `192.168.1.101`, **ETH1** `192.168.131.101`. You can leave ETH0 as is, change it to a different static IP, or switch it to DHCP – but **ETH0 must not be in the same network range as ETH1** (192.168.131.x). For the cloud connection the unit must have a **default gateway and DNS** filled in – with DHCP these are added automatically, with your own static IP they must be entered manually. The DNS need not be in the same network and is usually not the gateway address — a common default public DNS is `8.8.8.8`, which works on most networks. If the network blocks it, ask the local IT for the internal DNS address. For a permanent address we recommend a **DHCP reservation** based on the unit's MAC address.
- 3. Allow outgoing internet access.** From that network, outgoing **HTTPS (TCP 443)** must be permitted and **DNS** resolution must work so the unit can reach `proxy2.mervis.info`. On a normal network this is met automatically; only where outgoing traffic is restricted (whitelist) allow the destination `proxy2.mervis.info`.
- 4. Do not set up anything incoming.** No port forwarding, no public IP and no VPN – all communication is outgoing and encrypted from the unit all the way to the cloud.



No incoming connection reaches the unit – all communication is outgoing and encrypted.

Cloud security

- The cloud operator is certified to **ISO/IEC 27001:2022**, ready for the requirements of the NIS2 directive.
- Encrypted HTTPS** all the way from the unit to the user, **two-factor authentication (2FA)**.
- Hosting in **certified data centres in the EU**, backups every 24 hours to two independent locations.
- For critical infrastructure a **complete on-premise installation** can also be supplied.

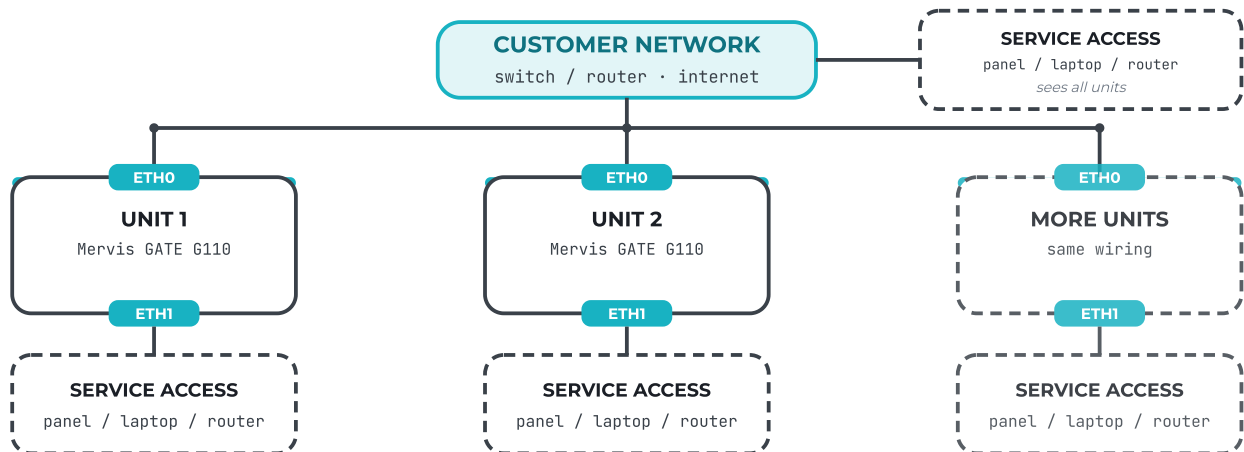
The most common reasons a unit fails to connect

1) a static IP address **without a default gateway or DNS filled in** – the unit then communicates on the local network but cannot reach the internet; 2) the network **blocks outgoing HTTPS** or **DNS** resolution of `proxy2.mervis.info` does not work.

Variant 1 – star

Each unit with its own connection into a single customer network

The **GATE G110** has two ethernet ports. In this variant each unit's ETH0 runs on its own cable into the customer network – a switch on the customer side is enough, and from a single point in that network all units are reachable at once. ETH1 stays for service access directly at the unit – a panel, laptop or router as needed, on **any** unit.



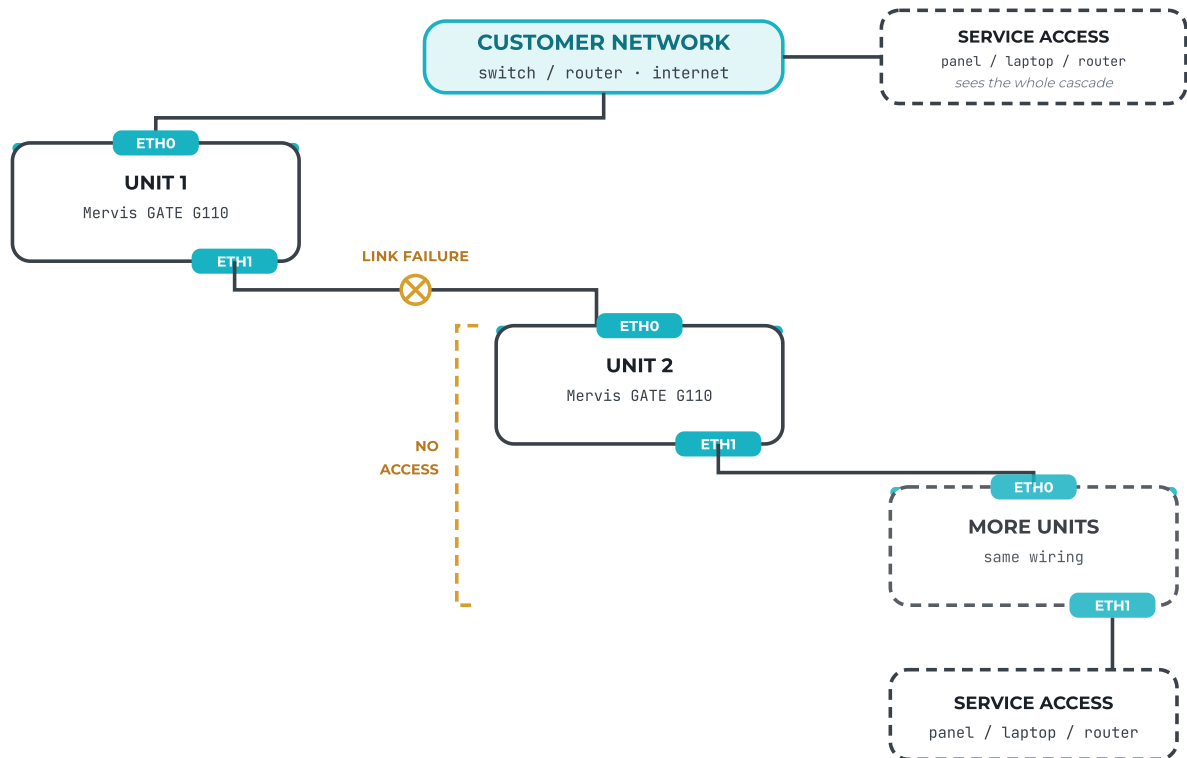
Service access can be connected directly to the customer network – from there all units are reachable at once; or locally on the ETH1 of any unit, with the same result. The ETH0/ETH1 pattern simply repeats with further units.

The units are network-independent — disconnecting or a failure of one does not affect the others, even though they are all in a single customer network. The trade-off: a connection from the customer to every unit.

Variant 2 – cascade

PLC as a switch – units chained through ETH0 / ETH1

Only the **first unit** is connected to the customer network. Each further unit hangs off the ETH1 of the previous one – addressing can be a static IP, or even active DHCP. Service access (panel / laptop / router) can be connected directly to the customer network just as in variant 1 – or locally on the ETH1 of the **last unit**, the only one that has it free.



Service access can also be connected directly to the customer network (sees the whole cascade) – or locally on the ETH1 of the last unit, the only one that has it free.

Breaking one link disconnects everything behind it too

In a cascade the GATE G110 acts as an unmanaged switch with no loop protection. The cascade must stay a chain – never wire it back into a loop.

Comparison and notes for the designer

When to use which variant

Criterion	Variant 1 — star	Variant 2 — cascade
Connections from the customer	1 per unit (N total)	1 total — only the first unit
Addressing	DHCP (required for cloud) or static IP	DHCP (required for cloud) or static IP — configured on each unit separately
Failure of a single link	only that unit is affected	all units behind it drop out too
Service access	on the customer network (sees all) or locally on the ETH1 of each unit	on the customer network (sees the whole cascade) or locally on the ETH1 of the last unit
Cabling between units	none — only to the customer switch	unit to unit, they must be close together along the route

DHCP and cloud

For a connection to the **Mervis Cloud** the port in question must have **DHCP** (see page 2) – a static IP set directly in the PLC disables the cloud. If you want both the cloud and a „fixed“ address, the solution is a **DHCP reservation** on the customer's DHCP server, not a static configuration directly in the PLC.

Further notes

- Copper ethernet (Cat5e / Cat6): max. 100 m per segment. In a cascade this applies to each link separately, not to the whole route.
- For variant 2, plan and write down the unit addresses in advance. Manual static configuration across multiple units is the main source of typos and address conflicts.
- Both variants can be combined within a single project in groups — units close together in a cascade, distant ones on their own. The topology need not be all-or-nothing.