

HID® M1

Transparent Gateway

Installation and Specifications

PLT-07917, Rev. A.0
December 2025



Copyright

© 2025 HID Global Corporation/ASSA ABLOY AB. All rights reserved.

This document may not be reproduced, disseminated, or republished in any form without the prior written permission of HID Global Corporation.

Trademarks

HID GLOBAL, HID, the HID Brick logo, HID Linq, HID Reader Manager, and HID Signo are trademarks or registered trademarks of HID Global, ASSA ABLOY AB, or its affiliate(s) in the US and other countries and may not be used without permission. All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.

DESFire, DESFire EV1, DESFire EV2, and DESFire EV3 are registered trademarks of NXP B.V. and are used under license.

Contacts

For technical support, please visit: <https://support.hidglobal.com>.

What's new

Date	Description	Revision
December 2025	Initial release.	A.0

A complete list of revisions is available in [Revision history](#).

Introduction	6
1.1 Scope	7
1.2 Product overview	7
1.3 Benefits of a Transparent Architecture	7
Solution Components	8
2.1 Hardware	9
2.1.1 Key Module	9
2.1.2 Main Node	10
2.1.3 IO Module	11
2.1.4 Transparent HID Signo reader	12
2.1.5 Card credentials	12
2.2 Software	12
2.2.1 HID Linq Key Manager	12
2.2.2 Main Node admin interface	12
2.2.3 HID Reader Manager app	12
Before Installation	13
3.1 Prerequisites	14
3.1.1 Existing PACS	14
3.1.2 Controller compatibility	14
3.1.3 Credentials	14
3.1.4 Software access	14
3.1.5 Secure environment	14
3.1.6 Network access	14
3.2 Required tools and materials	14
3.3 Safety precautions	15
System Architecture	16
4.1 System architecture overview	17
4.2 Typical deployment diagram	17
4.3 Key data flows	17
Installation Steps	18
5.1 Step 1: Prepare the Key Module using HID Linq Key Manager	19
5.1.1 Install HID Linq Key Manager	19
5.1.2 Connect the Key Module to a secure PC	19
5.1.3 Create Keysets and load configuration	19
5.1.4 Eject and disconnect the Key Module	19
5.2 Step 2: Install the hardware	20
5.2.1 Mount the Main Node	20
5.2.2 Mount the IO Module(s)	20

5.2.3 General wiring guidelines	21
5.2.4 Wiring the Main Node and IO Modules power	21
5.2.5 Wiring the Main Node TAMPER, AC FAIL, and BATT FAIL inputs	21
5.2.6 Wiring the IO Module to the Main Node (Ethernet network)	22
5.2.7 Wiring readers to the IO Module	23
5.2.8 Wiring the IO Module to an existing PACS controller (OSDP)	23
5.2.9 Wiring the IO Module TAMPER, BATT FAIL, and AC FAIL inputs	24
5.3 Step 3: Configure DIP switches	25
5.3.1 Main Node DIP switches	25
5.3.2 Main Node DIP switch settings	25
5.3.3 IO Module DIP switches	26
5.4 Step 4: Initial power up and network access	27
5.4.1 Powering on	27
5.4.2 Accessing the Main Node admin interface	27
5.5 Step 5: First-time login and secure password setup	28
5.5.1 Network configuration (Main Node)	28
5.5.2 Date and time configuration (NTP)	29
5.6 Step 6: System configuration via the Main Node admin interface	30
5.6.1 Install and Pair the Key Module	30
5.6.2 Pair IO Modules	31
5.6.3 Pair readers	32
5.6.4 Configure IO Module OSDP parameters (for PACS controller)	33
5.7 Step 7: Reader firmware update using HID Reader Manager app	34
Operational Information	35
6.1 Operational information overview	36
6.2 Status LEDs	36
6.2.1 Main Node initialization	36
6.2.2 Main Node running	36
6.2.3 Status LEDs - IO Module	37
Normal Operational Flows	38
7.1 Credential read and forwarding	39
7.2 Controller command passthrough	39
7.3 Tamper and error reporting	39
7.3.1 Reported conditions	39
7.4 Unavailable functionality in normal operation mode	39
Maintenance and Troubleshooting	40
8.1 Firmware updates	41
8.2 Main Node and IO Module firmware	41

8.2.1 Download firmware	41
8.2.2 Enable admin mode	41
8.2.3 Login to the admin interface	41
8.2.4 Update Main Node firmware (if needed)	41
8.2.5 Update IO Module firmware (if needed)	41
8.2.6 Perform manual system tests	41
8.2.7 Return to normal operation	42
8.3 Key Module firmware	42
8.4 Factory reset procedure	42
8.4.1 Important considerations before factory reset	42
8.4.2 Factory resetting an IO Module	42
8.4.3 Factory resetting the Main Node	43
8.4.4 Common issues and resolutions	43
Specifications	44
9.1 Main Node (M1-1100)	45
9.2 Key Module (M1-1001)	45
9.3 IO Module (M1-1002)	46

Section 01

Introduction

1.1 Scope

This document provides detailed instructions for the installation, initial setup, and configuration of the HID M1 Transparent Gateway solution. The document is intended for trained security technicians familiar with Physical Access Control Systems (PACS), network configuration, and Open Supervised Device Protocol (OSDP) communication.

1.2 Product overview

The HID M1 Transparent Gateway enhances the security of existing physical access control systems by implementing a transparent architecture. HID M1 is installed "in-line" between existing OSDP-compatible PACS controllers and HID Signo™ readers. This approach moves cryptographic operations from potentially vulnerable readers to a protected area within the building.

The HID M1 solution includes the following hardware components:

- Main Node
- Key Module
- IO Module(s)
- Transparent HID Signo readers

HID M1 supports the authentication of custom DESFire EV1/2/3 credentials using sovereign encryption keys managed by your organization, providing greater control and security over your access control infrastructure.

1.3 Benefits of a Transparent Architecture

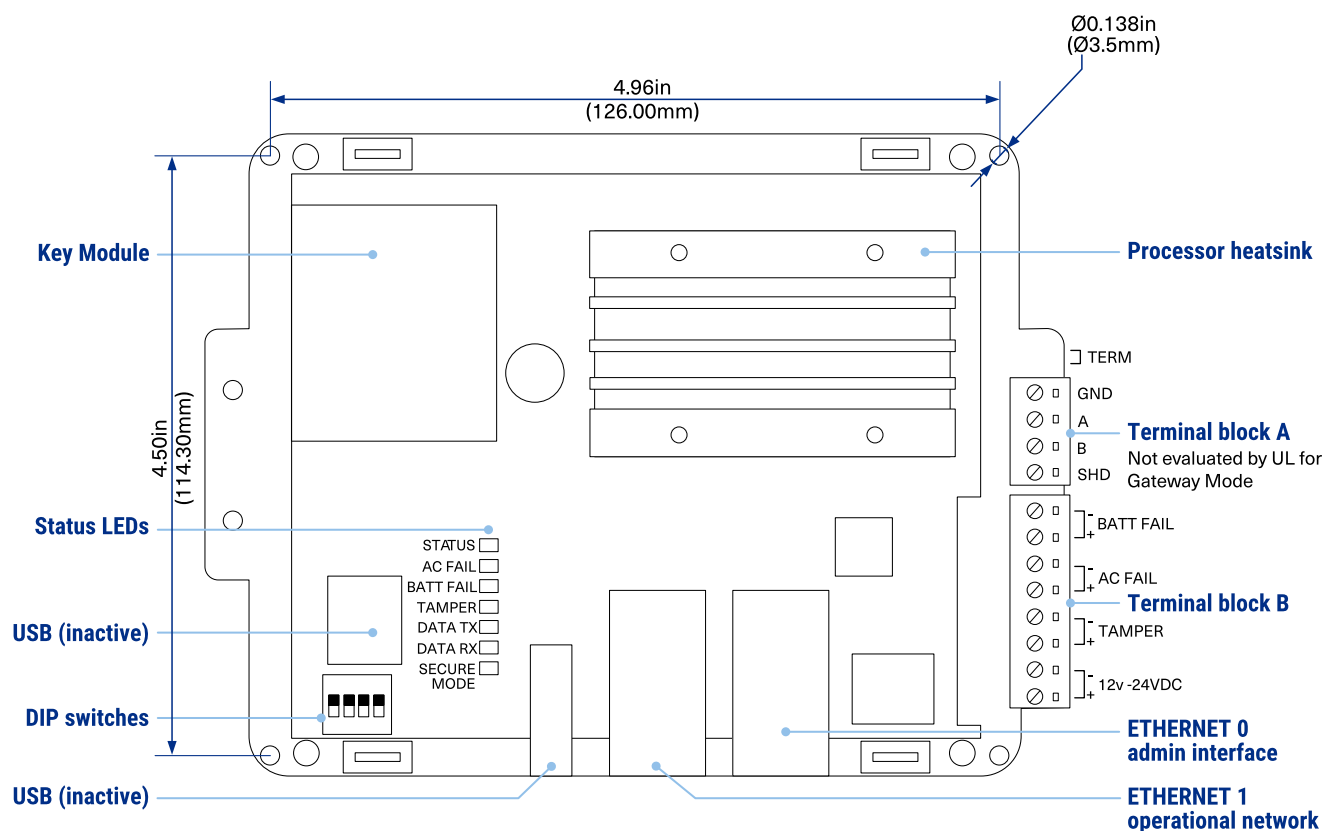
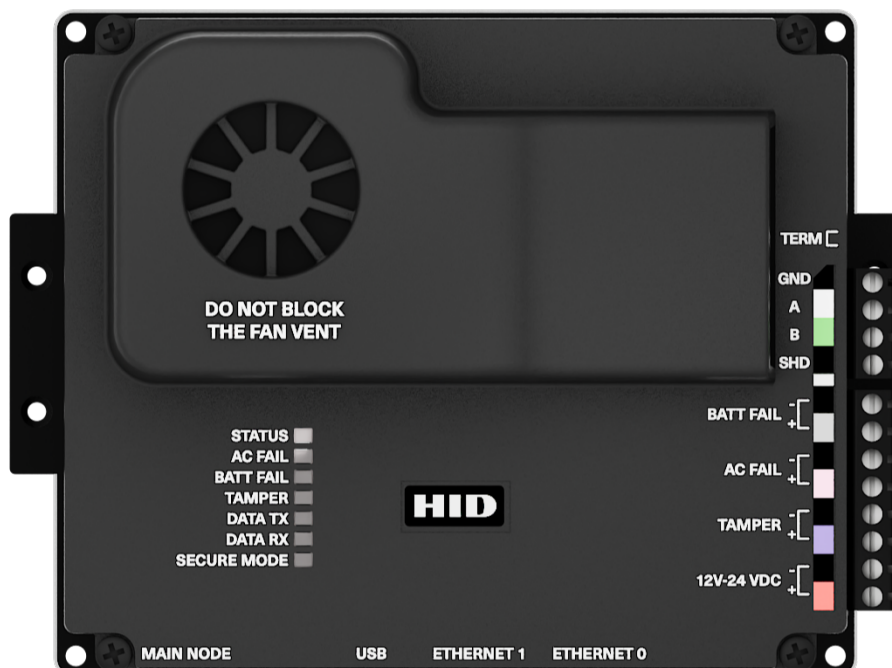
- **Enhanced security:** Moves the credential decryption and authentication processes from the publicly accessible reader to the secure Key Module located within the Main Node in a protected area.
- **Reduced attack surface:** Encrypts communication between the reader and the secure processing environment, minimizing the risk of data interception or reader tampering.
- **Protection of sovereign keys:** Ensures that your custom encryption keys remain within your control and are not managed by or shared with any third party.
- **Upgrade path:** Allows existing OSDP-based PACS installations to benefit from transparent readers without requiring a full replacement of the existing system.

Section 02

Solution Components

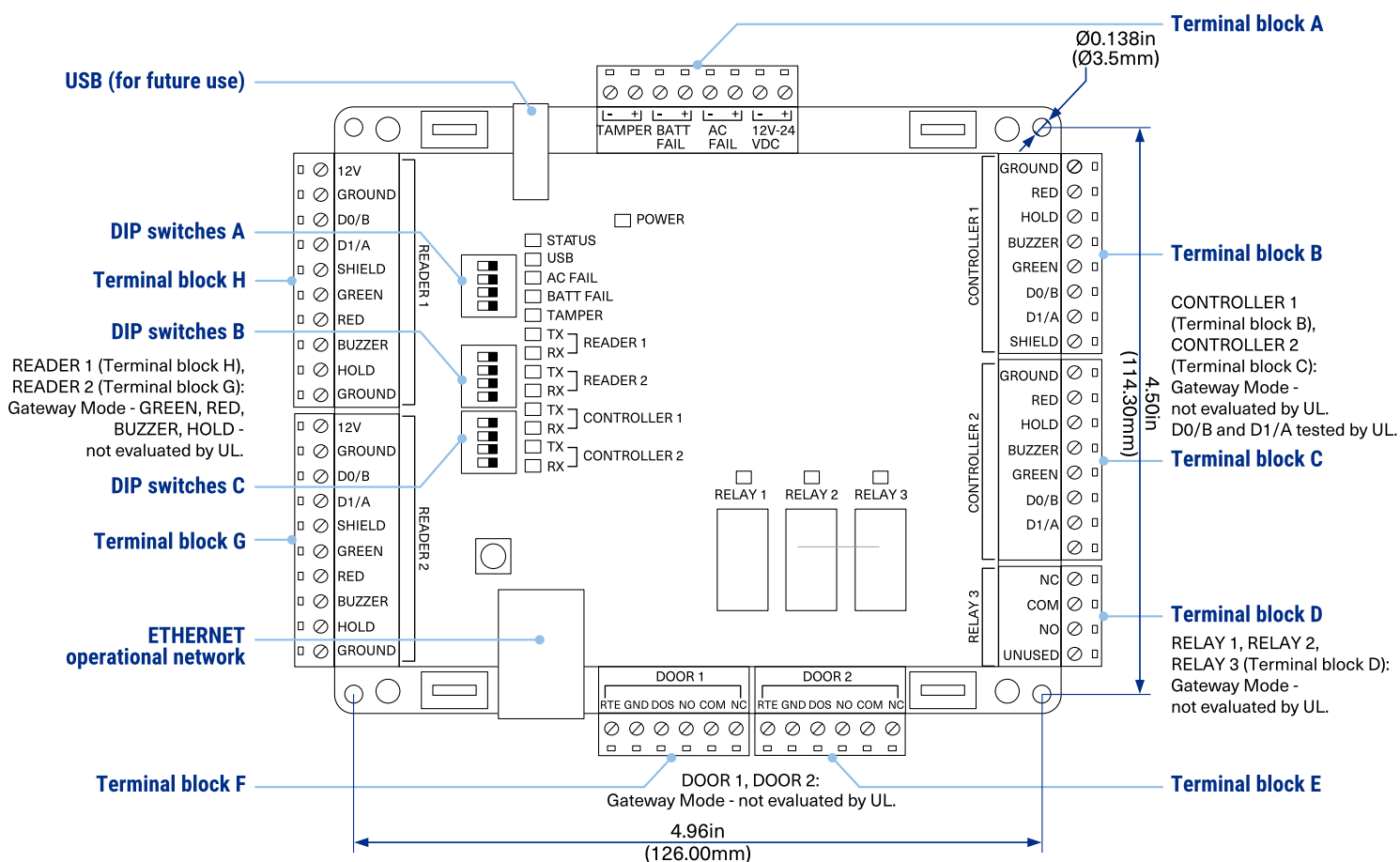
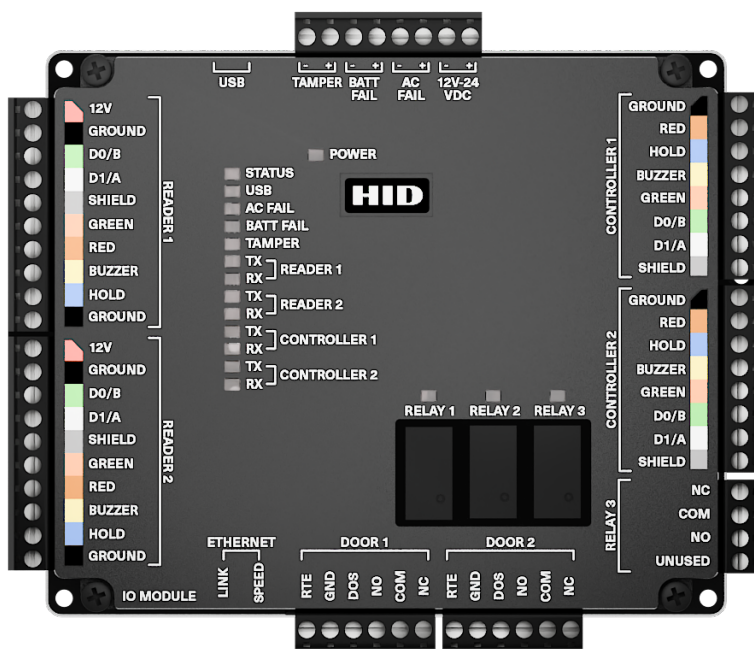
2.1.2 Main Node

The central processing unit of the gateway. The Main Node houses the Key Module and manages communication with downstream devices and configuration via the admin interface.



2.1.3 IO Module

Connects the Main Node to transparent HID Signo™ readers and the existing PACS controller. Each IO Module supports one or two reader/controller channels.



2.1.4 Transparent HID Signo reader

Standard HID Signo readers updated to SP11+ firmware support transparent conversion via a specific Device Configuration ID (DCID). These readers pass encrypted card data to the Key Module for processing.



2.1.5 Card credentials

Custom-programmed DESFire EV1/2/3 credentials compatible with the keys provisioned on the Key Module.

2.2 Software

2.2.1 HID Linq Key Manager

Used to provision your Key Module and inject custom encryption keys. Contact your HID representative for more information, or refer to the *HID Linq Key Manager User Guide* (PLT-08195).

2.2.2 Main Node admin interface

A web-based user interface hosted on the Main Node. Used for:

- System configuration (network settings, Key Module, IO Modules, readers)
- Monitoring
- Viewing system logs

2.2.3 HID Reader Manager app

Can be downloaded from the Google Play or the Apple app store. HID Reader Manager™ can be used to upgrade existing HID Signo readers to a firmware that allows them to perform transparent card reads.

Section 03

Before Installation

3.1 Prerequisites

3.1.1 Existing PACS

A functional PACS headend and controller must be installed and operational.

3.1.2 Controller compatibility

The existing PACS controller port that will be connected to the HID M1 solution must support OSDP v.2 for reader communication.

3.1.3 Credentials

Custom DESFire EV1/2/3 card credentials programmed for use with this system must be available for testing. The DESFire read key and SNMP keys must be accessible in plain text.

3.1.4 Software access

- **HID Linq™ Key Manager:** Obtain the LinqKeyManager.exe file from your HID representative or download from the [HID Developer Portal](#).
- **HID Reader Manager™ app:** Download onto a compatible mobile device from the Apple App Store or Google Play Store.
- **Firmware files:** Download the latest firmware files for the Main Node, IO Module(s), and transparent HID Signo™ readers from the [HID Developer Portal](#). Store these on a PC/laptop that will be accessible during installation.

3.1.5 Secure environment

A secure, controlled environment is required for provisioning the Key Module using HID Linq Key Manager.

3.1.6 Network access

If the Main Node will connect to an existing network, ensure the following are prepared:

- Necessary IP addresses
- Subnet masks
- Gateway information
- Firewall rules

3.2 Required tools and materials

- Standard technician toolkit (screwdrivers appropriate for mounting and terminal blocks, wire strippers/crimpers, etc.)
- Ethernet cables
- RS-485 cabling
- Power supply wiring
- Mounting hardware:
 - Supplied screws: 3.5 mm x 25 mm (0.138" x 1") for direct mounting.
 - If DIN rail mounting: Brackets (2) - Phoenix Contact, USA 10 Series Rail Adapter, part number 1201578; Screws (4) - Selftapping, countersunk, 3.0 mm x 10 mm (or 3.0 mm x 8 mm). Sold separately.

- PC/Laptop:
 - Windows 11 to run HID Linq Key Manager.
 - Ethernet port for direct connection to the Main Node admin interface.
- USB-C cable for connecting the Key Module to the PC.

3.3 Safety precautions

WARNING: ELECTRICAL HAZARD! ALWAYS DISCONNECT ALL POWER SOURCES (AC MAINS AND ANY BACKUP BATTERIES) TO THE PACS CABINET AND RELATED EQUIPMENT BEFORE MAKING ANY WIRING CONNECTIONS OR INSTALLING/REMOVING COMPONENTS.

Caution:

- **ESD SENSITIVE DEVICES!**
Use proper Electrostatic Discharge (ESD) precautions (for example, wrist strap, antistatic mat) when handling the Key Module, Main Node, and IO Modules to prevent damage.
- Follow all local and national electrical codes and safety regulations.

Important:

- Ensure the Main Node is completely powered OFF before inserting or removing the Key Module. Failure to do so may damage the components.
- Installation should only be performed by qualified personnel.

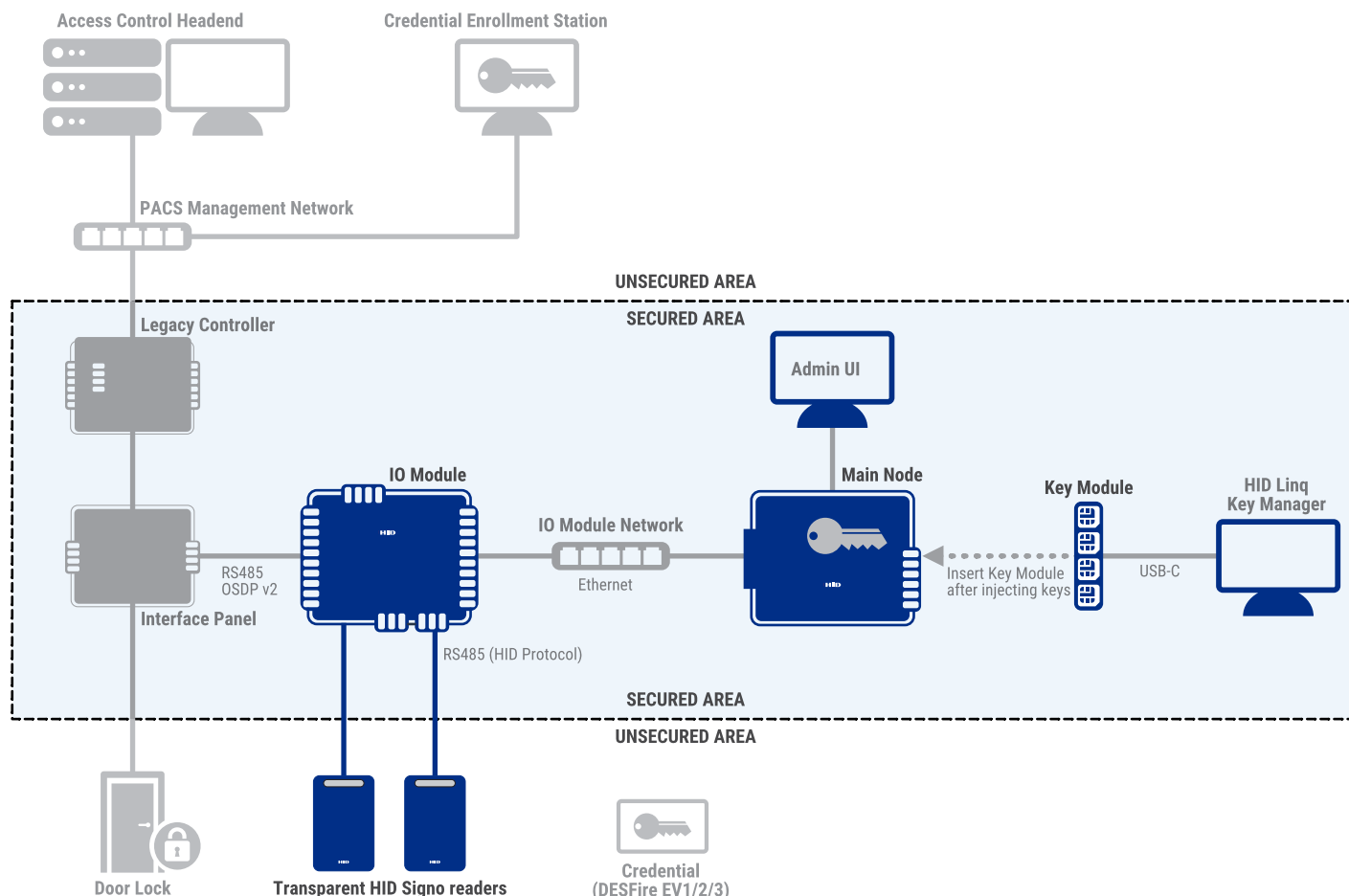
Section 04

System Architecture

4.1 System architecture overview

The HID M1 Transparent Gateway is designed to integrate seamlessly with existing OSDP-based access control systems. The Main Node and IO Module(s) are installed between the existing PACS controller and the HID Signo™ readers.

4.2 Typical deployment diagram



4.3 Key data flows

1. User presents a DESFire credential to a transparent HID Signo reader.
2. The reader captures encrypted card data and transmits the data via an HID transparent protocol to the connected IO Module.
3. The IO Module forwards the encrypted data over Ethernet to the Main Node.
4. The Key Module within the Main Node attempts to decrypt and authenticate the credential data using the provisioned keys.
5. If successful, the Main Node constructs an OSDP message containing the configured output format.
6. The Main Node sends this OSDP message back to the IO Module.
7. The IO Module forwards the OSDP message to the existing PACS controller for authorization.
8. The PACS controller processes the card data and controls door hardware as usual.
9. LED/Buzzer commands from the controller are passed back through the system to the reader.

Section 05

Installation Steps

5.1 Step 1: Prepare the Key Module using HID Linq Key Manager

The Key Module must be provisioned with your custom DESFire encryption keys and configuration before it can be used in the Main Node. Only AES128 is currently supported. This process uses the HID Linq™ Key Manager software and must be performed in a secure, controlled environment.

Note: Ensure the Main Node is powered OFF if you are removing an existing Key Module, or before inserting a newly provisioned one.

5.1.1 Install HID Linq Key Manager

1. If not already installed, obtain the LinqKeyManager.exe file from your HID representative or the [HID Developer Portal](#).
2. Follow the instructions in the *HID Linq Key Manager User Guide* (PLT-08195) to set up the software on a secure Windows 11 PC.

5.1.2 Connect the Key Module to a secure PC

Carefully connect the HID M1 Key Module to the secure PC using a USB-C cable.

5.1.3 Create Keysets and load configuration

1. Launch HID Linq Key Manager.
2. Refer to the *HID Linq Key Manager User Guide* (PLT-08195) for detailed instructions on:
 - Creating a database (if first-time use).
 - Creating a keystore.
 - Adding your custom DESFire and pairing key values to the keystore.
 - Creating DESFire and SNMP (if applicable) keysets.
 - Creating a configuration profile.
 - Loading a Main Node Pairing Key.
 - Applying the configuration to the connected Key Module.

5.1.4 Eject and disconnect the Key Module

1. Once provisioning is complete and confirmed successful in HID Linq Key Manager, use any "eject" functionality provided by Windows.
2. Carefully unplug the USB-C cable from the Key Module.
3. Store the provisioned Key Module in an anti-static bag until ready for installation into the Main Node.

5.2 Step 2: Install the hardware

Choose a secure location for the Main Node and IO Module(s), typically within the same cabinet as the existing PACS controller or a dedicated secure enclosure.

5.2.1 Mount the Main Node

Select a suitable flat surface or DIN rail within the secure cabinet.

Direct mounting

Use the four 3.5 mm x 25 mm (0.138" x 1") screws to mount the Main Node directly.



DIN rail mounting

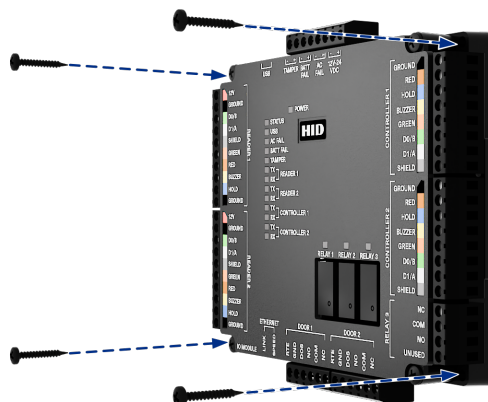
1. Attach two DIN rail adapter brackets (Phoenix Contact, Part No. 1201578 or equivalent) to the back of the Main Node using four 3.0 mm x 10 mm (or 3.0 mm x 8 mm) self-tapping, countersunk screws.
2. Clip the Main Node onto the DIN rail.

M1 to Mercury bracket mounting

Order the mounting bracket (M1-1100-1002-MB) accessory kit for mounting the Main Node or IO Module on top of Mercury LP or MP boards.

5.2.2 Mount the IO Module(s)

IO Modules are typically mounted near the Main Node or close to the termination points for reader and controller cables. Follow the same direct mounting or DIN rail mounting procedures as described for the Main Node, using the appropriate screws.



5.2.3 General wiring guidelines

- Plan cable routes carefully to avoid interference and ensure easy access for maintenance.
- Use appropriate cable types as specified.
- Label all cables clearly at both ends.
- Ensure all connections are secure and correctly terminated.

5.2.4 Wiring the Main Node and IO Modules power

The Main Node and IO Modules require 12 to 24V DC power.

1. Identify a suitable 12-24V DC power source (typically from the existing PACS power supply).
2. Using minimum 18 AWG wire, connect the positive (+) and negative (-) terminals from the power source to the corresponding power input terminals on the Main Node. Observe correct polarity.



3. Repeat step 2 for each IO Module.

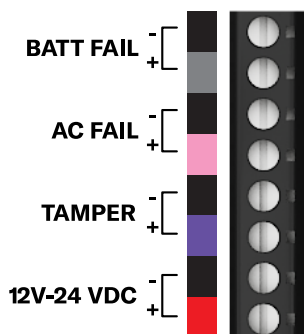


Caution: GROUNDING! Connect the GND (Ground) terminal of the Main Node (and optionally IO Modules, if separate power supplies are used) to a single, reliable earth ground point within the system (for example the cabinet chassis ground). Avoid multiple earth ground connections for the same power system to prevent ground loops.

5.2.5 Wiring the Main Node TAMPER, AC FAIL, and BATT FAIL inputs

The Main Node includes three inputs for monitoring critical system and power conditions:

- **TAMPER** – Cabinet tamper detection
- **AC FAIL** – Loss of primary AC power
- **BATT FAIL** – Battery backup fault



Input logic

Each input follows a **closed-contact convention**:

- **Closed contact** = Normal operating state (safe)
- **Open contact** = Alarm condition or fault

External power monitoring

The HID M1 system is typically powered by an external Power Supply Unit (PSU), which converts mains AC power to the DC voltage required by the system.

- The PSU, or an optional **Uninterruptible Power Supply (UPS)** (providing battery backup during AC outages), often includes status relay outputs.
- The **AC FAIL** and **BATT FAIL** inputs on the Main Node are designed to connect to these relay outputs.

Wiring the inputs

- **Cabinet tamper (TAMPER)** – Connect the cabinet door tamper switch wires to the **TAMPER** input terminals.
- **AC power status (AC FAIL)** – Connect the “**AC Input Fail**” relay output from your UPS (indicating the UPS is running on battery) or the “**AC Fail**” relay output from your PSU to the **AC FAIL** input terminals on the Main Node.
- **Battery backup status (BATT FAIL)** – Connect the “**Low Battery**,” “**Battery Discharged**,” or “**Battery Fault**” relay output from your UPS or PSU (if it manages its own batteries) to the **BATT FAIL** input terminals on the Main Node.

Note: If any monitoring input (TAMPER, AC FAIL, BATT FAIL) is not used, install a short jumper wire across its terminals. This simulates a normally closed-contact state.

Important:

- Always check the documentation for your PSU and UPS to identify their relay outputs and confirm their logic (for example, normally open or normally closed).
- The Main Node expects a closed contact for a normal/safe condition.

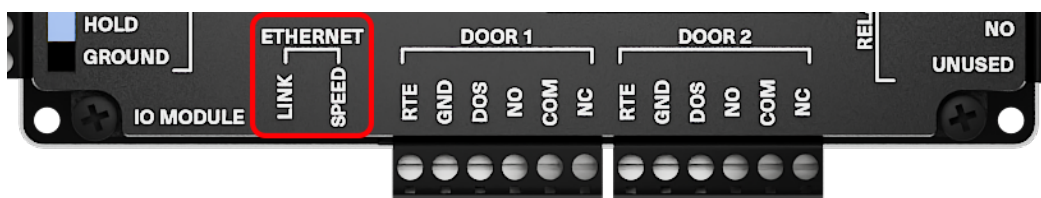
5.2.6 Wiring the IO Module to the Main Node (Ethernet network)

IO Modules communicate with the Main Node via an Ethernet network.

1. Connect an Ethernet cable (CAT-5 or newer) from the ETHERNET 1 port on the Main Node to:



- An Ethernet port on a dedicated network switch, if multiple IO Modules are used or if connecting to a wider management network.
 - Directly to the Ethernet port on a single IO Module if only one is used and no switch is present.
2. For each IO Module, connect an Ethernet cable from its ETHERNET port to the network switch (or directly to the Main Node if applicable for a single IO Module setup).

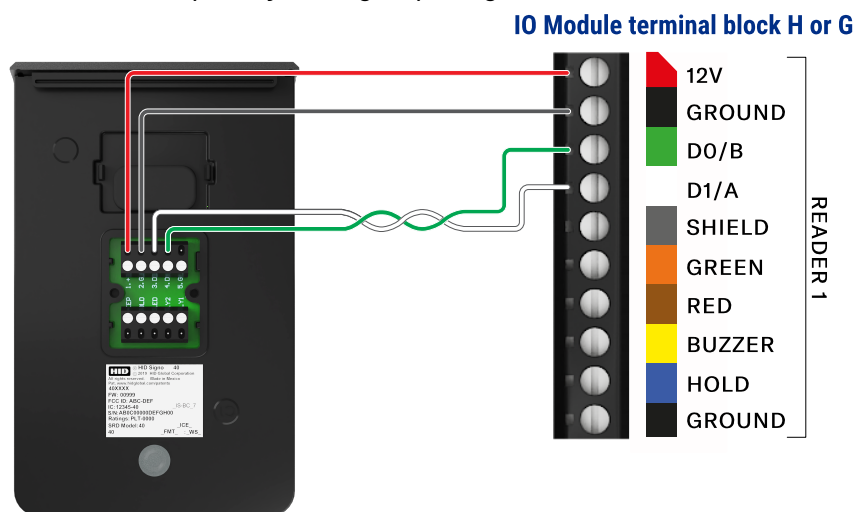


5.2.7 Wiring readers to the IO Module

Each IO Module supports HID transparent communication with transparent HID Signo™ readers.

1. For each reader connected to an IO Module:

- Use 4-conductor, shielded, twisted-pair cable suitable for RS-485.
- Connect the data lines (D1/A, D0/B), Power (+V), and Ground (GND) from the HID Signo reader to the corresponding READER 1 (terminal block H) or READER 2 (terminal block G) port terminals on the IO Module. Ensure correct polarity and signal pairing.



2. Termination:

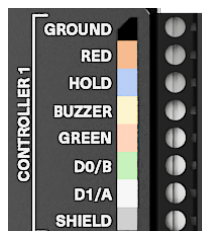
- The RS-485 bus requires 120Ω termination at both ends of the bus segment.
- The IO Module has internal termination resistors for its reader ports. If the IO Module reader port is at one end of the bus segment (i.e., only one reader connected directly to it), install the corresponding jumper (JMP1 for READER 1, JMP2 for READER 2) on the IO Module PCB to enable termination.
- The HID Signo reader also has termination capabilities. Ensure termination is enabled on the reader ONLY if it is the other end of the bus segment.

Important: Only one transparent HID Signo reader can be connected to each IO Module reader port. These ports do not support multi-drop reader connections.

5.2.8 Wiring the IO Module to an existing PACS controller (OSDP)

The IO Module acts as an OSDP peripheral (like a reader) to the existing PACS controller.

- For each controller connection to an IO Module:
 - Use 4-conductor, shielded, twisted-pair cable suitable for RS-485.
 - Connect the reader terminal data lines on the controller (D1/A, D0/B) to the corresponding CONTROLLER 1 (or CONTROLLER 2) port terminals on the IO Module.



5.2.9 Wiring the IO Module TAMPER, BATT FAIL, and AC FAIL inputs

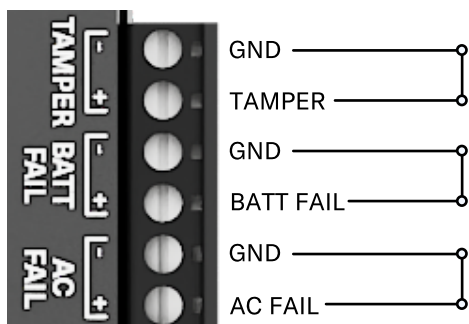
The HID M1 IO module includes three dedicated inputs for monitoring system integrity:

- **TAMPER** – Cabinet tamper detection
- **BATT FAIL** – Battery backup failure detection
- **AC FAIL** – AC power loss detection

Input logic

Each input uses a **closed-contact convention**:

- **Closed contact** = Normal operating state (safe)
- **Open contact** = Alarm condition or triggered event



External power monitoring

The IO Module is typically powered by an external Power Supply Unit (PSU), which converts mains AC power to the DC voltage required by the system.

- The PSU, or an optional **Uninterruptible Power Supply (UPS)** (providing battery backup during AC outages), often includes status relay outputs.
- The **AC FAIL** and **BATT FAIL** inputs on the HID M1 IO are designed to connect to these relay outputs.

Note: If any monitoring input (TAMPER, AC FAIL, BATT FAIL) is not used, install a short jumper wire across its terminals. This simulates a normally closed-contact state.

Important:

- Always refer to the documentation for your specific PSU and UPS to identify their relay status outputs and confirm their logic (for example, normally open or normally closed).
- The HID M1 IO expects a closed contact for a normal/safe condition.

5.3 Step 3: Configure DIP switches

DIP switches on the Main Node and IO Modules control their operating modes and default network settings. Configure the DIP switches before initial power-up for configuration, or ensure they are correctly set for normal operation. Settings are read on power-up (a power cycle is required for changes to take effect).

5.3.1 Main Node DIP switches

Remove the four screws on the Main Node's plastic cover to access the DIP switches.

Important: Disconnect the fan cable from the PCB before fully removing the cover.

The Main Node has a block of four DIP switches (see [2.1.2 Main Node](#)).

5.3.2 Main Node DIP switch settings

1	2	3	4	Mode description	IP address mode
ON	ON	ON	ON	Normal operation	Not applicable
ON	OFF	OFF	OFF	Admin mode	Default static
ON	OFF	ON	OFF	Admin mode	From config
ON	ON	OFF	OFF	Admin mode	DHCP
OFF	ON	ON	OFF	Factory reset (use with caution)	-

Default static IP

192.168.0.251 (Subnet: 255.255.255.0)

For initial setup

Use one of the admin modes. The default static IP option is recommended if no DHCP server is available on the admin connection.

Normal operation

After configuration, change to the normal operation mode.

Admin mode

Provides deeper system access, typically used for:

- Firmware updates
- Pairing devices
- Viewing logs

Factory reset

This erases all configuration. See [8.4 Factory reset procedure](#) for the full procedure and warnings.

5.3.3 IO Module DIP switches

Remove the four screws on the IO Module's plastic cover to access the DIP switches.

The IO Module has three blocks of four DIP switches (see [2.1.3 IO Module](#)).

Note: Block B and C are not used with the Transparent Gateway solution.

1	2	3	4	Mode description
ON	ON	ON	ON	Normal operation
ON	OFF	OFF	OFF	Admin mode (for pairing and discovery)
OFF	ON	ON	OFF	Factory reset (use with caution)

For initial setup and pairing

Set IO Modules to admin mode.

Normal operation

After pairing and configuration, set to normal operation.

Factory reset

This erases IO Module configuration. See [8.4 Factory reset procedure](#) for the full procedure and warnings.

5.4 Step 4: Initial power up and network access

5.4.1 Powering on

1. Ensure Main Node DIP switches are set to one of the admin modes and the IO Module is set to admin mode (as described in **5.3 Step 3: Configure DIP switches**).
2. Apply 12-24V DC power to the Main Node and all connected IO Modules.
3. Observe status LEDs on the devices for power-on indications (see **6.2 Status LEDs**).

5.4.2 Accessing the Main Node admin interface

The Main Node admin interface is a web-based UI used for configuration.

1. **Network connection:** Connect your PC/laptop Ethernet port directly to the ETHERNET 0 (admin) port on the Main Node using an Ethernet cable.
2. **PC Network configuration:**
 - If the Main Node DIP switches are set to default static IP (for example 192.168.0.251), configure your PC's Ethernet adapter to a static IP address in the same subnet (for example IP: 192.168.0.100, Subnet Mask: 255.255.255.0).
 - If the Main Node DIP switches are set to DHCP client, ensure your PC is also set to obtain an IP address automatically, and a DHCP server is active on this direct link if necessary.

Note: For direct connection, static is often more simple.

3. **Open web browser:** On your PC, open the Google Chrome web browser.

Note: Google Chrome and Microsoft Edge are the only supported web browsers.

4. **Navigate to the admin interface:**
 - **Using IP address:** If the Main Node is using its default static IP, type https://192.168.0.251 into the web browser address bar.
 - **Note:** https implies a self-signed certificate initially, so you may need to accept a browser security warning.
 - **Using mDNS:** If your PC has Bonjour or similar mDNS services installed, you may be able to access it by typing https://[MAC0].local (for example, https://00112233AABB.local). Replace [MAC0] with the actual MAC0 address that can be found on the Main Node label (remove colons).
5. **Login page:** You should see the Main Node admin interface login page.

Note: Admin mode remains active for one hour after it is enabled. To re-activate, restart the Main Node with the DIP switches set to the admin mode configuration.

5.5 Step 5: First-time login and secure password setup

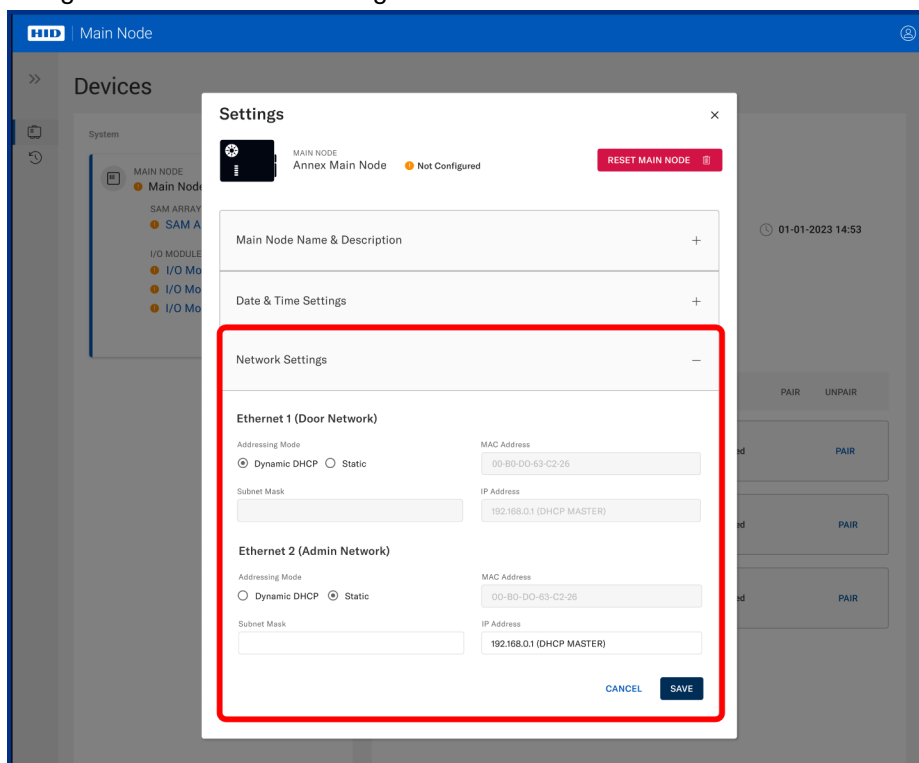
1. Upon first accessing the login page, you will be immediately prompted to create the administrator password.
2. Follow the on-screen prompts to set a strong, unique password for the administrator account.

WARNING: THIS ADMINISTRATOR PASSWORD CANNOT BE RECOVERED IF FORGOTTEN OR LOST. LOSING THIS PASSWORD WILL NECESSITATE A COMPLETE FACTORY RESET OF THE MAIN NODE, IO MODULES, AND READERS, ERASING ALL SYSTEM CONFIGURATIONS. STORE THIS PASSWORD SECURELY.

5.5.1 Network configuration (Main Node)

Configure the network settings for the Main Node's ETHERNET 1 port (the one used for communication with IO Modules and potentially a wider management network).

1. Navigate to the Network Settings section of the Main Node.



2. Configure the IP settings for ETHERNET 1:
 - **DHCP Client:** If the Main Node should obtain an IP address from a DHCP server on the management network.
 - **Static IP:** If assigning a fixed IP address. Enter the IP Address, Subnet Mask, Default Gateway, and DNS Server(s) information.

Important:

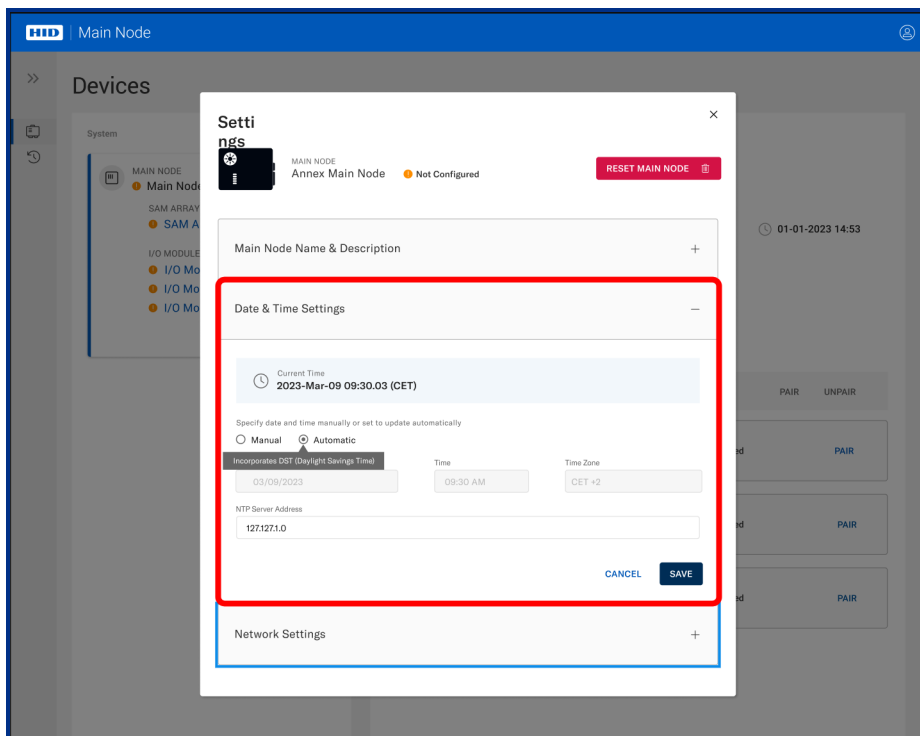
- If IO Modules are connected directly to Main Node ETHERNET 1 or through a local, dedicated, unmanaged switch (not part of a larger corporate network), the Main Node can act as a DHCP server for the IO Modules. In this scenario, set the Main Node DIP switches to a DHCP mode.
- If the Main Node and IO Modules are on a larger managed network with its own DHCP server, configure the Main Node (and IO Modules, if they have independent settings) as DHCP clients or assign appropriate static IPs.

3. Save the network settings.

Note: A reboot of the Main Node may be required for changes to take effect.

5.5.2 Date and time configuration (NTP)

Accurate system time is important for logging and event correlation.



1. Navigate to the Date/Time or NTP Settings section.

NTP Server: If there is an Network Time Protocol (NTP) server on the management network, enter its IP address or hostname. The Main Node will then synchronize its time automatically.

Manual Time Set: If no NTP server is available, set the system date and time manually.

Note: Manual time may drift.

2. Select the correct Time Zone.
3. Save the date and time settings.

5.6 Step 6: System configuration via the Main Node admin interface

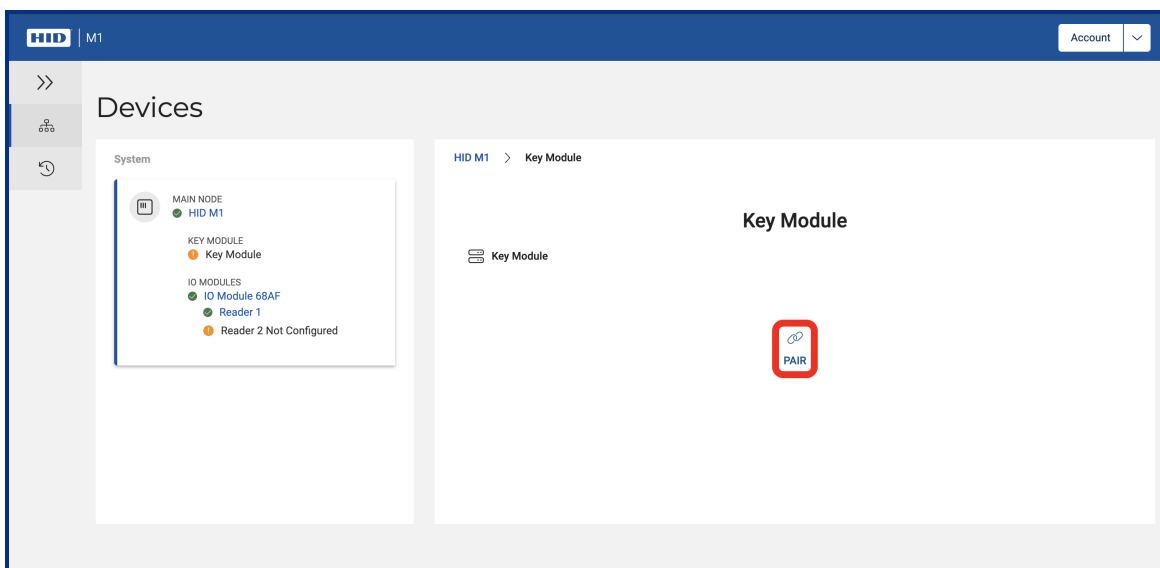
5.6.1 Install and Pair the Key Module

The Key Module must be physically installed and then paired with the Main Node.

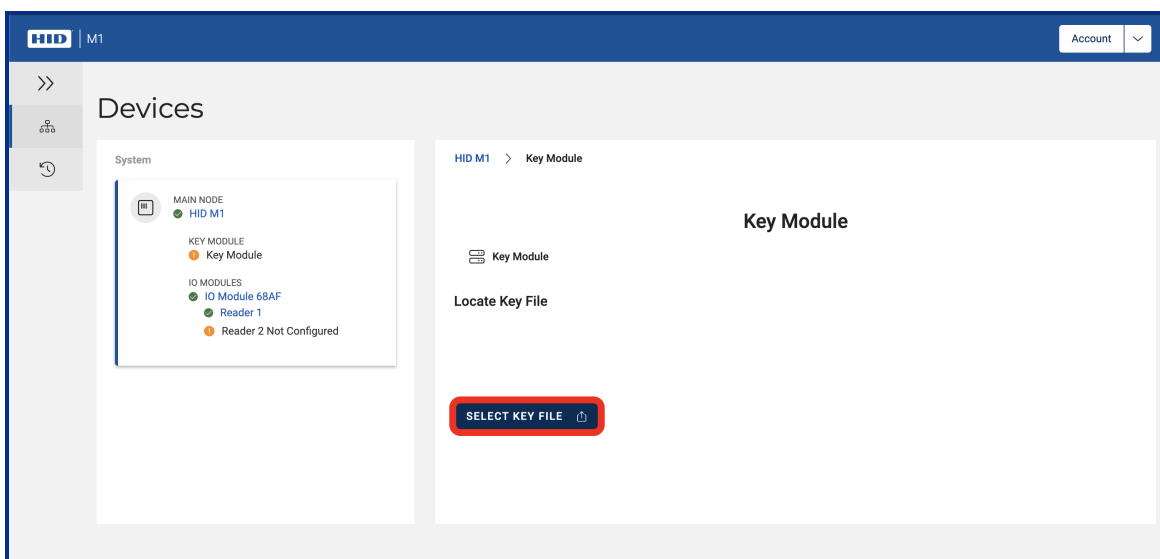
1. Power OFF the Main Node

Important: If you are physically inserting the Key Module, ensure the Main Node is completely powered OFF.

2. Carefully insert the provisioned Key Module into its dedicated slot in the Main Node (See [2.1.2 Main Node](#)) and secure in place with the provided screw.
3. Power ON the Main Node.
4. **Access the admin interface:** Log back into the admin interface of the Main Node in admin mode.
5. Select the Key Module, then click **PAIR**.

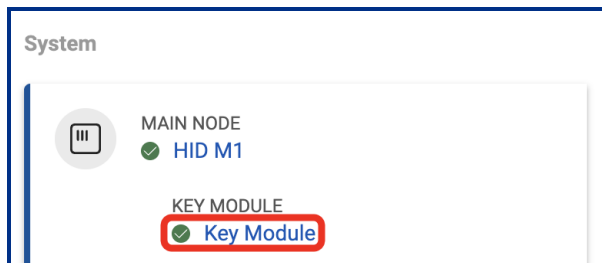


6. Click **Select Key File** and the Select file window will open.



7. Navigate to and select the .bin file with your Main Node Pairing key.

8. Click **Apply Key File**. Successful pairing is confirmed with a green tick icon.



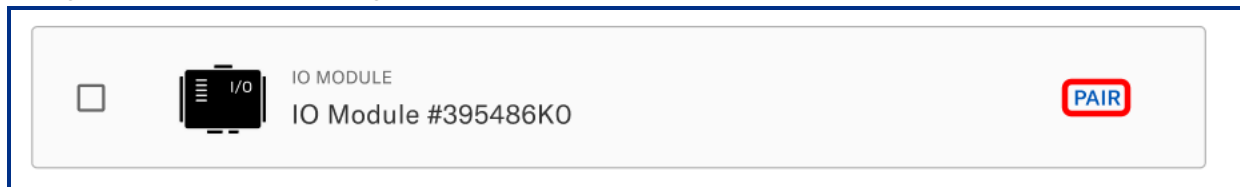
Note: A Key Module can be paired with any Main Node within a system, provided the Pairing Key is available.

Important: The Security Administrator is responsible for ensuring the Pairing Key is stored and transported securely. It must not be shared with unauthorized individuals.

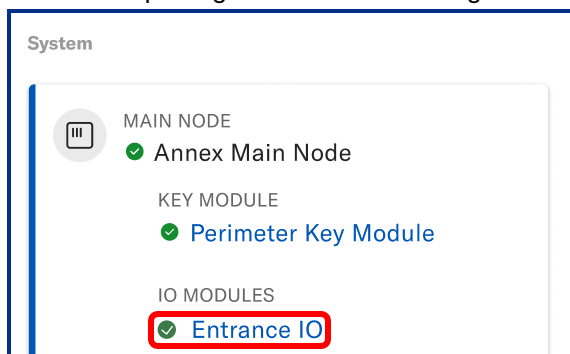
5.6.2 Pair IO Modules

Each IO Module physically connected to the Main Node's network, (ETHERNET 1) and set to admin mode (via DIP switches), must be discovered and paired.

1. **Navigate to IO Module Management:** Find the IO Module PAIR button under the components section.



2. **Discover IO Modules:** Discovered IO Modules appear in a list.
3. **Pair each IO Module:**
 - a. For each discovered IO Module you intend to use, select it and click **PAIR**.
 - b. Assign a friendly name to the IO Module (for example "Entrance IO," "Server Room IO").
 - c. Successful pairing is confirmed with a green tick icon.



4. **Set IO Module to normal operation:**
 - a. After an IO Module is successfully paired, you will need to physically change its DIP switches from admin mode to normal operation.
 - b. Power cycle the IO Module for the new DIP switch setting to take effect. The IO Module should then reconnect to the Main Node in normal operation mode.

5.6.3 Pair readers

Transparent HID Signo readers connected to the paired IO Modules must be discovered and associated with their respective IO Module ports.

1. **Navigate to Reader Management:** Find the readers in the IO Module tab under the components section.
2. Click **PAIR** to pair each reader.

Configure Reader Connections

Each IO Module can connect up to two transparent readers to the controller.

Connection 1



CONTROLLER

+



SIGNO20V2P1

FIRMWARE VERSION: 055A

UUID: 02722A8E-C654-517E-BB33-1E50EB27D5CE

+

Connection 2



CONTROLLER

+



SIGNO

PAIR

3. Successful reader pairing is confirmed with a green tick icon.

System



MAIN NODE



HID M1

KEY MODULE



Key Module

IO MODULES



IO Module 68AF



Reader 1



Reader 2 Not Configured

4. Assign a friendly name (for example "West Entrance Entry Reader A").

PLT-07917, A.0

32

December 2025

Note:

Once a reader is paired with an M1 system, it can reconnect to any IO device within that system, provided all devices are linked to the same Main Node. However, the reader cannot be used with a different Main Node until it is decommissioned.

To use the reader in a different system, it must first be decommissioned as follows:

1. Unmount the reader from the wall.
2. Connect the reader to the HID Linq Tool.
3. Apply a new DCID, which you can obtain from your HID Representative or the Customer Support team.

5.6.4 Configure IO Module OSDP parameters (for PACS controller)

For each IO Module channel that is connected to an existing PACS controller, you must configure the OSDP parameters that the IO Module will use to communicate as a device to that controller. These settings must match what the PACS controller expects for that OSDP reader port.

1. **Navigate to IO Module Settings:** Go to the configuration page for a specific paired IO Module. Find the section for OSDP settings.

Configure Reader Connections
Each IO Module can connect up to two transparent readers to the controller.

Connection 1

 CONTROLLER

Configure Controller

Name

Address Baud

UNDO

2. **For each connected controller port (for example CONTROLLER 1, CONTROLLER 2):**
 - **OSDP address:** Enter the OSDP address that the PACS controller is configured to poll on this specific channel (for example 0, 1, 2, etc.).
 - **Baud rate:** Select the OSDP baud rate that matches the PACS controller's port configuration (for example 9600, 19200, 38400, 115200 bps).

Note: Higher baud rates may improve card read time at the cost of maximum wiring distance.

3. Save the OSDP settings for each IO Module controller port.

5.7 Step 7: Reader firmware update using HID Reader Manager app

Ensure all connected HID Signo readers have SP11+ firmware for compatibility with the HID M1 Transparent Gateway. You can order readers pre-configured as transparent or update older firmware to SP11+. Apply a specific DCID to make the readers transparent. Contact your HID Representative for the correct DCID.

Note: Readers that support "OSDP Transparent Mode" are not compatible with HID M1. HID M1 is only compatible with HID Signo readers that have compatible firmware and the transparent DCID.

Important: Updating reader firmware using HID Reader Manager™ will deactivate access to any keys previously on the reader. If your security policy requires that no old keys remain (even if inactive), order preconfigured transparent HID Signo readers for HID M1 directly from HID.

1. **Identify readers that need to be updated:** The reader needs to be updated if the firmware version is below SP11.
2. **Download the HID Reader Manager app:** If not already done, download and install the app on a compatible smartphone.
3. **Obtain the DCID:** A specific DCID is required to make the reader transparent. Contact your HID representative or customer support to obtain the correct DCID for your readers and firmware version.
4. **Perform firmware update (for each reader):**
 - a. Make sure the reader is powered on.
 - b. Follow the instructions in the HID Reader Manager app to:
 - Discover and connect to the Signo reader via Bluetooth.
 - Select the downloaded SP11+ transparent firmware file.
 - Apply the firmware update.
 - If required, apply the specific DCID using the app (the **Reader Configuration ID** in the app).

Note: Once a reader is converted to transparent via a DCID, the HID Reader Manager app will no longer be able to connect to it for standard configuration, as Bluetooth is disabled on the reader. Future firmware updates for these readers can only be done via HID LinQ tools.

Validate in the admin interface

After updating and applying the DCID, go back to the Main Node admin interface and check the status of the reader to ensure it is recognized correctly with the new firmware.

Section 06

Operational Information

6.1 Operational information overview

This section describes the normal operational indicators and data flows of the HID M1 Transparent Gateway system after successful installation and configuration.

6.2 Status LEDs

Status LEDs on the Main Node and IO Modules provide visual feedback on their operational state.

6.2.1 Main Node initialization

During initialization, the LEDs will illuminate in the following sequence:

1. **SECURE LED** – ON for about 10 seconds
2. **TAMPER LED** – ON for about 8 seconds
3. **BATT FAIL LED** – ON for about 4 seconds
4. **AC FAIL LED** – ON for about 2 seconds
5. **STATUS LED** – ON for about 1 second
 - If a firmware update is in progress, the **STATUS LED** flashes (500ms ON, 500ms OFF) until the update completes.

Important: Do not power cycle the device during this state.

6.2.2 Main Node running

LED	State	Description
STATUS	Flashing (2s ON, 500ms OFF)	Main Node is running
	Flashing (500ms ON, 500ms OFF)	Firmware update in progress
	Rapid flash (9 rapid flashes, then 2s pause)	Critical error
AC FAIL	Slow flash	AC power present
	Fast flash	AC power absent
BATT FAIL	Slow flash	UPS/Battery present and healthy/fully charged
	Fast flash	UPS/Battery failed, disconnected, or critically low
TAMPER	Slow flash	Cabinet tamper input secure (closed contact)
	Fast flash	Cabinet tamper input active (open contact/tamper event).
DATA TX	N/A	Reserved for future use
DATA RX	N/A	Reserved for future use
SECURE MODE	Flashing (2s ON, 500ms OFF)	Normal operation
	Flashing (500ms ON, 2s OFF)	Admin mode
	Flashing (100ms ON, 400ms OFF)	Factory reset in progress

Note: LED behavior (solid vs. slow flash for normal) may vary slightly by firmware. Refer to specific release notes if behavior differs.

6.2.3 Status LEDs - IO Module

LED	State	Description
POWER	Solid	IO Module is powered ON
	OFF	No power
STATUS	Solid	IO Module is starting up and initializing
	Flashing (100ms ON, 400ms OFF)	Factory reset is in progress
	Flashing (500ms ON, 2s OFF)	IO Module is looking for a network link
	Flashing (1s ON, 1s OFF)	IO Module is running but not paired
	Flashing (2s ON, 500ms OFF)	IO Module is running and paired
	Flashing (500ms ON, 500ms OFF)	A firmware update is in progress
USB	Solid	USB device connected
	OFF	USB device not connected
AC FAIL	Solid	AC fail input active
	OFF	AC fail input inactive
BATT FAIL	Solid	Battery fail input active
	OFF	Battery fail input inactive
TAMPER	Solid	Tamper input active
	OFF	Tamper input inactive
TX READER 1	Flashing	Data transmitting to READER 1
RX READER 1	Flashing	Data receiving from READER 1
TX READER 2	Flashing	Data transmitting to READER 2
RX READER 2	Flashing	Data receiving from READER 2
TX CONTROLLER 1	Flashing	Data transmitting to CONTROLLER 1
RX CONTROLLER 1	Flashing	Data receiving from CONTROLLER 1
TX CONTROLLER 2	Flashing	Data transmitting to CONTROLLER 2
RX CONTROLLER 2	Flashing	Data receiving from CONTROLLER 2
RELAY 1/2/3	Solid	Corresponding output relay is energized
	OFF	Corresponding output relay is de-energized

Section 07

Normal Operational Flows

7.1 Credential read and forwarding

1. A DESFire credential is presented to a connected HID Signo™ transparent reader.
2. The reader captures the encrypted card data and sends it to its connected IO Module.
3. The IO Module forwards the encrypted data over Ethernet to the Main Node.
4. The Key Module in the Main Node decrypts the data and performs credential authentication against the provisioned keys.
5. If valid, the Main Node formats the card data as required and sends it as an OSDP message via the IO Module to the existing PACS controller for authorization.

7.2 Controller command passthrough

1. The Main Node (via the IO Module) forwards LED control and buzzer commands received from the PACS controller to the appropriate reader.
2. Keypad input from readers (if applicable) is passed through to the PACS controller.

7.3 Tamper and error reporting

The system detects and reports tamper events and internal errors to the PACS controller via OSDP. These are typically communicated as a general "reader tamper" or offline event for the associated OSDP address.

7.3.1 Reported conditions

- **Reader wiring faults**

Includes loss of communication and short circuits (if detectable).

- **Tamper switch activation** on the Main Node, IO Module (if wired), or reader.

- **Reader tamper switch:** The access control software reports a reader tamper alarm.
- **IO Module tamper switch:** The access control software reports tamper alarms for both readers connected to the IO Module.
- **Main Node tamper switch:** The access control software reports tamper alarms for all readers connected to the M1 system.

- **Internal errors**

Errors within the Main Node or IO Modules are logged and can be viewed through the Main Node administrative interface (admin mode must be enabled).

7.4 Unavailable functionality in normal operation mode

The following functions are disabled when the Main Node is in normal operation mode:

- Pairing/unpairing of Key Modules, IO Modules, or readers.
- System configuration changes (network, OSDP settings, etc.).
- Firmware updates.
- Access to logs.

To perform these actions, set the Main Node DIP switches to admin mode, power cycle the unit, and log on to the admin interface.

Section 08

Maintenance and Troubleshooting

8.1 Firmware updates

HID will release firmware updates for the Main Node, IO Modules, and HID Signo™ readers to provide new features, improvements, or security enhancements. Always download firmware from the official [HID Developer Portal](#), the Reader Manager app, or HID Linq™ tools.

8.2 Main Node and IO Module firmware

Firmware for the Main Node and connected IO Modules is updated via the Main Node admin interface.

8.2.1 Download firmware

Obtain the latest firmware files for the Main Node and IO Modules from the [HID Developer Portal](#). Save them to your PC.

8.2.2 Enable admin mode

1. Remove the cover from the Main Node. Be mindful to disconnect the fan cable.
2. Set the Main Node DIP switches to an admin mode (see [5.3.1 Main Node DIP switches](#)).
3. Power cycle the Main Node.

8.2.3 Login to the admin interface

1. Access the Main Node admin interface via your web browser.
2. Select a device.
3. The interface displays the current firmware versions for the Main Node and any paired IO Modules. Compare these with the versions you downloaded.

8.2.4 Update Main Node firmware (if needed)

1. Click **Update Firmware**
2. Browse to and select the downloaded Main Node firmware file from your PC.
 - The file type is ".tar" and does not require extraction.
 - Initiate the upload. The system will validate the firmware, perform the update, and then perform a self-test automatically. This process may take several minutes. Do not interrupt power.

8.2.5 Update IO Module firmware (if needed)

1. After the Main Node has rebooted and is accessible, log back into the admin interface.
2. Select an IO Module to update.
3. Click **Update Firmware**.
4. Browse to and select the downloaded IO Module firmware file.
5. Initiate the upload. The system will validate the firmware, perform the update, and then perform a self-test automatically. This process may take several minutes. Do not interrupt power.
6. Repeat for each IO Module.

8.2.6 Perform manual system tests

After all updates, thoroughly test the system with credentials to ensure proper functionality.

8.2.7 Return to normal operation

1. Set the Main Node/IO Module DIP switches back to normal operation mode.
2. Power cycle the devices.
3. Re-connect the fan cable for the Main Node and replace the cover on the Main Node/IO Module.

8.3 Key Module firmware

Key Module firmware cannot be updated in the field after order and delivery.

8.4 Factory reset procedure

A factory reset erases all configuration settings on a device and returns it to its original default state. Perform a factory reset only as a last resort, for example, if the Main Node admin password is lost.

8.4.1 Important considerations before factory reset

- **DATA LOSS:** A factory reset will delete all configurations, including network settings, paired devices (Key Modules, IO Modules, readers), OSDP parameters, and any custom settings. The entire system will need to be reconfigured from scratch.
- **SYSTEM-WIDE RESET SEQUENCE:** For a complete system reset, it is crucial to follow the correct order to avoid potential persistent pairing issues with readers that might have established secure channel keys.
 1. Unpair all readers and then the IO Modules from the Main Node via the admin interface.
 2. Factory reset each IO Module individually.
 3. Factory reset the Main Node.

WARNING: FAILURE TO FOLLOW THIS SEQUENCE, ESPECIALLY IF OSDP SECURE CHANNEL WAS USED WITH READERS, MAY RESULT IN READERS THAT CANNOT BE RE-PAIRED WITHOUT SPECIALIZED PROCEDURES OR EVEN REPLACEMENT. CONSULT HID SUPPORT IF YOU ENCOUNTER SUCH ISSUES.

8.4.2 Factory resetting an IO Module

1. Power OFF the IO Module.
2. Remove the IO Module cover.
3. Set the IO Module DIP switches to factory reset mode.
4. Power ON the IO Module.
5. Wait until the Status LED on the IO Module becomes stable.
6. Power OFF the IO Module.
7. Set the IO Module DIP switches back to normal operation or admin mode if you intend to re-pair it immediately.

Important: Ensure the factory reset DIP switch combination is not left active, or the IO Module will reset again on the next power cycle.

8. Replace the cover.
9. Power ON the IO Module.

8.4.3 Factory resetting the Main Node

1. Power OFF the Main Node.
2. Remove the Main Node cover. Be mindful to disconnect the fan cable.
3. Set the Main Node DIP switches to factory reset mode.
4. Power ON the Main Node.
5. Wait until the Status LED on the Main Node indicates the reset is complete.
6. Power OFF the Main Node.
7. Set the Main Node DIP switches to your desired initial configuration mode.

Important: Ensure the factory reset DIP switch combination is not left active.

8. Re-connect the fan cable and replace the cover.
9. Power ON the Main Node. You will need to go through the first-time login and password setup again (see [5.5 Step 5: First-time login and secure password setup](#)).

8.4.4 Common issues and resolutions

Issue	Possible cause(s)	Suggested solution(s)
Cannot access Main Node admin interface	• Incorrect PC IP config • Main Node not powered/booted • Incorrect Main Node IP/DIP mode • Firewall blocking	• Verify PC network settings • Check Main Node power and Status LED • Confirm Main Node DIP switch mode and IP address • Temporarily disable PC firewall
IO Module not discovered/pairing	• IO Module not in Install Mode • Network issue between Main Node and IO • IO Module not powered	• Set IO Module DIP to install mode and power cycle • Check Ethernet cabling and switch • Verify IO Module power and Status LED
Reader not discovered/pairing	• Incorrect wiring to IO Module • Reader firmware is not updated to SP11+ • transparent DCID is not applied	• Check reader wiring (power, data, ground) • Ensure reader has HID M1 compatible transparent firmware • Ensure reader has transparent DCID applied
"INVALID PAIRING" displayed in admin interface	IO Module or Reader was factory reset without unpairing, or pairing data mismatch.	Attempt to unpair the device from Main Node, then factory reset the problematic IO Module/reader again. Re-attempt pairing. If Secure Channel was used, reader may need HID support.
Credential not read / No response at controller	• Key Module not paired/incorrect keys • Incorrect OSDP config to controller • Wiring issue	• Verify Key Module is paired and has correct keys • Double-check OSDP address and baud rate on IO Module for the controller port • Inspect all wiring • Check Main Node logs
Intermittent OSDP communication	• Improper OSDP bus termination • Electrical noise/interference • Cable length exceeded	• Ensure 120Ω termination at BOTH ends of each OSDP segment • Use shielded OSDP cable, route away from noise sources • Keep OSDP cable runs within spec

Section 09

Specifications

9.1 Main Node (M1-1100)

Mounting	Direct, DIN rail, or HID M1 to Mercury bracket.
Primary power	12V to 24V DC ($\pm 10\%$)
Max input current	2A @ 12V or 1A @ 24V (24W max)
USB ports	USB 2.0 Type A (internal), 500mA @ 5V ($\pm 10\%$) - temporary connection only USB 3.0 Type A (external), 1A @ 5V ($\pm 10\%$) - temporary connection only
Inputs	Cabinet tamper (0V to 3.3V) Battery failure (0V to 3.3V) AC failure (0V to 3.3V) Cable lengths must be ≤ 98 feet (30 m)
Outputs	None
Ethernet host requirements	10BASE-T/100BASE-TX/1000BASE-T (Gbit)
CABLE REQUIREMENTS	
Power	1 twisted pair, 18 AWG (when using local 12V DC power supply)
Ethernet	CAT-5 minimum (shielded) Ethernet 0: Cable length must be ≤ 98 feet (30 m) Ethernet 1: Cable length can be ≥ 98 feet (30 m)
Alarm input	1 twisted pair per input, 30 Ω maximum (not evaluated by UL)
Outputs	As required for the load
ENVIRONMENTAL	
Storage temperature	-67° F to 185° F (-55° C to 85° C)
Operating temperature	32° F to 158° F (0° C to 70° C)
Humidity	5% to 95% Relative humidity, Non-Condensing (RHNC)
MECHANICAL	
Dimensions	4.85 inches (123.3 mm) W x 6.47 inches (164.4 mm) L x 1.75 inches (44.4 mm) H
Weight	13.5 oz. (383 g)

9.2 Key Module (M1-1001)

Mounting	The Key Module (M1-1001) is installed inside the Main Node (M1-1100)
Primary power	Powered by Main Node (M1-1100)
USB port	USB-C, 500mA @ 5V ($\pm 10\%$)
ENVIRONMENTAL	
Storage temperature	-67° F to 185° F (-55° C to 85° C)
Operating temperature	32° F to 158° F (0° C to 70° C)
Humidity	5% to 95% Relative humidity, Non-Condensing (RHNC)

9.3 IO Module (M1-1002)

Mounting	Direct, DIN rail, or HID M1 to Mercury bracket.
Primary power	12V to 24V DC ($\pm 10\%$)
Maximum input current	1.6A @ 12V and 0.8A @ 24V (19.2W max)
USB port	USB 2.0 Type A, 500mA @ 5V ($\pm 10\%$) - temporary connection only
Relays	5A @ 30V DC - Relays 1, 2, and 3 not evaluated by UL (Gateway Mode)
Inputs	Two transparent HID Signo™ readers (-7V to 12V) - 12V DC, 280 mA wiring must be shielded Cabinet tamper (0V to 3.3V) - Cable length must be ≤ 98 feet (30 m) Battery failure (0V to 3.3V) - Cable length must be ≤ 98 feet (30 m) AC failure (0V to 3.3V) - Cable length must be ≤ 98 feet (30 m) Request to Exit (REX) (0V to 3.3V) REX: Not evaluated by UL Door Position Sensor (DPS) (0V to 3.3V) DPS: Not evaluated by UL
Outputs	Controller 1 and 2 output reader PACS data to the upstream controller. Cable lengths must be ≤ 98 feet (30 m)
Ethernet host requirements	10BASE-T/100BASE-TX
CABLE REQUIREMENTS	
Power	1 twisted pair, 16 to 18 AWG
Ethernet	CAT-5 minimum (shielded) - Cable length can be ≥ 98 feet (30 m)
Reader data (TTL)	6-conductor, 18 AWG, 500 feet (152 m) maximum per reader (not evaluated by UL)
Reader data (RS-485)	1 twisted pair, shielded. 24 AWG, 120 Ω impedance, 2000 feet (610 m) maximum per reader (not evaluated by UL)
Alarm input	1 twisted pair per input, 30 Ω maximum (not evaluated by UL)
Outputs	As required for the load
ENVIRONMENTAL	
Storage temperature	-67° F to 185° F (-55° C to 85° C)
Operating temperature	32° F to 158° F (0° C to 70° C)
Humidity	5% to 95% Relative humidity, Non-Condensing (RHNC)
MECHANICAL	
Dimensions	4.85 inches (123.2 mm) W x 6.46 inches (164.2mm) L x 1.04 inches (26.3 mm) H
Weight	12.87 oz. (365 g)

Revision history

Date	Description	Revision
December 2025	Initial release.	A.0



hidglobal.com

For technical support, please visit: <https://support.hidglobal.com>

© 2025 HID Global Corporation/ASSA ABLOY AB.

All rights reserved.

PLT-07917, Rev. A.0

Part of ASSA ABLOY