Access control configuration in PRO series modules

Document number: PO-245-EN Version: 1.0 Date of publication: July 10, 2025

Managing Cards via Ampio Designer

The **Access Control** tab allows you to manage RFID cards and configure the API PIN, which is required if you want to integrate card management via RAW commands.

Purpose of card management

RFID cards can be used for:

- unlocking entrance doors,
- controlling lighting,
- activating alarms,
- managing air conditioning and heating,
- enabling or disabling access zones (e.g., offices, warehouses).

Thanks to the ability to assign card types and set their validity period, you can precisely define who has access to specific system functions and when.

Adding a new card

Click the icon to add a new card entry. Required data to add a card:

- UID: must be 8 characters in hexadecimal format (`A1B2C3D4`)
- Mode: `always` – for permanent cards, `from-to` – for cards with time-limited access
- Start and end dates: required when using the 'from-to' mode
- Card type: selected from a list to define card privileges

Scanning the card's UID

You can add a card by scanning it with the reader after starting the scanning procedure:

1. Click the card icon next to the UID field.
2. Place the physical RFID card on the reader.
3. The UID will be read from the module and automatically filled into the field.

Manually Eentering the UID

It is also possible to manually add a card by typing its UID on the keyboard or by scanning it using an external USB card reader connected to the computer.

- The UID field accepts exactly 8 hexadecimal characters (e.g., `A1B2C3D4`).
- Incorrect lengths will trigger an error.
- If using an external card reader, configure it to read the card UID as an 8-character HEX (reversed if necessary).

Operation mode

- `Always`: the card has no time restrictions; it works whenever presented to the reader.
- `From-to`: allows setting a time range during which the card will work.

If the card list becomes full, when adding a new card, the card with the oldest expiration date will be removed. Permanent cards are not considered for removal.

Card type

The list of card types is predefined. You can search and assign a specific card type. Card types allow you to build logic based on the type rather than specific UID, enabling you to have a fully working logic just by assigning the appropriate type when adding new cards.
If you need a new card type, please contact Ampio technical support.

Removing a card

Click the icon to remove a card from the list.

Saving cards

Click the icon to save all changes to the device. The button will only activate when all UIDs are exactly 8 characters long.

Setting the API PIN

The module allows integration with external systems using the RAW function, which enables direct data transmission to the device. To accept such data, the device requires the correct 8-digit API PIN as a security measure.
The following section describes how to properly set the PIN to enable RAW operations. You can find more details on card handling and sending RAW commands in the next section.

- Enter exactly 8 digits in the PIN field.
- The field only accepts numeric digits.
- Click **Set PIN** to send the PIN to the device.

Managing cards via RAW

If you wish to integrate RFID card management with external systems, you can use the RAW function available in Ampio devices.
We provide a ready-to-use Node-RED example, available in the attached file `Card_Management_RAW.json`. The file contains three predefined scenarios:

- Adding a new card
- Deleting a specific card
- Deleting all UID entries from the device

When using RAW card saving, it is normal for the card memory area in the designer to show maximum capacity.

How to use the provided file?

1. Import the file `Card_Management_RAW.json` into your Node-RED environment.
2. Configure the MQTT connection in the “MQTT Card” node:
    - Set the MQTT broker address (default is localhost),
    - Configure authentication in the `Security` tab.
3. In each “inject” node (e.g., “Add Card”), edit the following parameters:
    - mac – the MAC address of the target device.
    - pin – the previously set 8-digit API PIN from the Access Control tab.
    - uid – RFID card UID in hexadecimal format (8 characters).
    - type – card type number (e.g., 01).
    - tsStart and tsEnd – timestamps (in HEX format) defining the card’s validity period. Use 00000000 and FFFFFFFF for permanent cards.
4. Do not modify the `actionType` field – it defines the action type:
    - 01 – add card,
    - 02 – delete card,
    - 03 – delete all cards.
    - trigger – always set to true to initiate the sending process.
5. After setting the parameters, click the button in the “inject” node to send data to the device.
6. The response will be shown in Node-RED’s debug console in the “RAW Response” node.

Example use case

Below are examples of adding permanent and temporary cards. Deleting individual cards works similarly to adding but requires full data input; just the UID is not sufficient.

Adding a permanent card

Adding a card with UID AABBCCDD, type 01, permanent validity, for a module with MAC address 123456 and API PIN 12345678:

- mac: 123456
- pin: 12345678
- uid: AABBCCDD
- type: 01
- tsStart: 00000000
- tsEnd: FFFFFFFF
- actionType: 01
- trigger: true

Adding a time-limited card

To add an RFID card that will work only within a specific time period, provide the appropriate dates in the tsStart and tsEnd fields.
These dates must be in UNIX timestamp format (seconds since 1970-01-01) and then converted to an 8-character HEX string.

Example:

- Start date: January 1, 2025, 00:00 → UNIX timestamp: 1735689600 → HEX: 6786A800
- End date: December 31, 2025, 23:59 → UNIX timestamp: 1767225599 → HEX: 697ADFFF

Adding a card with UID AABBCCDD, type 01, valid in 2025, for a module with MAC address 123456 and API PIN 12345678:

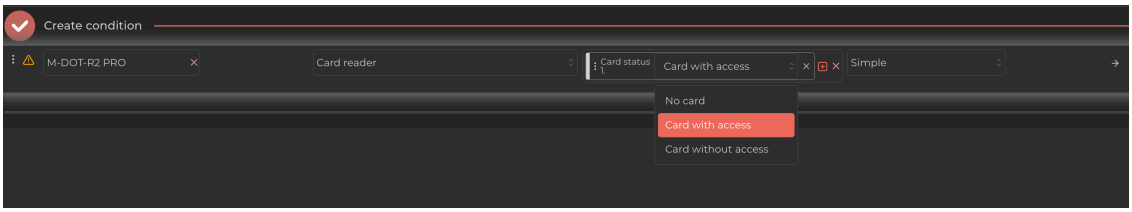
- mac: 123456
- pin: 12345678
- uid: AABBCCDD
- type: 01
- tsStart: 6786A800
- tsEnd: 697ADFFF
- actionType: 01
- trigger: true

Creating logic from cards

Checking Card Status

This condition allows you to verify whether the currently presented card meets a specific access criterion. To configure it:

1. Select the module from the list.
2. Select Card Reader as the input type.
3. Choose the input number as Card Status.
4. Select the desired value:
    - No Card – no card detected,
    - Card with Access – card recognized and granted access,
    - Card without Access – card detected but access not granted.



Checking Card Type

You can also check the card type, which enables assigning separate logic for guest, service, or other card types. To configure it:

1. Select the module from the list.
2. Select Card Reader as the input source.
3. Choose the input number as Card Type.
4. Select the card type from the list.