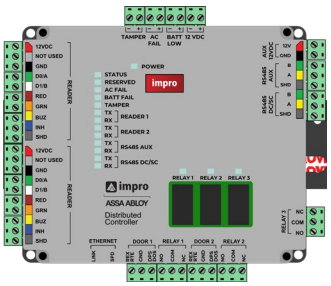
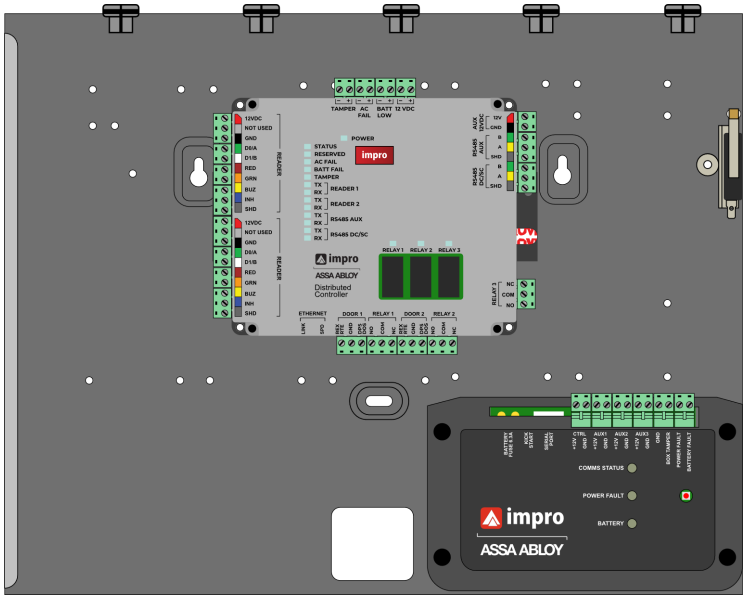
Distributed Controller

User Guide

PLT-06326, A.1

December 2024





Copyright

Trademarks

Contact technical support:

- Visit https://www.impro.net/tech-support/
- Email support@impro.net
- Call Impro 24hour Support: +27 (31) 717 0750

What's new

Date	Description	Revision
December 2024	Included HCD901, HCD902, HCD903, HCD904, HCD905.	A.1

A complete list of revisions is available in **Revision history**.

Contents

1. Introduction

Overview

The impro distributed controller provides all the control, communications, credential buffer and memory, digital inputs and relays required to serve two readers and up to two doors. The distributed controller supports OSDP RS485 readers in addition to Wiegand and Multi-Discipline readers.

The unit can be configured for one of three different roles depending on the size of the installation and the location within the access control installation:

1. A Door Controller, as part of a small or large access control system.
2. A stand-alone access control for small premises (via an integrated web application).
3. A System Controller, as part of a large access control system – Impro Technologies' Primo (or Access Portal) software, able to control downstream door controllers, which could be other distributed controllers or other Access Portal hardware combos configured as door controllers.

iTRT2 Combinations

This user guide covers the following hardware combinations:

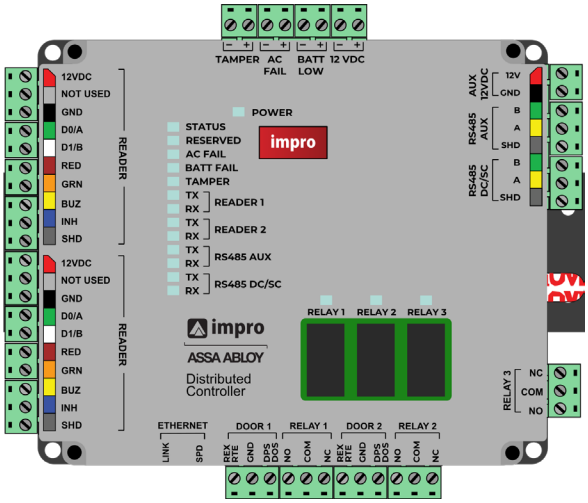
Item number	Hardware description
HCD900-0-0-GB-XX	A stand-alone distributed controller with accessible terminals. This will need a 12V DC 2.5 A DC power supply (not included)
HCD901-0-0-GB-XX	Distributed controller in steel cabinet Integrated DC Power supply AC Mains input terminal block. Space for a 12V SLA backup battery. Lid tamper sensing.
HCD902-0-0-GB-XX	Distributed controller in steel cabinet Integrated DC Power supply IEC320 AC mains input socket Space for a 12V SLA backup battery. Lid tamper sensing. Cabinet dismount sensing.
HCD903-0-0-GB-XX	Distributed controller in steel cabinet Integrated PoE++ power adaptor Space for a 12V SLA backup battery. Lid tamper sensing.
HCD904-0-0-GB-XX	Distributed controller in steel cabinet Integrated DC Power supply with AC Mains input terminals Space for a 12V SLA backup battery. Lid tamper sensing.
HCD905-0-0-GB-XX	Distributed Controller in a plastic enclosure. Lid tamper sensing. This will need a 12V DC 2.5 A DC power supply (not included)

Guarantee or warranty

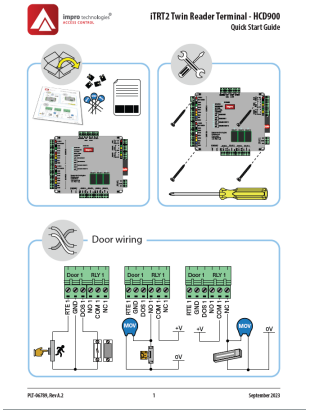
This product conforms to our guarantee or warranty details placed on our website, visit **www.impro.net** for more information.

2. What's in the box

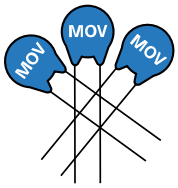
HCD900-0-0-GB - carton contents



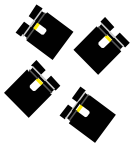
ITRT2 distributed controller



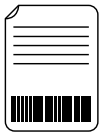
Quick start guide



Metal Oxide Resistors (MOVs)



Jumpers



Fixed address label

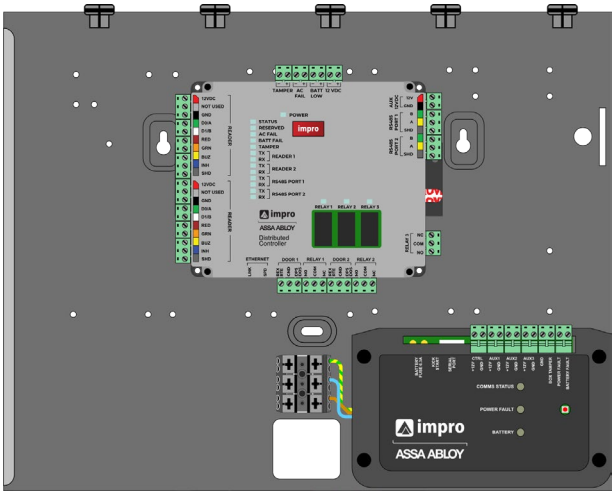
3 of 5 lid screws

(2 already on the unit)

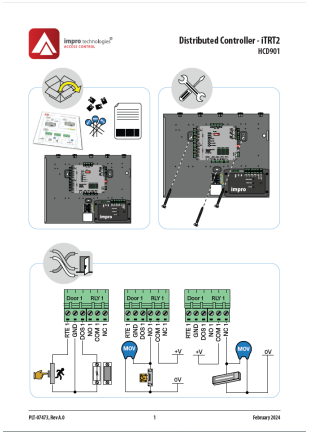
You will need

- Basic electrical installation tools.
- 12V DC 2.5 A DC power supply to power the Distributed Controller.
- An auxiliary power supply to power the electric locks.
- Cables for Ethernet, readers, door sensor inputs and relay loads.
- Magnetic reed switches for Door Open Sensor (DOS).
- Push buttons for Request To Exit (RTE).
- Mag locks or strike locks.
- Mounting hardware: Fasteners suitable for the mounting surface.

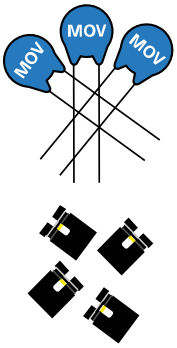
HCD901-0-0-GB - carton contents



ITRT2 distributed controller in a steel cabinet, built-in DC PSU and mains input terminal block



Quick start guide



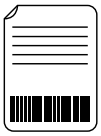
Metal Oxide Resistors (MOVs)

Jumper links

Nylon Wall plug

3 of 5 lid screws

(2 already on the unit, 1 is spare)



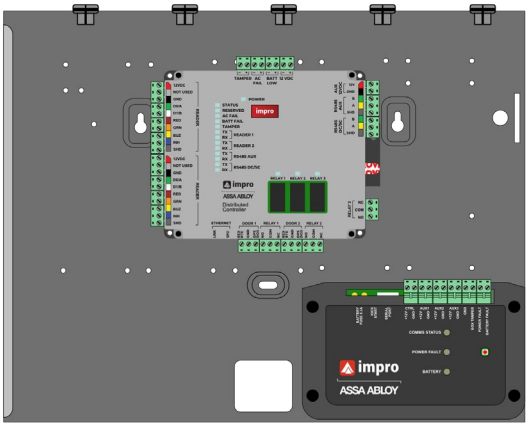
Fixed address label

Cable Ties

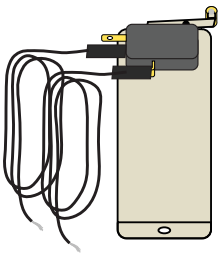
You will need

- Basic electrical installation tools.
- An AC supply cable to wire into the AC power (220V AC) terminal block.
- An auxiliary power supply to power the electric locks.
- Cables for Ethernet, readers, door sensor inputs and relay loads.
- Magnetic reed switches for Door Open Sensor (DOS).
- Push buttons for Request To Exit (RTE).
- Mag locks or strike locks.
- Mounting hardware: Fasteners suitable for the mounting surface.

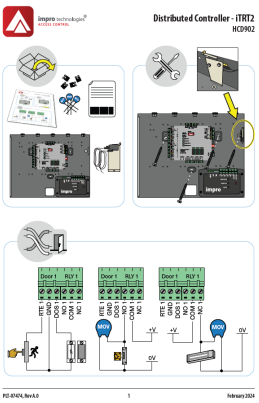
HCD902-0-0-GB - carton contents



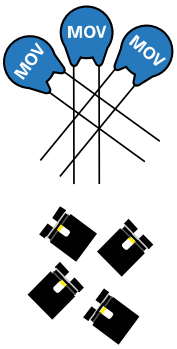
ITRT2 distributed controller in a steel cabinet, built-in DC PSU with an IEC320 mains input socket



Cabinet Tamper Bracket

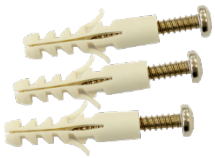


Quick start guide



Metal Oxide Resistors (MOVs)

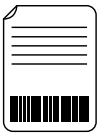
Jumper links



Nylon Wall plug

3 of 5 lid screws

(2 already on the unit, 1 is spare)



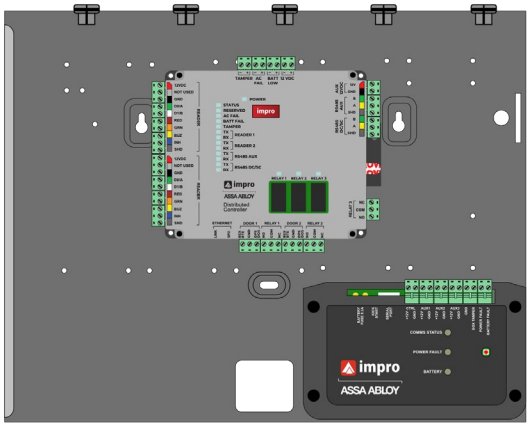
Fixed address label

Cable Ties

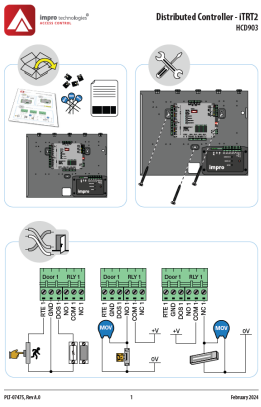
You will need

- Basic electrical installation tools.
- An AC mains cable with a right-angled “kettle” plug that fits the IEC320 socket in the PSU module.
- An auxiliary power supply to power the electric locks.
- Cables for Ethernet, readers, door sensor inputs and relay loads.
- Magnetic reed switch for Door Open Sensor (DOS).
- Push button for Request To Exit (RTE).
- Mag locks or strike locks.
- Mounting hardware: Fasteners suitable for the mounting surface.

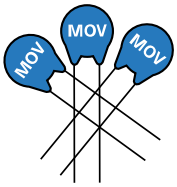
HCD903-0-0-GB - carton contents



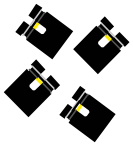
ITRT2 distributed controller in a steel cabinet, built-in DC PSU fed from POE++



Quick start guide



Metal Oxide Resistors (MOVs)

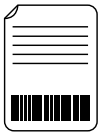


Jumper links

Nylon Wall plug

3 of 5 lid screws

(2 already on the unit, 1 is spare)



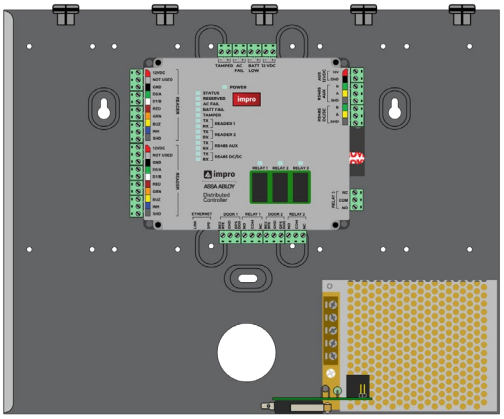
Fixed address label

Cable Ties

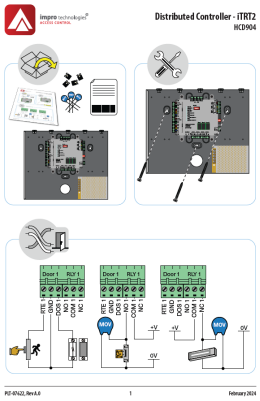
You will need

- Basic electrical installation tools.
- Access to a PoE++ switch, or a suitable PoE++ injector.
- An auxiliary power supply to power the electric locks.
- Cables for Ethernet, readers, door sensor inputs and relay loads.
- Magnetic reed switch for Door Open Sensor (DOS).
- Push buttons for Request To Exit (RTE).
- Mag locks or strike locks.
- Mounting hardware: Fasteners suitable for the mounting surface.

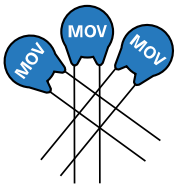
HCD904-0-0-GB - carton contents



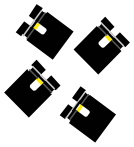
ITRT2 distributed controller in a steel cabinet, built-in DC PSU



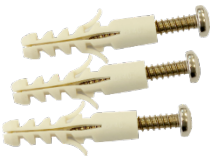
Quick start guide



Metal Oxide Resistors (MOVs)



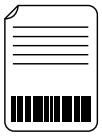
Jumper links



Nylon Wall plug

3 of 5 lid screws

(2 already on the unit, 1 is spare)



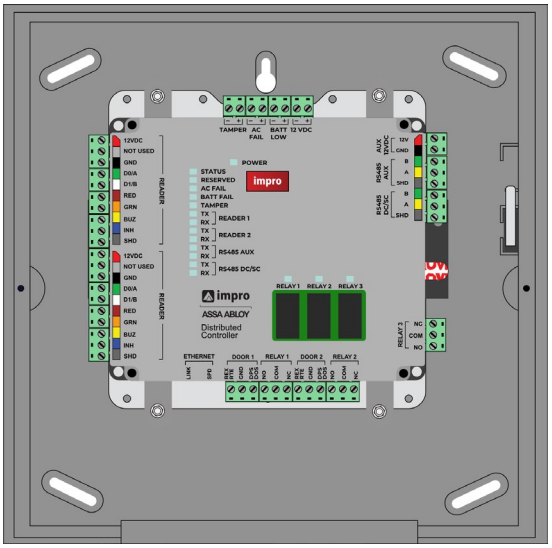
Fixed address label

Cable Ties

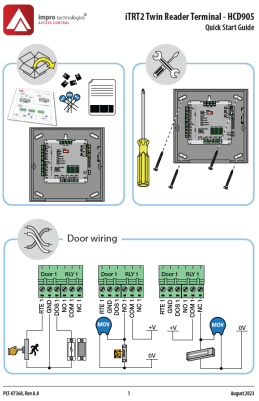
You will need

- Basic electrical installation tools.
- An AC supply cable to wire into the AC terminals (220V AC) on the factory installed mains power adaptor.
- An auxiliary power supply to power the electric locks.
- Cables for Ethernet, readers, door sensor inputs and relay loads.
- Magnetic reed switches for Door Open Sensor (DOS).
- Push buttons for Request To Exit (RTE).
- Mag locks or strike locks.
- Mounting hardware: Fasteners suitable for the mounting surface.

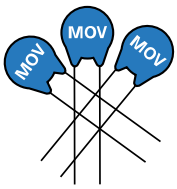
HCD905-0-0-GB - carton contents



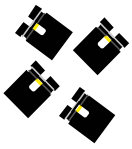
ITRT2 distributed controller in a plastic housing



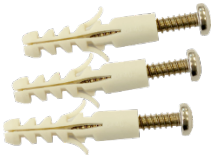
Quick start guide



Metal Oxide Resistors (MOVs)



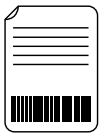
Jumper links



Nylon Wall plug

3 of 5 lid screws

(2 already on the unit, 1 is spare)



Fixed address label

You will need

- Basic electrical installation tools.
- 12V DC 2.5 A DC power supply to power the Distributed Controller.
- An auxiliary power supply to power the electric locks.
- Cables for Ethernet, readers, door sensor inputs and relay loads.
- Magnetic reed switches for Door Open Sensor (DOS).
- Push buttons for Request To Exit (RTE).
- Mag locks or strike locks.
- Mounting hardware: Fasteners suitable for the mounting surface.

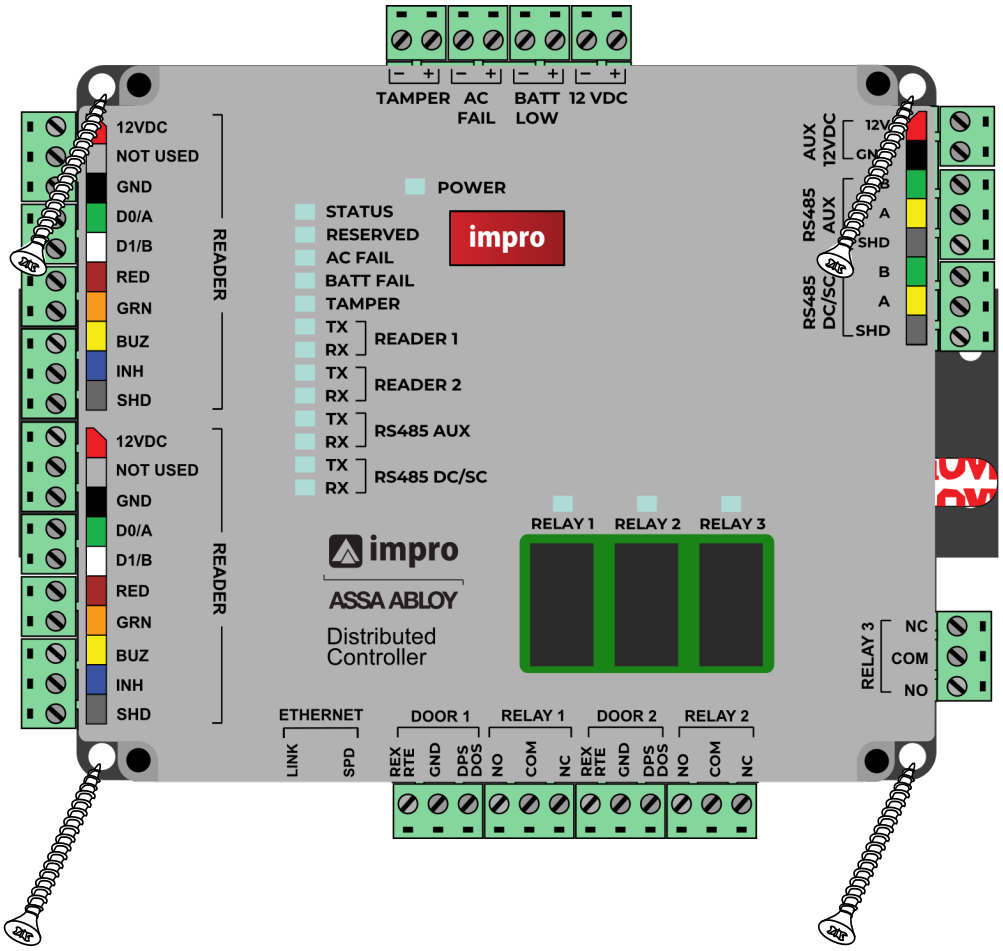
3. Mounting

Choice of mounting location

- Choose a vibration free surface that is sheltered from the sun and the weather.
- Allow for the routing requirements for the cabling.

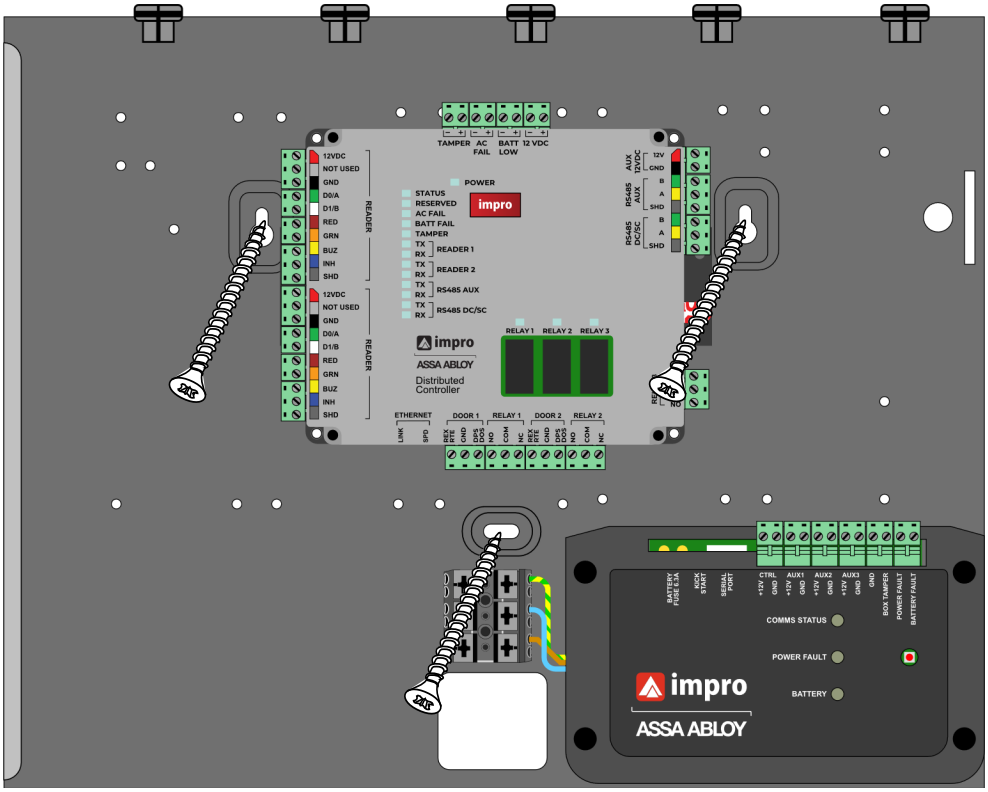
Skip to the mounting instructions for the distributed controller combination you are installing.

Mounting the HCD900-0-0-GB



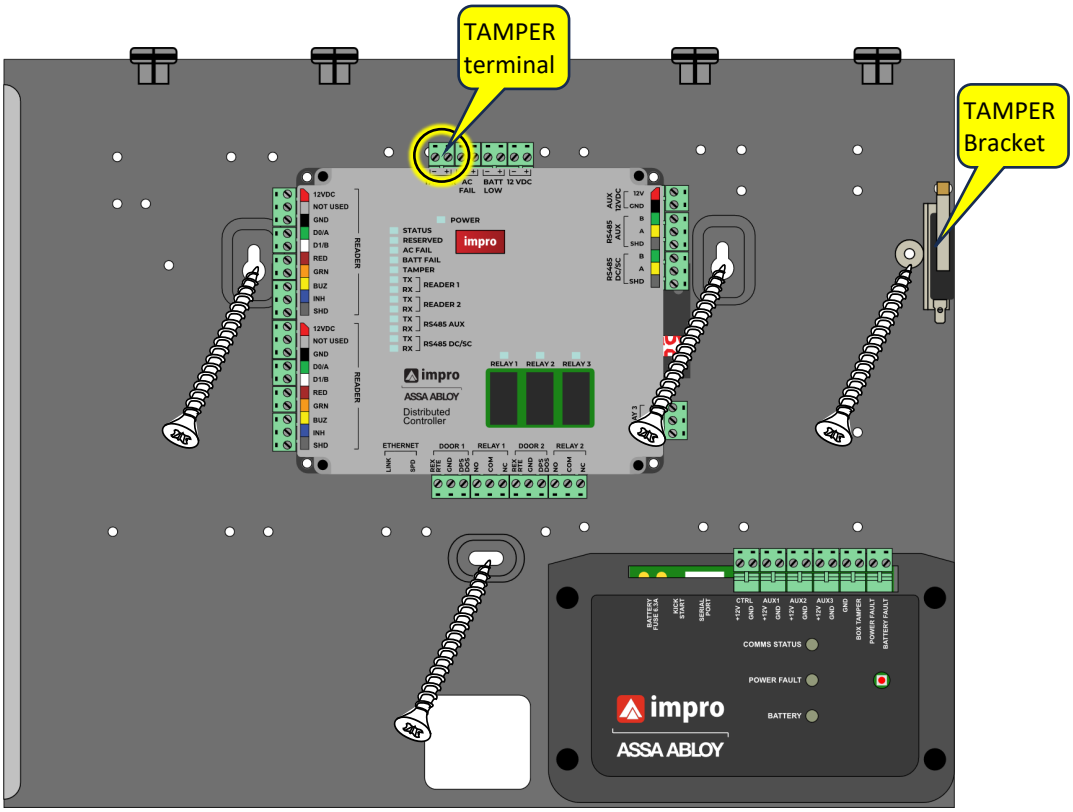
1. Hold the Distributed Controller against the mounting surface (making sure to position it level) and mark the position of the mounting holes on the mounting surface, remove the Distributed Controller and drill the mounting holes.
2. Secure the Distributed Controller to the mounting surface, using suitable screws and wall plugs or bolts and nuts (*note that the mounting holes in the controller have a diameter of 4 mm*).
3. Note the relevant door location and the fixed address of the Distributed Controller – see Site mapping.

Mounting the HCD901-0-0-GB

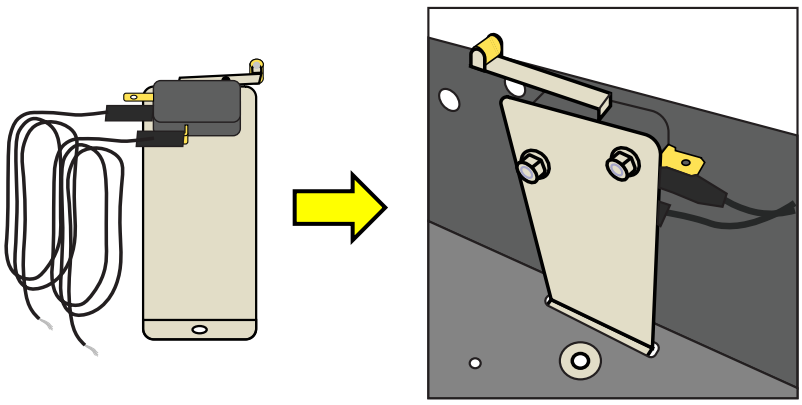


1. Hold the steel cabinet against the mounting surface (making sure to position it level) and mark the location of the three mounting holes on the mounting surface, remove the cabinet and drill the mounting holes.
2. Secure the cabinet to the mounting surface, using suitable screws and wall plugs.
3. Note the relevant door location and the fixed address of the Distributed Controller – see Site mapping.

Mounting the HCD902-0-0-GB

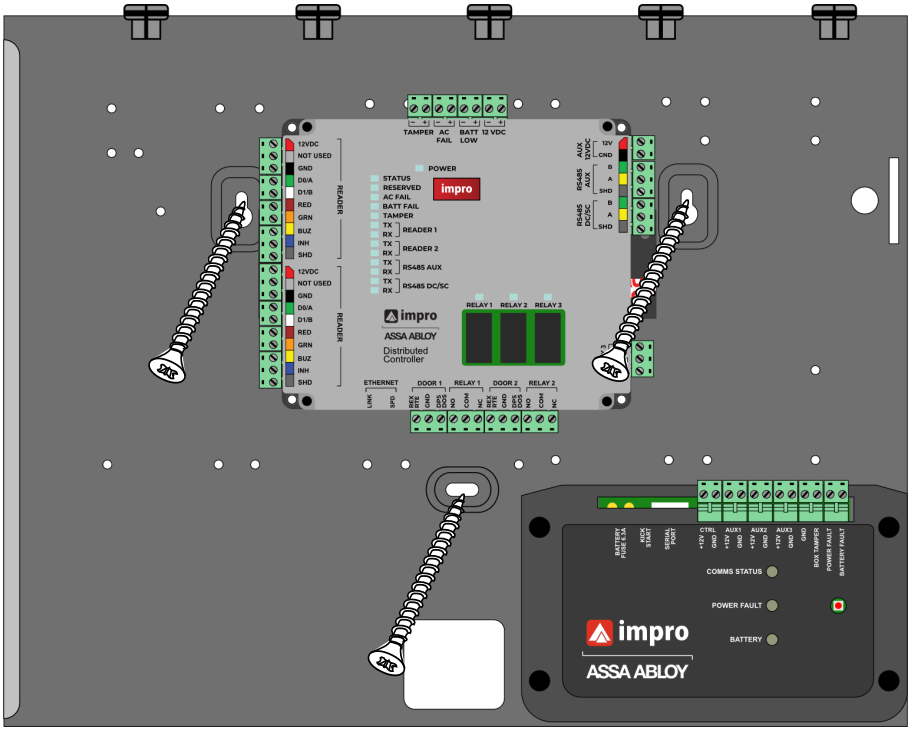


1. Hold the steel cabinet against the mounting surface (making sure to position it level) and mark the position of the three cabinet mounting holes and the centre for the anti-tamper bracket hole on the mounting surface, remove the steel cabinet and drill the mounting holes, and inserting the plastic plugs.
2. Before securing the metal cabinet to the surface, tuck the anti-tamper bracket tab (included in the carton) through the slot in the floor of the cabinet so that the hole in the tag lines up behind the hole in the floor:



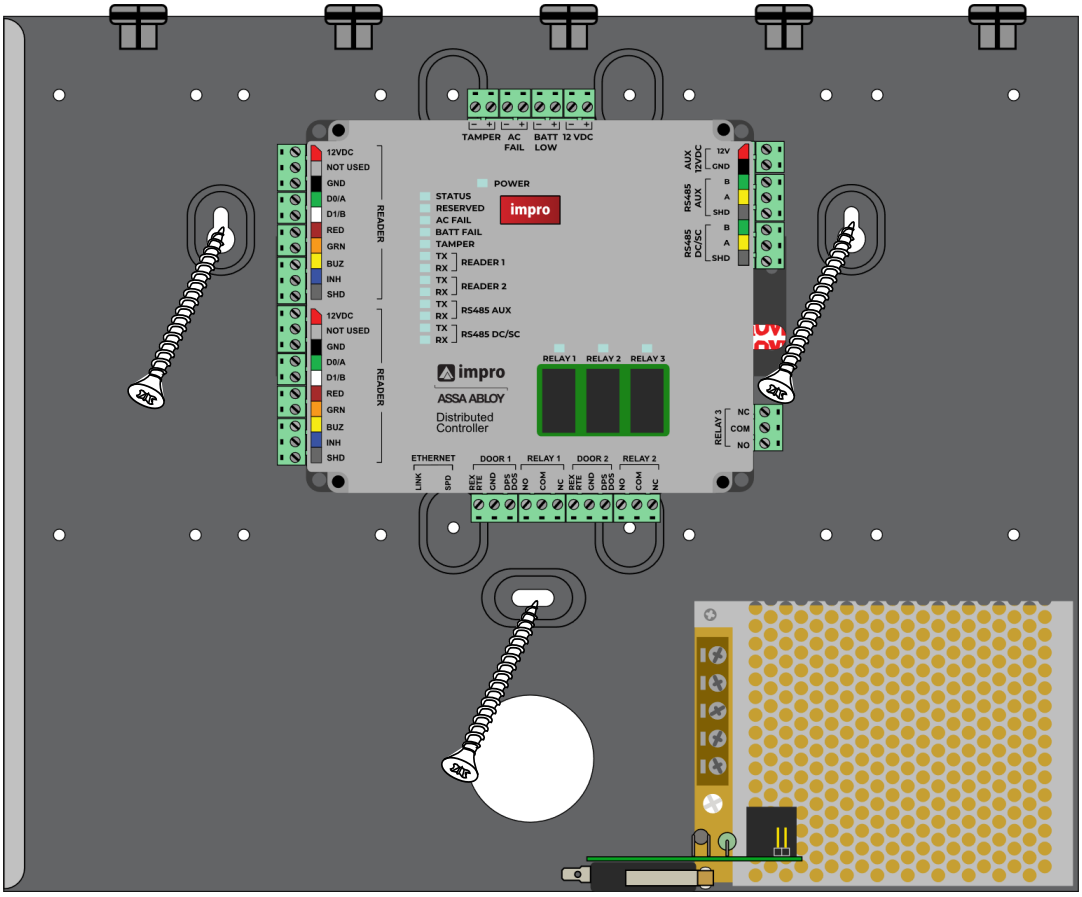
3. Secure the steel cabinet (and the anti-tamper bracket) to the mounting surface, using suitable screws and wall plugs.
4. Wire the anti-tamper switch leads to the “TAMPER” terminal highlighted at the top of this page.
5. Note the relevant door location and the fixed address of the Distributed Controller – see Site mapping.

Mounting the HCD903-0-0-GB



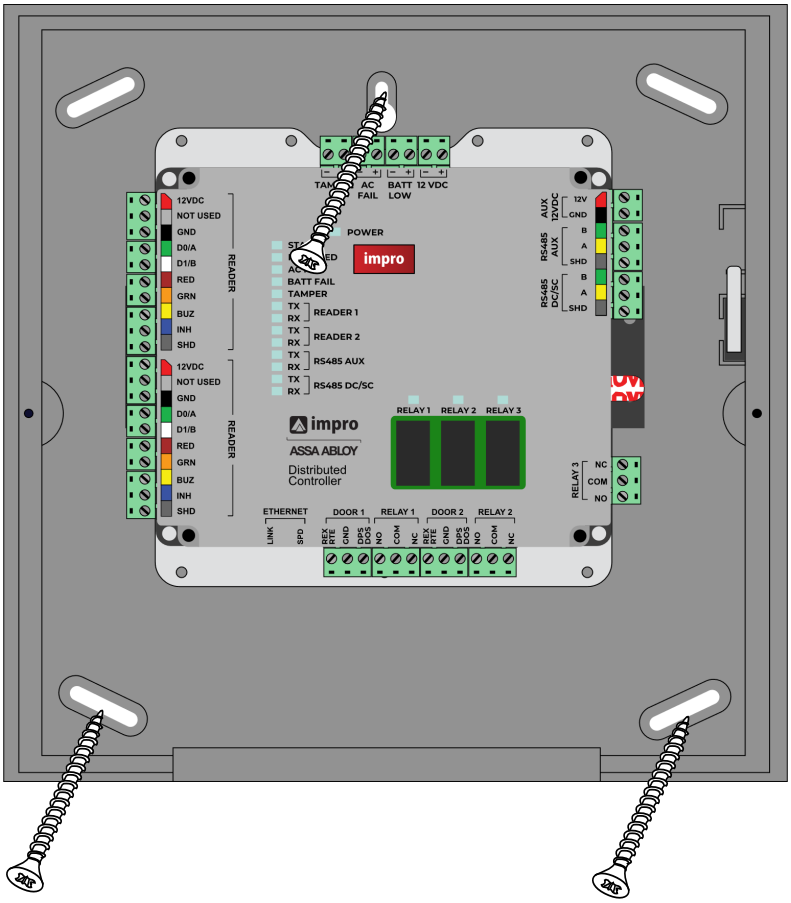
4. Hold the steel cabinet against the mounting surface (making sure to position it level) and mark the location of the three mounting holes on the mounting surface, remove the cabinet and drill the mounting holes.
5. Secure the cabinet to the mounting surface, using suitable screws and wall plugs.
6. Note the relevant door location and the fixed address of the Distributed Controller – see Site mapping.

Mounting the HCD904-0-0-GB



1. Hold the steel cabinet against the mounting surface (making sure to position it level) and mark the location of the three mounting holes on the mounting surface, remove the cabinet and drill the mounting holes.
2. Secure the cabinet to the mounting surface, using suitable screws and wall plugs.
3. Note the relevant door location and the fixed address of the Distributed Controller – see Site mapping.

Mounting the HCD905-0-0-GB

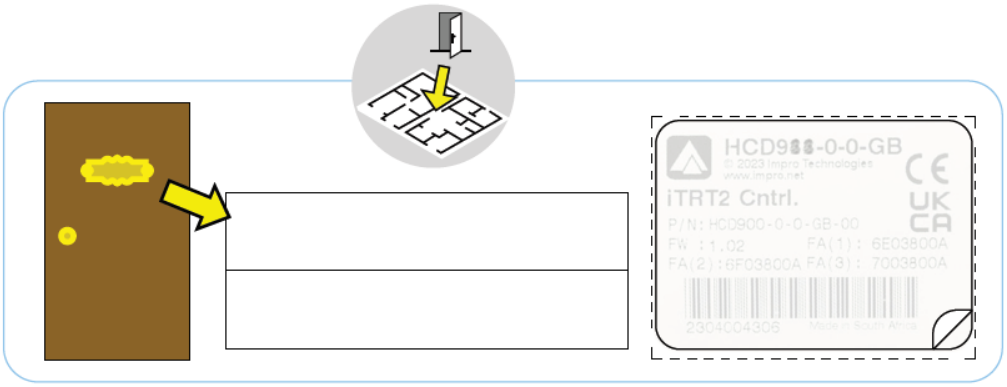


1. Remove the housing lid and hold the plastic housing base against the mounting surface (making sure to position it level) and mark the location of three mounting holes on the mounting surface, remove the cabinet and drill the mounting holes.
2. Secure the housing to the mounting surface, using suitable screws and wall plugs.
3. Note the relevant door location and the fixed address of the Distributed Controller – see Site mapping.

4. Site mapping

Do the following for every iTRT2 that is installed:

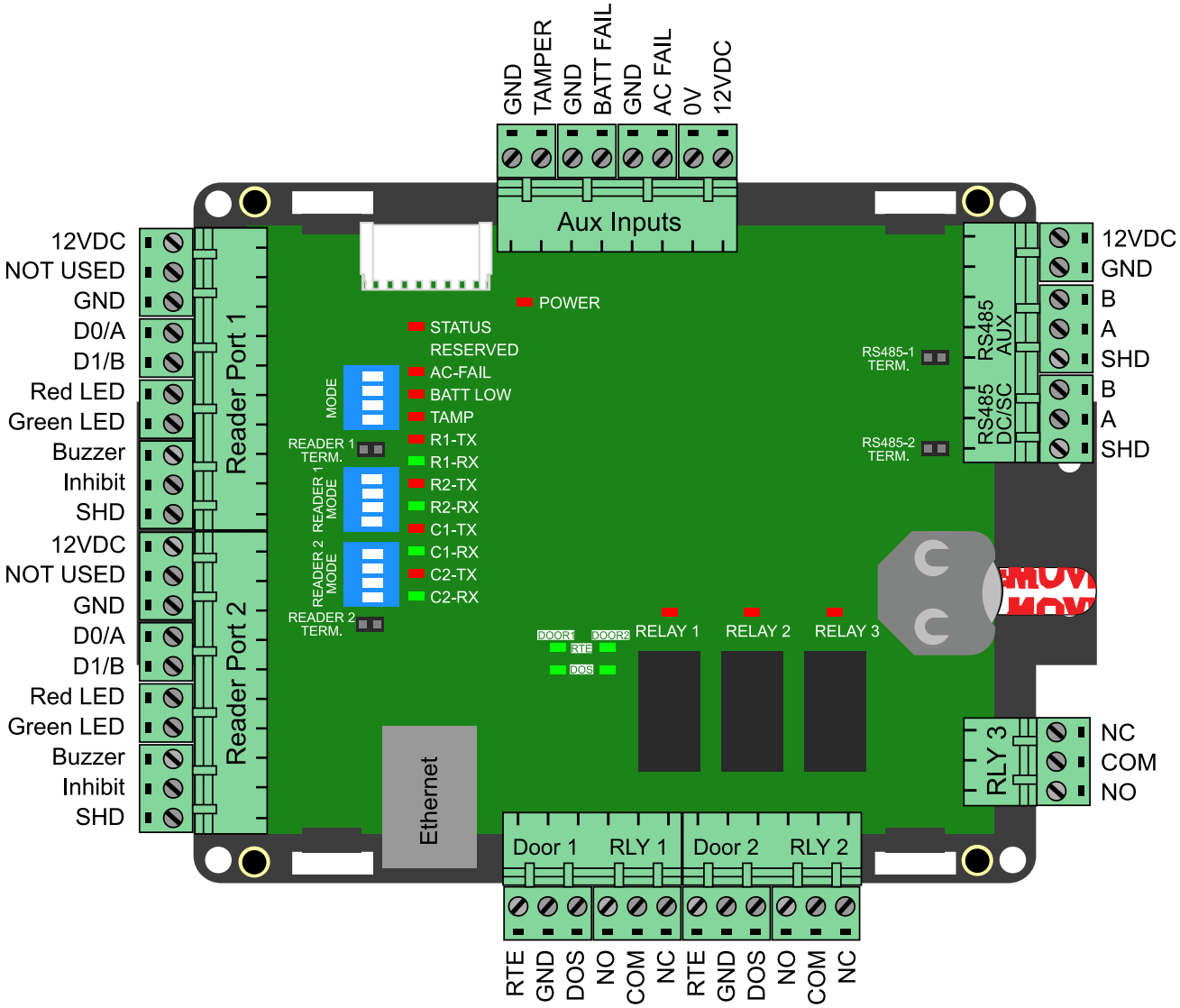
- Apply the spare fixed address label for the Distributed Controller to the Quick Start Guide that is also included with the Distributed Controller.
- Fill in a name for the door served by this iTRT2 - examples: Front reception, Goods receiving, Main gate, etc.



- Alternatively, you can print a plan, or sketch up a rough plan on a sheet of paper and apply the address labels to the plan.
- Keep this site mapping material safe and available for use during the configuration of the access control software.

5. Pinout configuration

Pinout and key components

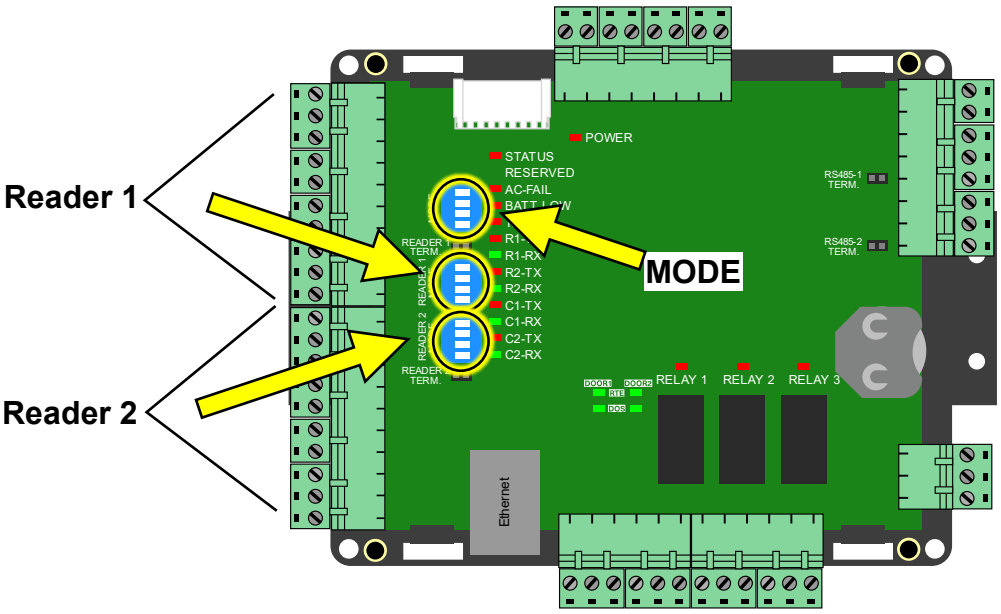


6. DIP switch settings

NOTE

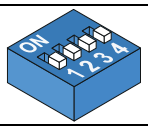
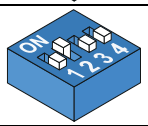
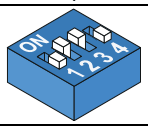
The DIP switch settings (Reader 1, Reader 2 and mode) are only read on power-up.

Remember to cycle the power any time you make changes to these DIP switches.



Controller mode settings

The Distributed Controller can function as a Door Controller or as one of two system controller options:

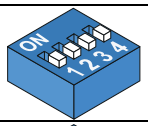
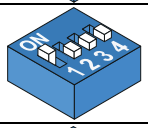
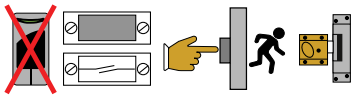
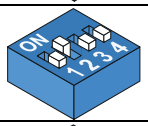
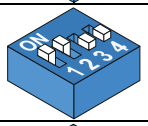
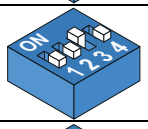
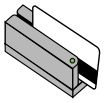
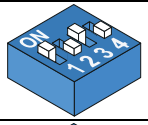
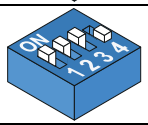
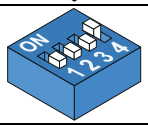
MODE switches	Controller mode	
0000 	Door Controller mode	
0100 	http://aplite/	Access Portal Lite system controller mode Built-in browser accessible web application All AP Lite functions include built-in help
0110 		System controller mode Requires Access Portal or Primo Software running on a networked Windows PC
1XXX 		Factory default mode On power-up this setting will default the Distributed Controller Be sure to return the first switch to OFF after power-up.

Reader port settings

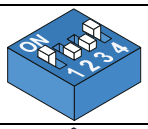
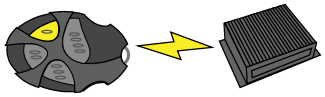
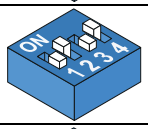
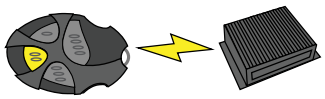
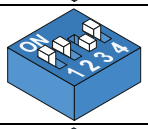
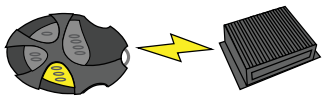
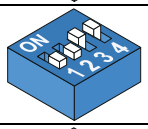
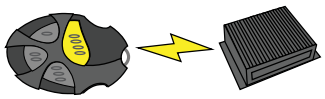
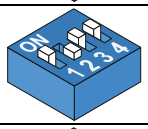
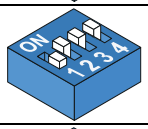
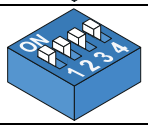
Each of the two reader ports has a dedicated 4-way DIP-switch to select the function of that port.

Notes:

- *Where you have no Impro Multi-discipline Reader connected, setting both remote DIP-switches to the all off position during an Auto-ID will not return any Fixed Addresses.*
- *When Wiegand and Multi Discipline Readers are used on the same system, all DIP Switches should take on the Wiegand settings.*

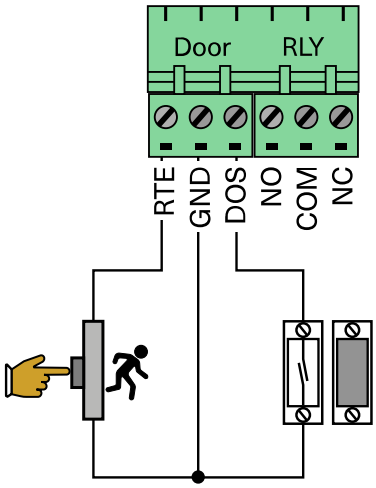
Reader switches	Reader port function	
0 		Channel unused OR Advanced Wiegand Reader (Impro Multi-discipline Readers). Full Tag codes and types
1 		Reader port is disabled. The associated relay and digital inputs remain operative
2 	Not used.	
3 	Legacy support for older Impro RF 4-Channel Receiver and other such hardware Contact Technical Support for further info.	
4 		Magstripe reader. Contact Technical Support for more information.
5 	Not used.	
7 		Wiegand 26, 32, 34, 35, 37, 38, 40, 42, 44, 48-bit, Tag + PIN-code or Reason Code mode. (Idemia Sigma range)
8 		Wiegand open format

This table is continued on the next page.

Reader switches	Reader port function	
9 		UHF Receiver Support If the UHF Receiver is connected, then Button 1 of the Quad Transmitter reports.
10 		UHF Receiver Support If the UHF Receiver is connected, then Button 2 of the Quad Transmitter reports.
11 		UHF Receiver Support If the UHF Receiver is connected, then Button 3 of the Quad Transmitter reports.
12 		UHF Receiver Support If the UHF Receiver is connected, then Button 4 of the Quad Transmitter reports.
13 	 #	OSDP Reader
14 		OSDP Reader - Report parity stripped PACS
15 	Not used	

7. Door wiring

Wiring door sensors and push buttons

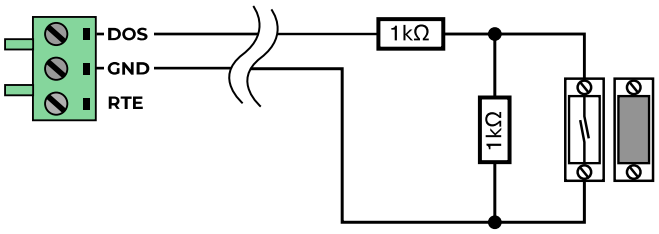


Wiring end-of-line (EOL) sensing circuit (optional)

End-of-line (EOL) sensing enables the Distributed Controller to raise an alarm when somebody tampers with the circuit (cutting or shorting the wires) connected to any of the RTE or DOS inputs – as long as the EOL resistors have been fitted, and the access control software is configured for end-of-line monitoring.

The resistors must be located at the door sensor / push button, on the secure side of the door.

When the circuit is cut, or the resistors are bypassed, the Distributed Controller detects the invalid resistance and raises an alarm. (This feature works identically for the RTE input)



Wiring the relay terminals

Relay contact specifications

Voltage	Maximum Current
< 28V DC	10A

Note:

It is recommended that a separate power supply is used for the external loads.

AUX Relay

The AUX relay is reserved for future functionality.

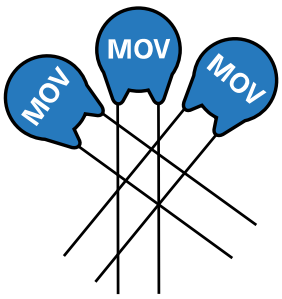
Wiring snubber devices (warranty requirement)

Snubber devices suppress sparking across the relay contacts caused by switching current to inductive loads, such as solenoid driven strike locks and mag locks. Failure to install suitable snubber devices will severely impact relay life and void the manufacturer's warranty.

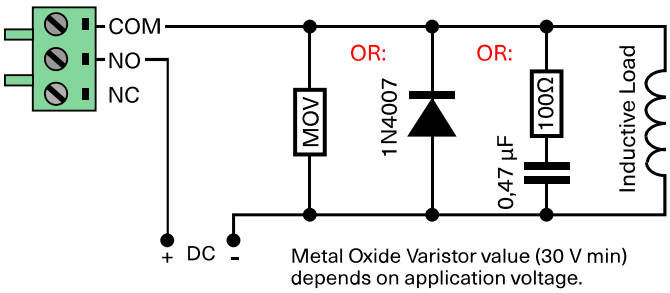
Note:

Some locks include built-in snubber components, some don't.

In the case of the latter, Metal Oxide Varistors (MOVs) suitable for inductive loads up to 24 V DC are included with the Distributed Controller.



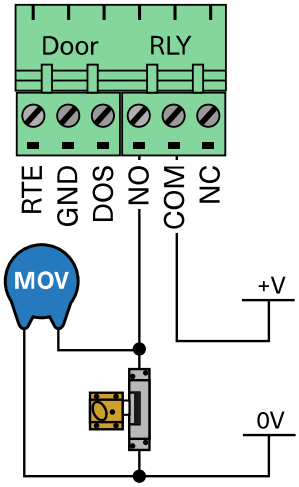
The diagram below shows alternative snubber arrangements.



Wiring a strike lock

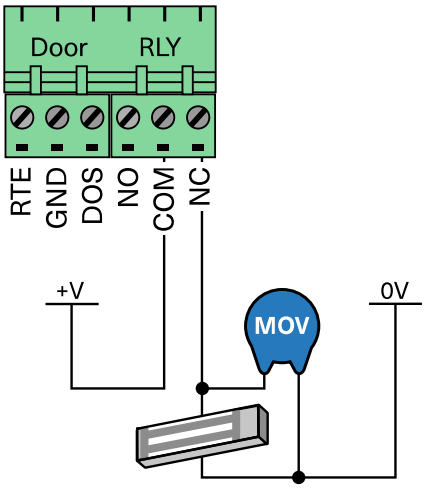
This method is suitable for inductive loads that are powered from a DC supply of up to 24V, using the Metal Oxide Varistors MOVs that are included in packaging with the Distributed Controller.

This wiring arrangement will be "fail SECURE": Loss of control of the relay, or a broken wire, would leave the door in the LOCKED state.



Wiring a magnetic lock

This wiring arrangement will be fail SECURE: Loss of control of the relay would leave the door in the LOCKED state. If the supply to the solenoid is cut off the door is no longer locked.



Door wiring cable specifications

Application	Conductors (# of wires)	Cross Sectional Area	AWG	Max Length
Door Strike / Mag Lock (12V and higher)	2	0.75 mm2 (0,0012 in2)	20	150m (492 ft)
Door Open Sense (DOS)	2	0.75 mm2 (0,0012 in2)	20	150m (492 ft)
Request To Exit (RTE)	2	0.75 mm2 (0,0012 in2)	20	150m (492 ft)

Relay contact specifications

Voltage	Maximum Current
< 28V DC	10A

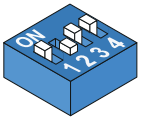
8. Reader wiring

Wiring OSDP readers

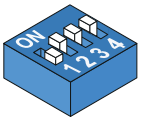
The two reader channels on the Distributed Controller are independent and can be set up to accommodate different reader types.

Note:

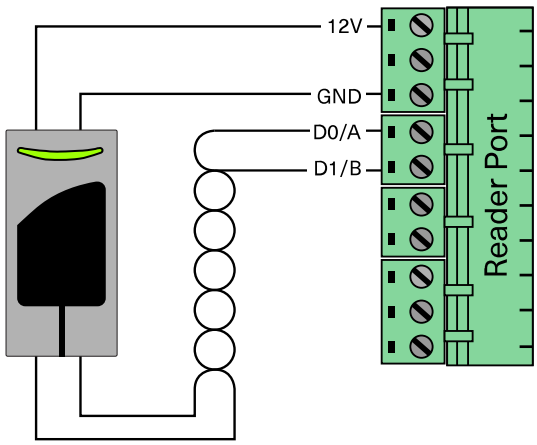
The 12V terminal is internally fused and can supply up to 350 mA. The fuse will reset when current falls below the 350 mA threshold.



OSDP Reader



OSDP Reader - Report parity stripped PACS



OSDP pairing (During Commissioning)

1. Set the reader to Installation Mode (referring to the reader's installation guide on how to do this).
2. TOGGLE the first switch on the relevant iTRT2 reader port.
3. When the TX and RX LEDs for that reader port return to regular, rapid flashing, the reader is ready for use.

WARNING:

A factory default of the iTRT2 will require steps 1-3 to be performed again.

OSDP cable specifications

Notes:

- *While the cable suggested for Wiegand readers (up to 150m long) can work for OSDP reader, it is recommended that OSDP cables any longer than 150m should comply fully to the RS-485 EIA/TIA standard.*
- *If the reader cable length exceeds 150m, a local 12V DC power supply will be needed to power the OSDP reader. The volt drop across long cables would otherwise result in insufficient supply voltage at the reader.*

Cable length	Power source	Cable Spec
Up to 150m	+12V from the Distributed Controller	as per Wiegand
Up to 1000m	Local DC power source	full RS-485 EIA/TIA

Wiring Wiegand readers and Impro multi-discipline readers

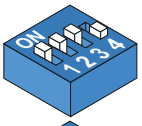
The diagram below shows the connections for Wiegand readers, including the wire colours for the pigtail variants of the Impro readers. The coloured labels on the Distributed Controller cover are included in the diagram for reference.

Impro readers without pigtails will have labelled wiring terminals that use the same naming convention as the Distributed Controller terminals.

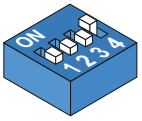
Notes:

There are two DIP switch setting options for Wiegand readers.

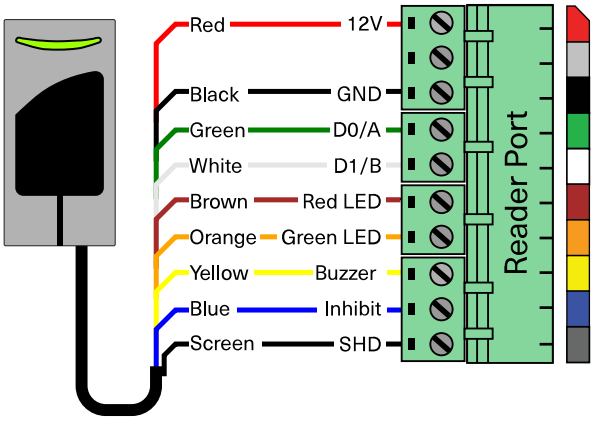
The 12V terminal is internally fused and can supply up to 350 mA. The fuse will reset when current falls below the 350 mA threshold.

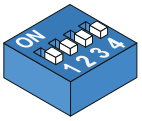


Wiegand 26, 32, 34, 35, 37, 38, 40, 42, 44, 48-bit, Tag + PIN-code or Reason Code mode.
(Idemia MA100, MA200, MA300 or Idemia J-Series)



Wiegand open format





Impro Multi-discipline readers

Wiegand cable specifications

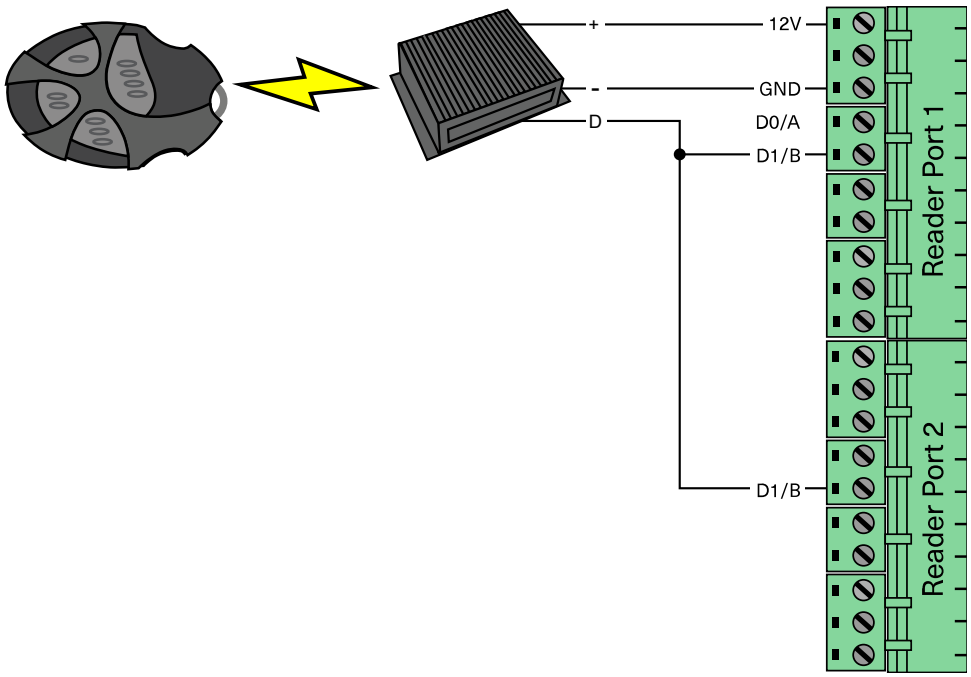
Application	Conductors (# of wires)	Cross Sectional Area	AWG	Max Length
Wiegand / Multi-discipline	10 (8 used)	0.32 mm2 (0.0005 in2)	20	150 m (492 ft)

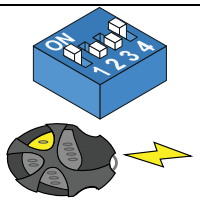
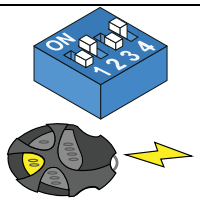
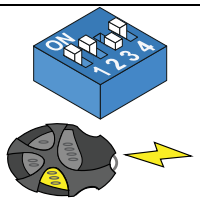
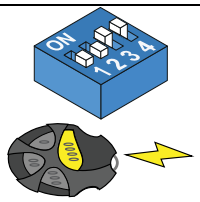
Wiring the UHF receiver

The Impro Quad Receiver allows the access control system to respond to a four-button UHF remote. One iTRT2 can handle the monitoring of any TWO of the four buttons (selected by the Reader 1 and Reader 2 DIP switch setting on the Distributed Controller).

Note

The Impro Quad Transmitter also contains an RFID credential that can be read by Impro Multi-discipline readers.



Reader port DIP switch settings			
Reader mode 09	Reader mode 10	Reader mode 11	Reader mode 12
 Relay responds to button #1 on the remote	 Relay responds to button #2 on the remote	 Relay responds to button #3 on the remote	 Relay responds to button #4 on the remote

Quad Receiver cable specifications

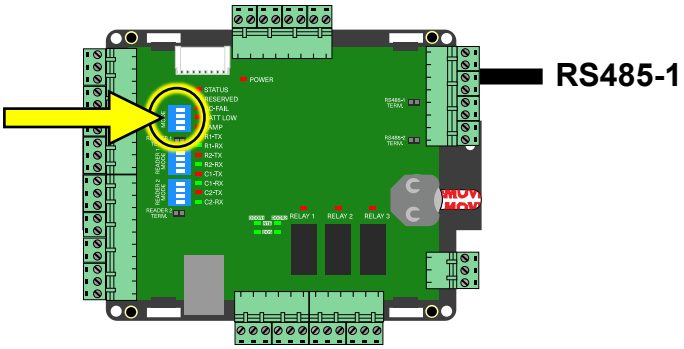
Conductors (# of wires)	Cross Sectional Area	AWG	Max Length
3 used	0.32 mm2 (0.0005 in2)	20	150m (492 ft)

Download the Quad Receiver Installation Manual for more information:

https://ftp.impro.net/

Navigate: Manuals > Hardware > Impro Technologies >General Hardware > Readers > Quad Rec-insm-en-*XX.pdf*

9. Controller MODES



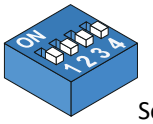
Door controller mode

Use this mode when this iTRT2 is part of an Access Portal System, where:

- **T**he Door Controller iTRT2 is networked via IP -
- OR via RS485 from another iTRT2 configured as an Access Portal System Controller.

Use this mode when this iTRT2 is part of an AP Lite System, where:

- The Door Controller iTRT2 must be networked (via RS485) to another iTRT2 configured as an AP Lite System Controller.



Set the controller mode DIP switch settings to 0000 for Door Controller mode.

Fixed address handling capacity

As a Door Controller the Distributed Controller only uses up a maximum of two fixed addresses.

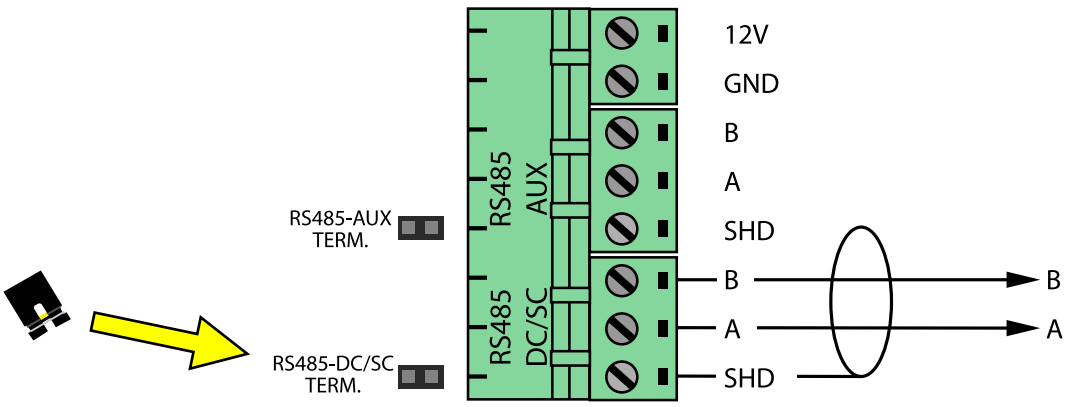
RS485 wiring

Use the RS485-1 port for iTRT2 Door Controller networking.

Daisy-chain the connections and be sure to install the RS485-DC/SC terminating jumper, only on the door controlling iTRT2 that is most distant from the networked system controller iTRT2.

Note:

The 12V terminal is internally fused and can supply up to 350 mA. The fuse will reset when current falls below the 350 mA threshold.



APLite Controller mode

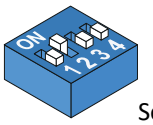
- This system controller mode configures the Distributed Controller to function as a stand-alone Physical Access Control System (PACS) for maximum of 32 fixed addresses.
- The user can manage and configure the system on any (HTML 5 compliant) browser via the Ethernet Port, using the embedded web application within the Distributed Controller.
- Make sure that you back up the AP LITE settings using the Firmware Update Utility:

https://ftp.impro.net/

***Navigate**: Software > APLite & Access in a Box > v3.185 > Firmware Upgrade Utility.exe*

Note:

APLite mode does NOT support IP communications with other controllers.



Set the controller mode DIP switches to 0100 for APLite mode.

Fixed address handling capacity

Access Portal Lite mode can handle a maximum of 32 fixed addresses including:

- Up to two addresses for the on-board reader interfaces.
- Daisy-chained Door Controllers on RS485-1, with their reader port addresses contributing to a total no larger than 32.

Ethernet connection

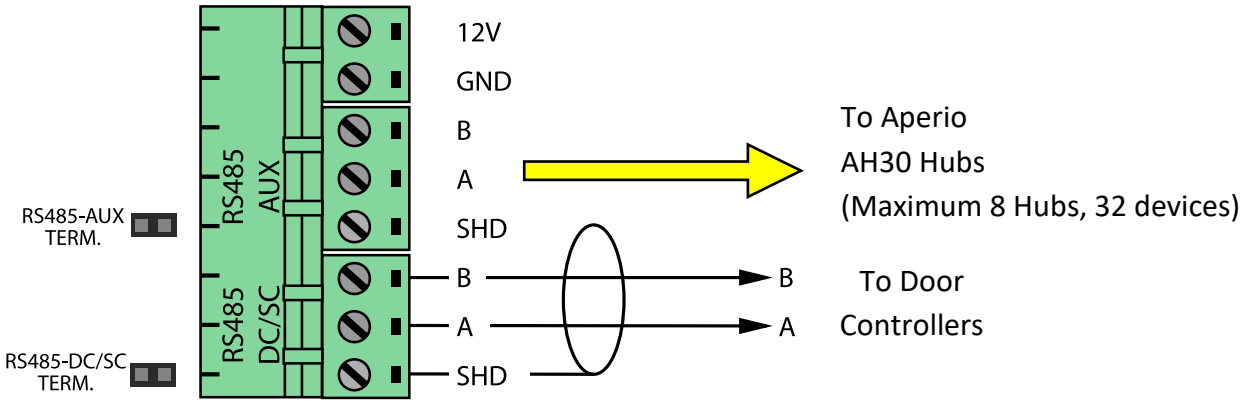
Connect this to the Ethernet network to allow access to the built-in AP Lite web application. Login and setup as discussed under AP Lite in the commissioning section.

RS485 wiring

- Use the RS485-AUX port to daisy-chain to any downstream Door Controllers. Be sure to connect the RS485-2 terminating jumper on the door controlling iTRT2 that is most distant from the controlling iTRT2.
- Use the RS485-CD/SC port to connect to Aperio™ hubs for wireless lock control.

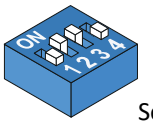
Note

Only connect the controller end of the RS485 screen to SHD, this will prevent ground loops.



System Controller mode

This system controller mode sets up the Distributed Controller to be used in an Access Portal or Primo access control system.



Set the controller mode DIP switches to 0110 for System Controller mode

Offline operation

The Distributed Controller will remember all credentials that have successfully accessed the doors that it controls. If the network connection is broken or lost, the Distributed Controller will continue to allow access for those credentials.

Fixed address handling capacity via RS485

Access Portal Controller mode will allow the Distributed Controller to handle up to 64 fixed addresses, including:

- Up to two addresses for the on-board reader interfaces.
- Daisy-chained Door Controllers on RS485, with their reader port addresses contributing to a total no larger than 64.

Ethernet connection

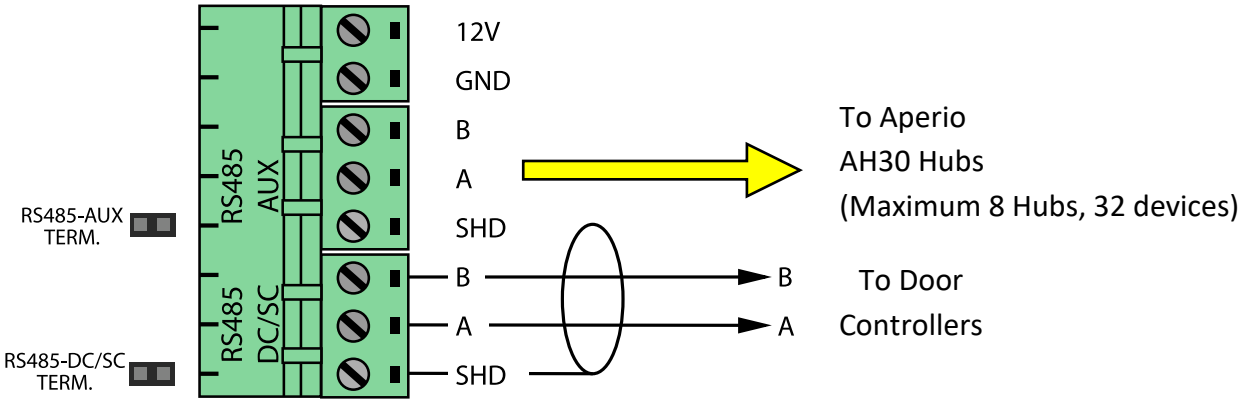
Connect the Distributed Controller to the access control system computer via Ethernet.

RS485 wiring

Use the RS485-DC/SC port to daisy-chain to any downstream Door Controllers. Be sure to connect the RS485-DC/SC terminating jumper on the door controlling iTRT2 that is most distant from the controlling iTRT2.

Note

Only connect the controller end of the RS485 screen to SHD, this will prevent ground loops.



10.Networking Distributed Controllers

mode settings for different locations in an installation.

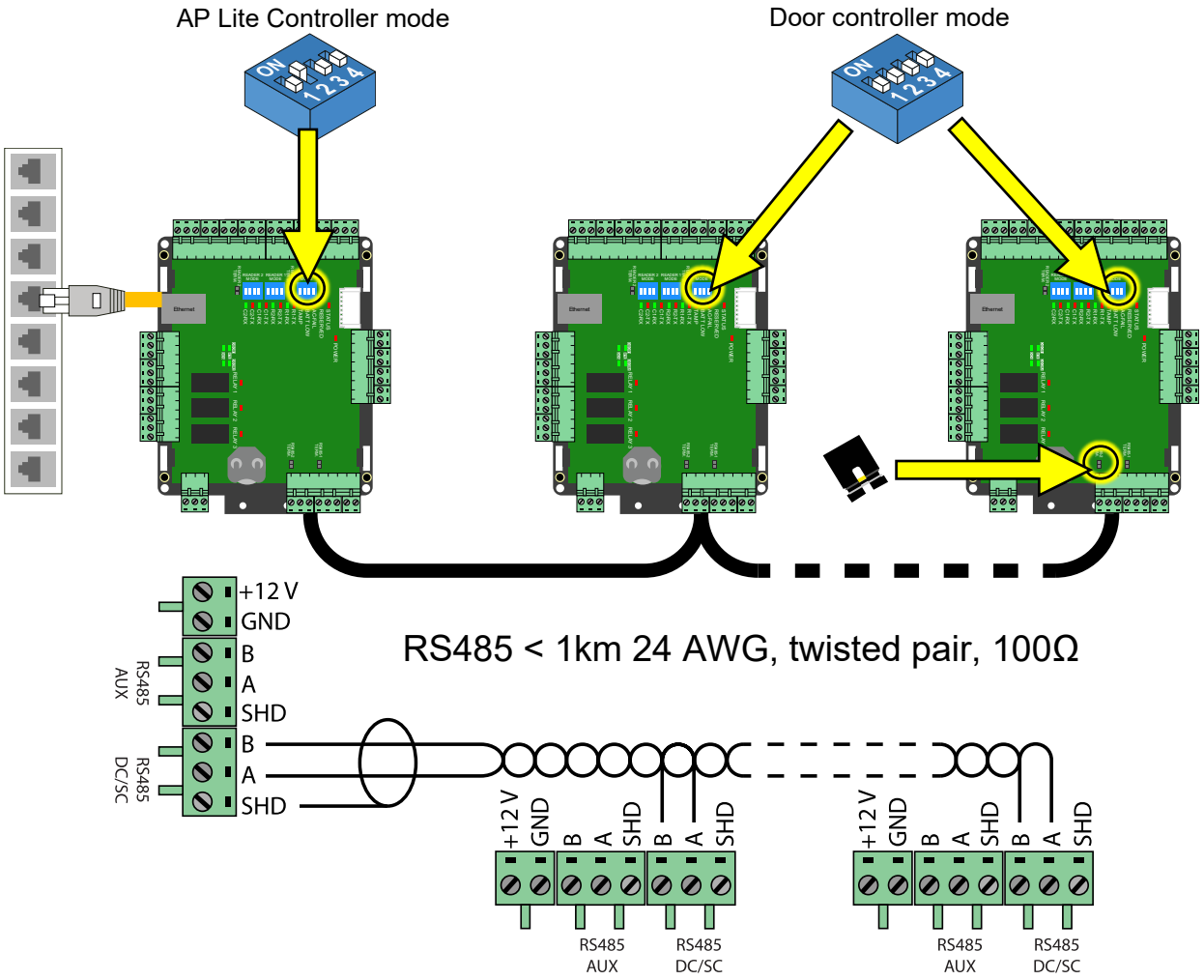
AP Lite installations

Notes

In AP Lite installations all Door Controllers must be daisy-chained to the AP Lite Controller.

Install RS485-2 jumper for most distant iTRT2 on the RS485 daisy-chain.

Only connect the controller end of the RS485 screen to SHD, this will prevent ground loops.



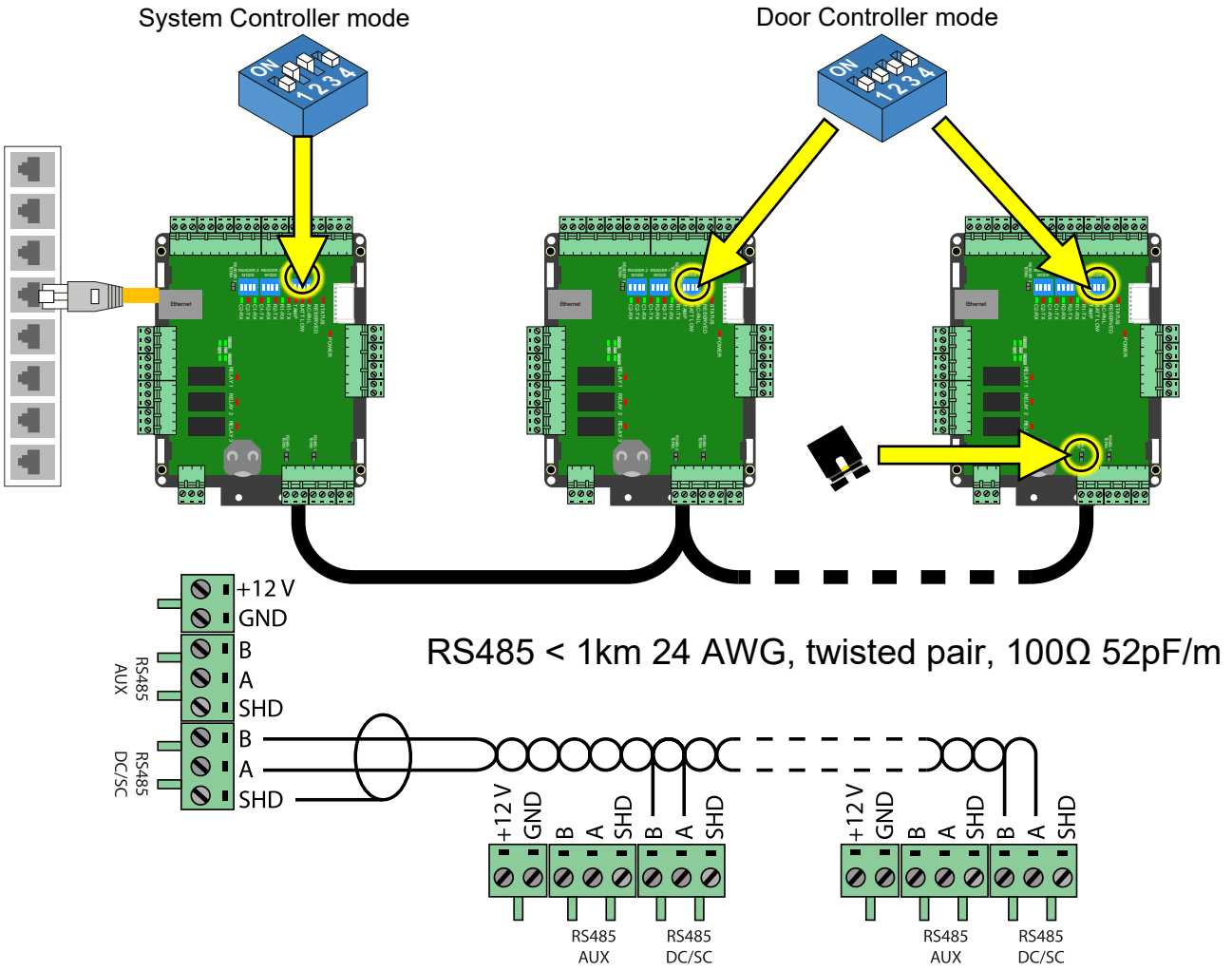
Access Portal or Primo installations

Notes

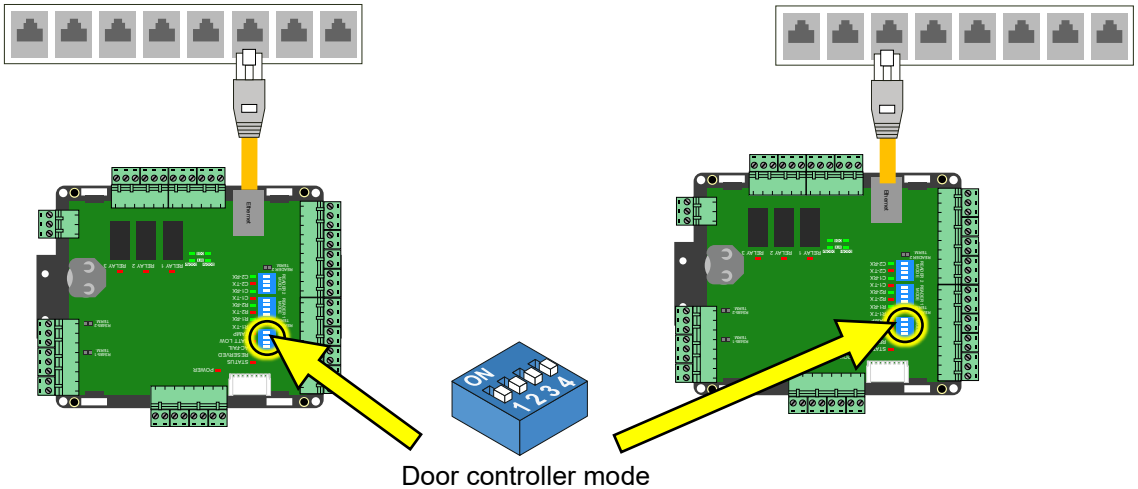
*Door Controllers in Access Portal or Primo installations can be daisy-chained to a System Controller **OR** connected directly to an Ethernet switch, **OR** some to each – whatever is most practical for the site.*

Install RS485-2 jumper for most distant iTRT2 on the RS485 daisy-chain.

Only connect the controller end of the RS485 screen to SHD, this will prevent ground loops.



Door Controllers can connect to Access Portal or Primo via Ethernet:



Using the Distributed Controller in legacy installations

The Distributed Controller will work (in Door Controller mode) in legacy installations, as per the legacy iTRT - but take note that the pinout of the Distributed Controller terminals is a little different.

There are no 5V terminals.

Observe the Distributed Controller pinout shown in this manual to avoid any mistakes.

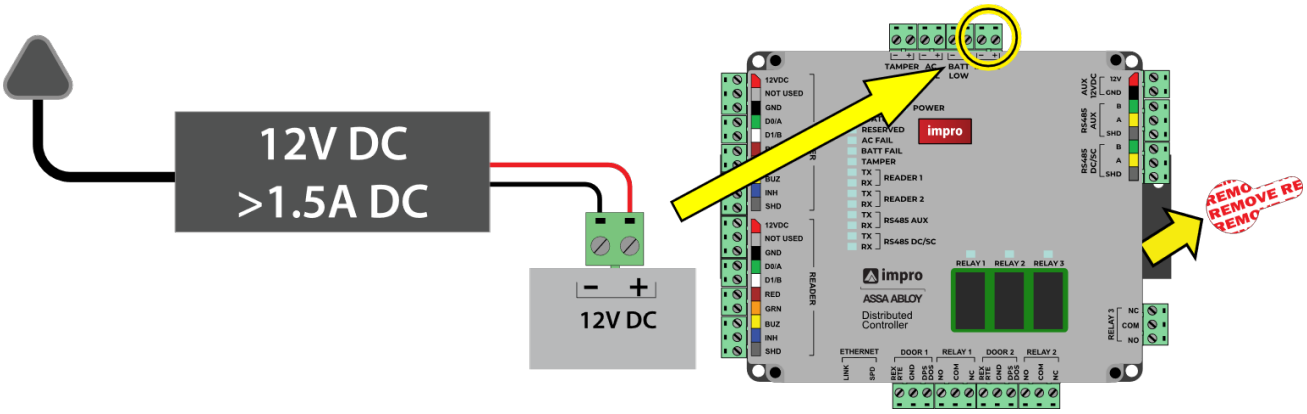
11.Commissioning

Before powering up:

- Check the wiring, making sure that any peripheral wiring, such as door sensors and locks, are correct and properly secured.
- If Door Controllers are linked with RS485, make sure that the most distant unit has the RS485-1 line termination jumper in place.
- Skip to the heading for powering up the combo that you are working with:

Powering up the HCD900

1. Wire a 12V DC power supply (not included) to the 12V DC terminal block on the Distributed Controller.
2. Remove the insulating tag from the button cell holder on the PCB.
3. Plug the mains cable into a mains outlet and switch it on.
4. Allow a minute for the Distributed Controller to boot up and test both the RAM and flash checksums.
5. When the Distributed Controller passes the self-test, the red status LED will remain steadily illuminated as long the unit is powered up.
6. Use a separate power supply to power up any loads that are switched using the onboard relays.



Notes:

If any part of the self-test fails, the red status LED will keep flashing.

If installing OSDP readers be sure to follow the three OSDP pairing steps on page 27

7. The access control software can now be configured:

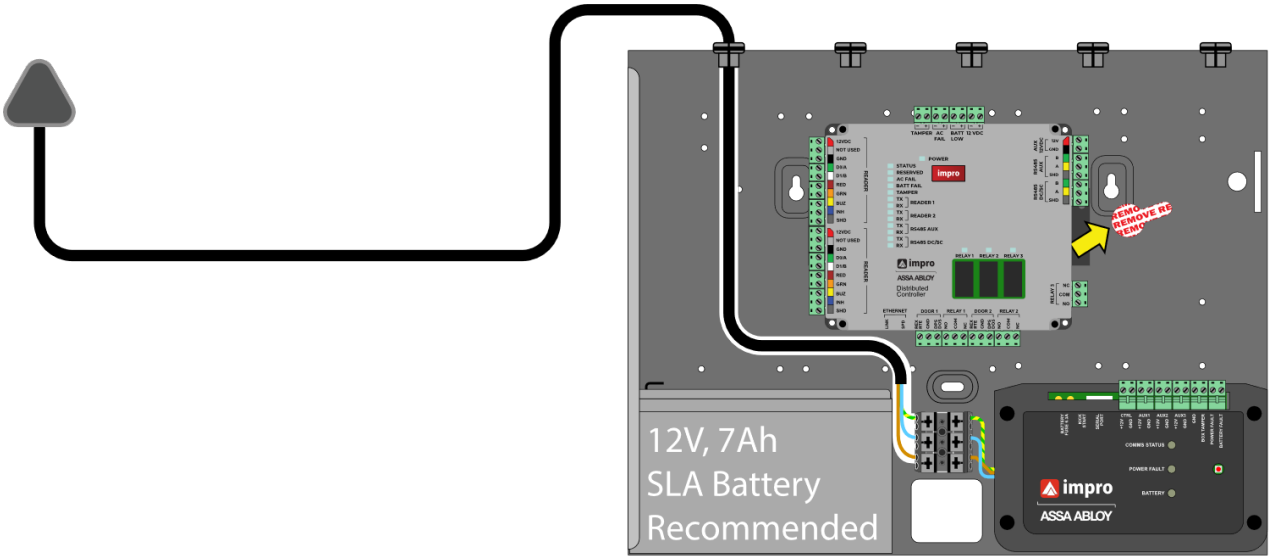
- Access Portal Lite (APLite) for small installations
- Primo (or Access Portal) for medium, large and multi-site installations

Powering up the HCD901

1. Wire the 220V AC power cable to the AC terminal block inside the cabinet.
2. Remove the insulating tag from the button cell holder on the PCB.
3. Plug the mains cable into a mains outlet and switch it on.
4. Allow a minute for the Distributed Controller to boot up and test both the RAM and flash checksums.
5. When the unit passes the self-test, the red status LED will remain steadily illuminated as long the unit is powered up.
6. Use a separate power supply to power up any loads that are switched using the onboard relays.

Optional gel battery

Installing the recommended 12V gel battery will allow the Distributed Controller to continue normal operation in the event of a power outage. Connect the factory installed battery leads to the battery, observing the correct polarity.



Notes:

If any part of the self-test fails, the red status LED will keep flashing.

If installing OSDP readers be sure to follow the three OSDP pairing steps on page 27

7. The access control software can now be configured:

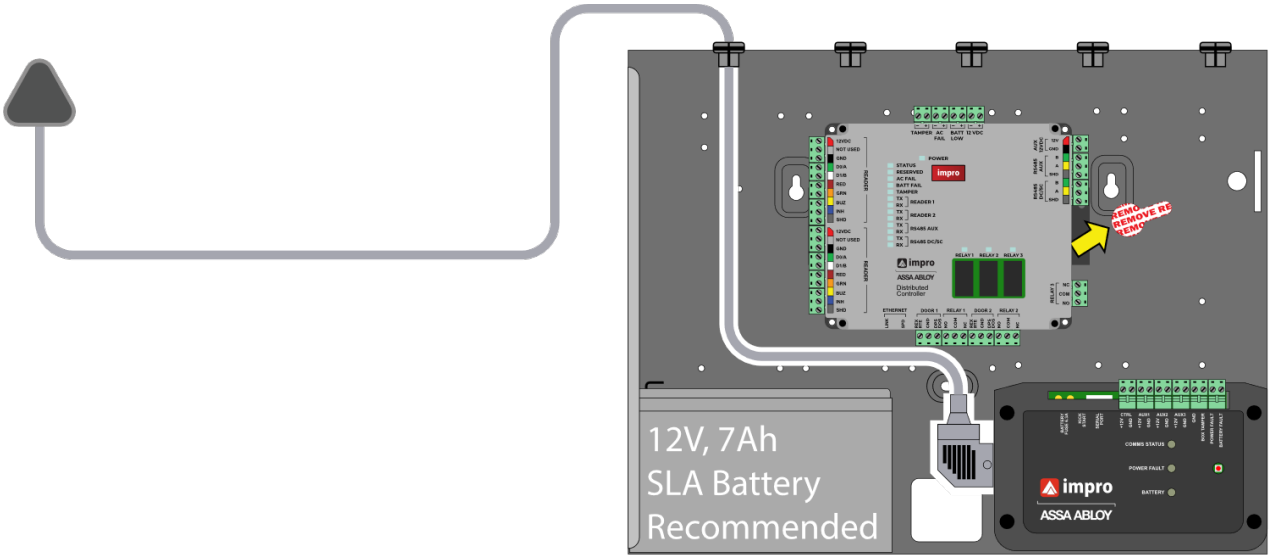
- Access Portal Lite (APLite) for small installations
- Primo (or Access Portal) for medium, large and multi-site installations

Powering up the HCD902

1. Plug a right-angled “kettle” plug power cable into the IEC320 socket of the impro power supply.
2. Remove the insulating tag from the button cell holder on the PCB.
3. Plug the mains cable into a mains outlet and switch it on.
4. Allow a minute for the Distributed Controller to boot up and test both the RAM and flash checksums.
5. When the unit passes the self-test, the red status LED will remain steadily illuminated as long the unit is powered up.
6. Use a separate power supply to power up any loads that are switched using the onboard relays.

Optional gel battery

Installing the recommended 12V gel battery will allow the Distributed Controller to continue normal operation in the event of a power outage. Connect the factory installed battery leads to the battery, observing the correct polarity.



Note:

If any part of the self-test fails, the red status LED will keep flashing.

If installing OSDP readers be sure to follow the three OSDP pairing steps on page 27

7. The access control software can now be configured:

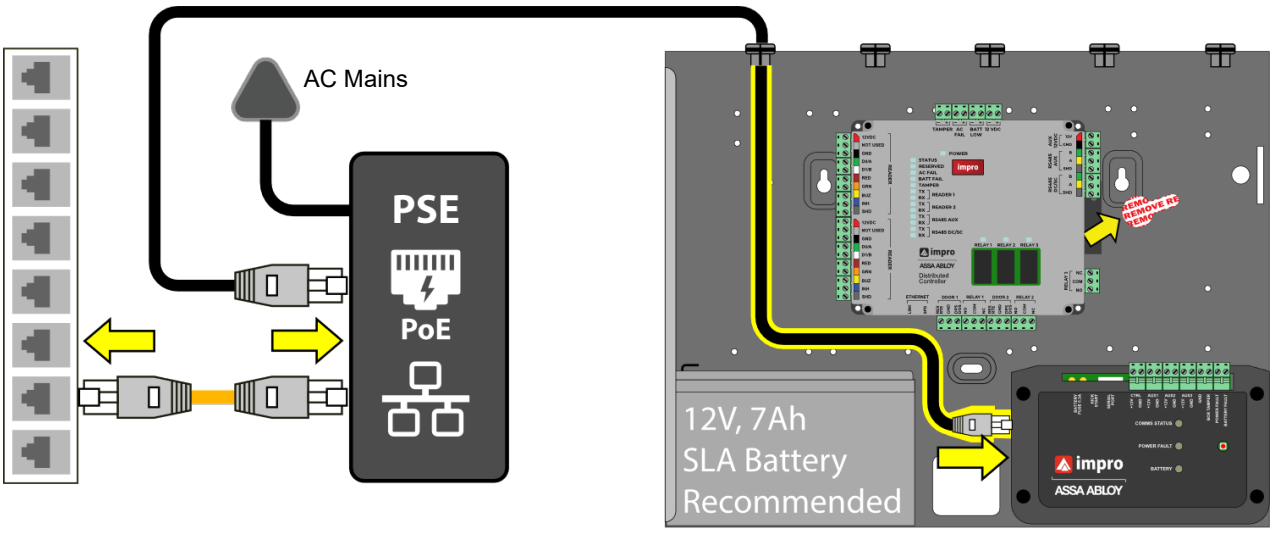
- Access Portal Lite (APLite) for small installations
- Primo (or Access Portal) for medium, large and multi-site installations

Powering up the HCD903

1. This unit is powered via PoE (Power over Ethernet) and will require a PoE switch – or a PoE injector (illustrated below).
2. Remove the insulating tag from the button cell holder on the PCB.
3. Plug the mains cable into a mains outlet and switch it on.
4. Allow a minute for the Distributed Controller to boot up and test both the RAM and flash checksums.
5. When the unit passes the self-test, the red status LED will remain steadily illuminated as long the unit is powered up.
6. Use a separate power supply to power up any loads that are switched using the onboard relays.

Optional gel battery

Installing the recommended 12V gel battery will allow the Distributed Controller to continue normal operation in the event of a power outage. Connect the factory installed battery leads to the battery, observing the correct polarity.



Note:

If any part of the self-test fails, the red status LED will keep flashing.

If installing OSDP readers be sure to follow the three OSDP pairing steps on page 27

7. The access control software can now be configured:

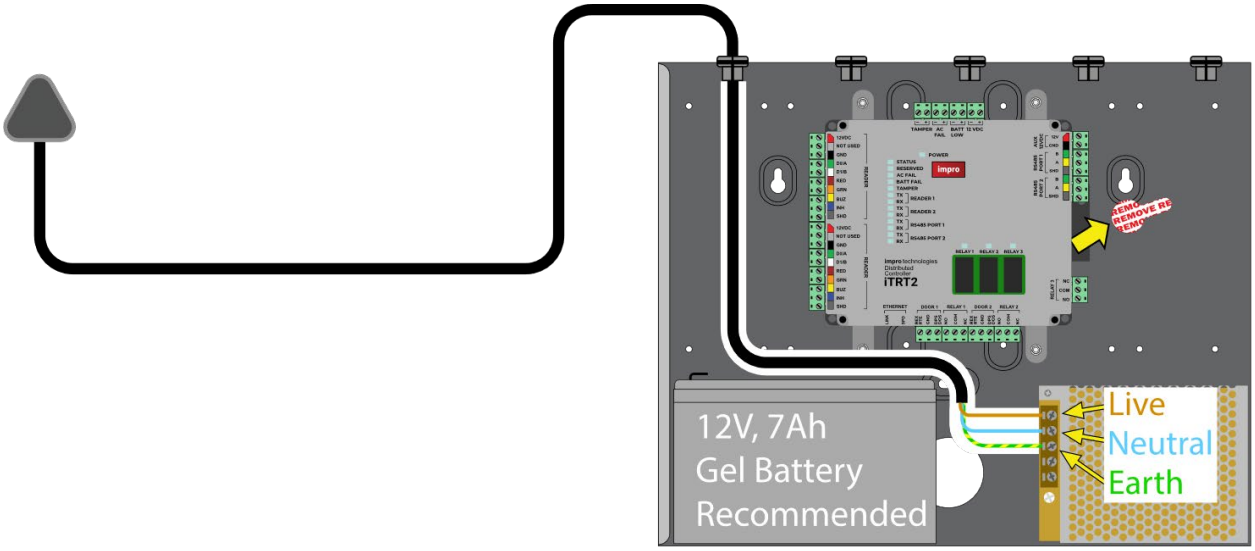
- Access Portal Lite (APLite) for small installations
- Primo (or Access Portal) for medium, large and multi-site installations

Powering up the HCD904

8. Wire the 220V AC power cable to the AC power terminals on the power supply module inside the cabinet.
9. Remove the insulating tag from the button cell holder on the PCB.
10. Plug the mains cable into a mains outlet and switch it on.
11. Allow a minute for the Distributed Controller to boot up and test both the RAM and flash checksums.
12. When the unit passes the self-test, the red status LED will remain steadily illuminated as long the unit is powered up.
13. Use a separate power supply to power up any loads that are switched using the onboard relays.

Optional gel battery

Installing the recommended 12V gel battery will allow the Distributed Controller to continue normal operation in the event of a power outage. Connect the factory installed battery leads to the battery, observing the correct polarity.



Note:

If any part of the self-test fails, the red status LED will keep flashing.

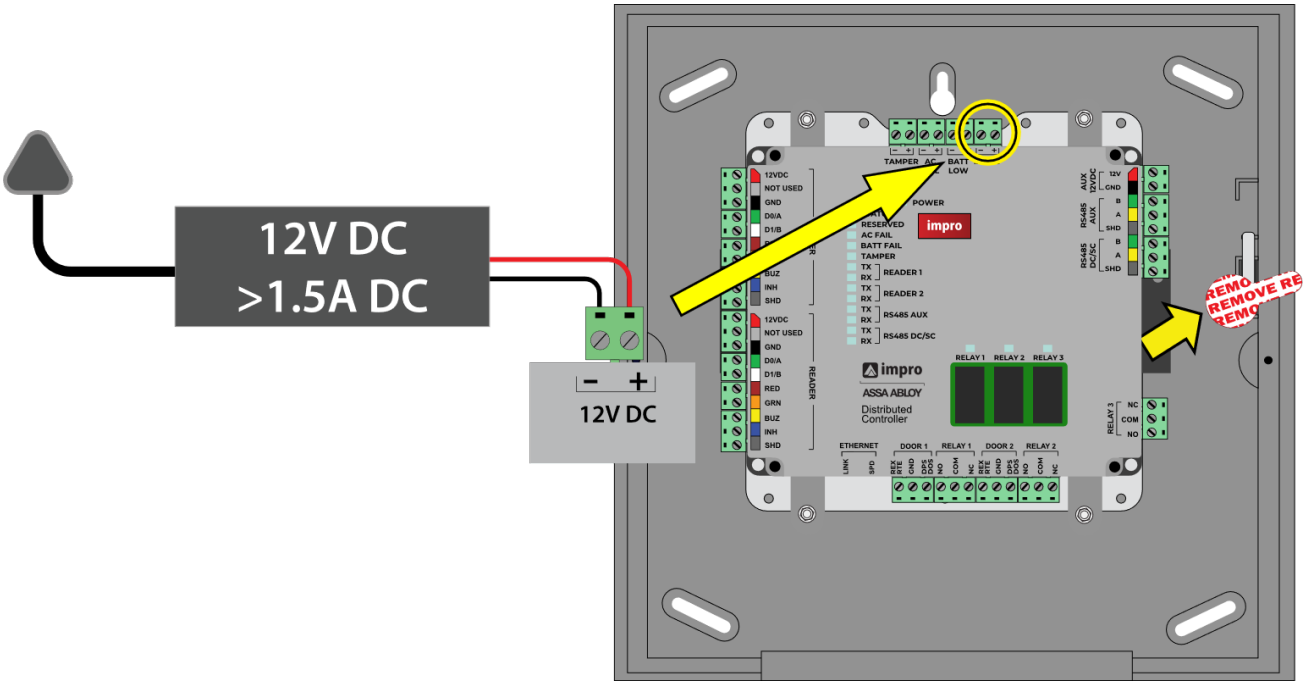
If installing OSDP readers be sure to follow the three OSDP pairing steps on page 27

14. The access control software can now be configured:

- Access Portal Lite (APLite) for small installations
- Primo (or Access Portal) for medium, large and multi-site installations

Powering up the HCD905

1. Wire a 12V DC power supply (not included) to the 12V DC terminal block on the Distributed Controller.
2. Remove the insulating tag from the button cell holder on the PCB.
3. Plug the mains cable into a mains outlet and switch it on.
4. Allow a minute for the Distributed Controller to boot up and test both the RAM and flash checksums.
5. When the unit passes the self-test, the red status LED will remain steadily illuminated as long the unit is powered up.
6. Use a separate power supply to power up any loads that are switched using the onboard relays.



Note:

If any part of the self-test fails, the red status LED will keep flashing.

If installing OSDP readers be sure to follow the three OSDP pairing steps on page 27

7. The access control software can now be configured:

- Access Portal Lite (APLite) for small installations
- Primo (or Access Portal) for medium, large and multi-site installations

Setting up the access control system

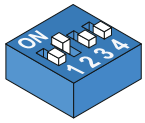
The impro Distributed Controllers accommodate two system modes

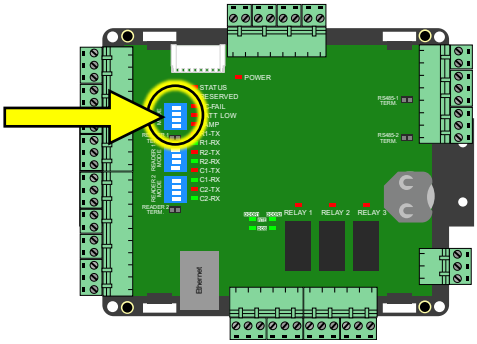
- Access Portal Lite (APLite) for small installations
- Primo (or Access Portal) for medium, large and multi-site installations

Setting up the built-in Access Portal Lite (AP Lite)

AP Lite is suitable for installations having 32 or less readers/doors and a maximum of 1000 credential holders.

Getting started with Access Portal Lite web application

mode: 



You will need any site mapping information that was gathered during the hardware installation.

1. Use an HTML 5 compliant browser to access the web application embedded in the Distributed Controller - with only ONE* iTRT2 (set for AP Lite mode) connected to the network.
2. Follow this link: http://aplite/
3. Login using the default username and access code:
    - username: **admin**
    - Access code: **12345**

Create the necessary user accounts and use the options available to add and configure hardware. All functions include context sensitive help.

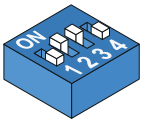
Contact technical support for more assistance.

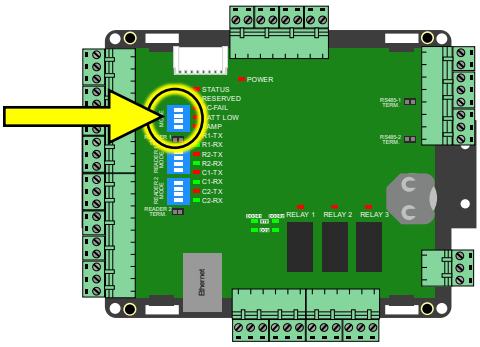
Notes:

** More than one AP-Lite Distributed Controller can exist on the same network – but in such cases you will have to manually specify the IP for each unit.*

All Impro Technologies hardware includes spare fixed address labels that should be applied to a site map that you can refer to when allocating the hardware devices to their respective doors and areas.

Setting up the external access control system

mode: 



Visit the impro Technologies website This full-featured access control system is offered with different license options suitable for sites ranging from medium to large, as well as enterprises that are located on multiple campuses any distance apart. If Primo (or Access Portal) is not already installed on the site host computer, it can be downloaded from the Impro Technologies website: www.impro.net

With the Access Portal software installed and running, log in, create the necessary user accounts, and use the options available to add and configure hardware. All functions include context sensitive help.

Contact Technical Support for more assistance.

Note:

All Impro Technologies hardware includes spare fixed address labels that should be applied to a site map that you can refer to when allocating the hardware devices to their respective doors and areas.

12.Factory reset and RTC

Factory reset

Note:

Defaulting the Distributed Controller will erase all AP Lite related user data stored in the Distributed Controller.

- Back up the AP Lite data using the Firmware Update Utility.
  - This same Firmware Update Tool can be used to restore the AP LITE settings after a factory reset is performed – or if the Distributed Controller is replaced, for any reason.
- If you have set a static IP address, make a note of it as it will be reset when you perform a factory reset.

The most likely reason to perform a factory reset would be when the Distributed Controller has been inadvertently allocated an IP Address that falls outside of the system mask. In this state, the Distributed Controller module will get a DHCP assigned address. If no address is assigned by a DHCP server, the module will revert to 192.168.100.1 with a subnet of 255.255.255.0.

How to factory reset

Note:

The DIP switches are read on power-up.

Do the following with the **mode** bank of DIP switches:

1. Set **DIP Switch 1** to the **ON** position (ignore the other switches)

2. Cycle the DC power to the Distributed Controller PCB (remove and replace the power plug on the PCB).
3. Allow 30 seconds for the start-up process to complete.
4. Set **DIP Switch 1** back to the **OFF** position. (If you don't do this the controller will factory reset every time the power cycles.)

Real-time clock (RTC)

The on-board real-time clock is synchronised with the network through the access control software applications. The RTC is powered by a CR2032 3V lithium button cell, ensuring correct time is kept if DC power to the iTRT is interrupted.

13.Specifications

Working temperature range

-20 ºC to +65 ºC

Environment

Designed to work in an indoor (dry) environment (IP20), the Distributed Controller is not sealed against water.

Power supply requirements

Input Voltage Range	12 to 15 V DC, polarity sensitive	
Power Requirements	**Current (mA)**	**Power (W)**
12 V DC with no readers connected and relays off	20	0.24
12 V DC with maximum reader load and both relays energised	600	7.2

12V DC Power outputs

Reader 1	To power readers 1&2	Maximum current output 350 mA per output Fuse resets when the current falls below 350 mA
Reader 2		
AUX	To power Aperio lock hubs	

Communication ports

ETHERNET PORT

Port type	Standard Ethernet RJ45 connector 10/100 Base T, half/full duplex

RS485 AUX

Purpose	This port is reserved for controlling Aperio wireless lock hubs
Electrical Interface	RS485
Baud Rate	19 200
Data Format	8 bits, no parity, 1 stop bit
Communications Protocol	Aperio Communications Protocol
Line Termination (RS485)	Provision is made for line termination (jumper)

RS485 DC/SC

Purpose	This port is for networking Impro controller hardware
Electrical Interface	RS485
Baud Rate	38 400
Data Format	8 bits, no parity, 1 stop bit
Communications Protocol	Impro Secure Communications Protocol
Line Termination (RS485)	Provision is made for line termination (jumper)

Power and Status indicators

LED indication	Meaning of the indication
Continuous red	Power is on
Intermittent flashing red	Door Controller Communications failure
Continuous flashing red	iTRT2 fault

Power supply and tamper indicators

LED indication	Meaning of the indication
Red AC-FAIL LED on	AC power is down and the Distributed Controller is running on battery
Red BAT LOW LED on	The battery is either flat or not connected
Red TAMP LED on	Open circuit across the tamper switch terminals

Ethernet indicators

LED indication	Meaning of the indication
Link LED continuous red	Ethernet is connected
SPD LED continuous red	Speed at 100 MHz
SPD LED OFF	Speed at 10 MHz

RS485 indicators (1 & 2)

LED indication	Meaning of the indication
Red TX LED on	Sending data
Green RX LED on	Receiving data

Reader indicators (1 & 2)

LED indication	Meaning of the indication
Red TX LED on	Sending data
Green RX LED on	Receiving data

Revision history

Date	Description	Revision
March 2023	Initial release	A.0
September 2024	Included mention of Primo and all housing combo variants of the iTRT2	A.1

Impro Technologies
has over 30 years' experience
in the access control industry

HQ tel: +27 (31) 717 0700
Email: info@impro.net
Web: www.impro.net

PLT-06326, A.1
December 2024