

AVIGILONTM ALTA

Access Control System

Installation Guide

Some hardware may show the Openpath logo.

© 2024, Avigilon Corporation. All rights reserved. AVIGILON, the AVIGILON logos, and AVIGILON ALTA are trademarks or registered trademarks of Avigilon Corporation. Allegion, ENGAGE technology and Schlage are trademarks of Allegion plc, its subsidiaries and/or affiliates in the United States and other countries. Safari is a trademark of Apple Inc., registered in the U.S. and other countries and regions. IOS is a trademark or registered trademark of Cisco in the U.S. and other countries and is used under license. All other trademarks are the property of their respective owners.

This document has been compiled and published using product descriptions and specifications available at the time of publication. The contents of this document and the specifications of the products discussed herein are subject to change without notice. Avigilon Corporation reserves the right to make any such changes without notice. Neither Avigilon Corporation nor any of its affiliated companies: (1) guarantees the completeness or accuracy the information contained in this document; or (2) is responsible for your use of, or reliance on, the information. Avigilon Corporation shall not be responsible for any losses or damages (including consequential damages) caused by reliance on the information presented herein.

Avigilon Corporation
avigilon.com

20240730-en

Revisions

Guide	Description
July 2024	Regulatory notice updates: Regulatory notice on page 67 Software and firmware updates (blinking yellow, blinking red): Expansion board Status LED indicator on page 53 , Access Control Core Status LEDs on page 54 , Smart Reader LED indicator on page 54 , Avigilon Pro Series Reader LED indicator on page 55
April 2024	App name updates: Avigilon Alta Open app (formerly, Openpath Mobile Access app), Avigilon Alta Access app (formerly, Open Admin app)
March 2024	Pro Series Readers (Video Intercom Reader Pro, Video Reader Pro) updates: UL 294 on page 67 , Electrical specifications on page 71 Resolve common issues on page 63
October 2023	Core Series Smart Hub (SYS-4ENT-DVE1, SYS-ELEV-SVE1, SYS-8ENT-DVE2, SYS-8ENT-DVE4, SYS-16ENT-DVE6) and Access Control Core (OP-CR-ACC) updates: For more information on page 9 , Mounting options on page 12 , Install the Core Series boards in E1 enclosure on page 15 , Install the Core Series boards in E2 enclosure on page 18 , Install the Core Series boards in E4 enclosure on page 19 , Install the Core Series boards in E6 enclosure on page 20 Wiring the 12/24V 4-Door Smart Hub on page 40 , Wiring the 24V Elevator Smart Hub on page 40 , Wiring the 12/24V 8-Door Smart Hub on page 42 , Wiring the 12/24 8-Door Large Smart Hub on page 43 , Wiring the 12/24 16-Door Large Smart Hub on page 44 , Power, Relay, Status, and Board ID LEDs on page 52 Appendix: Best practices - Wiring a REX to your Avigilon Alta access control system on page 64 , FCC on page 67 , IC RSS-102 on page 70 , Electrical specifications on page 71
July 2023	Reader updates: Install the Smart Reader v2 on page 23 , Install the Smart Keypad Reader on page 25 , Install the Embedded USB Smart Reader on page 27 , Regulatory notice on page 67
June 2023	Enable Static Cloud IP field: Add one ACU on page 57 , Add ACUs using Alta Control Center on page 56
March 2023	Video Intercom Reader Pro support: For more information on page 9 , Install the Video Reader Pro on page 30 , Install the Video Intercom Reader Pro on page 35 , Avigilon Pro Series Reader LED indicator on page 55 , Reset video readers and video intercom readers on page 63 , Electrical specifications on page 71
January 2023	Menu name updates in the Openpath Alta Control Center Other updates:

Guide	Description
	<p>Embedded USB Smart Reader support: For more information on page 9, Avigilon reader wiring on page 22</p> <p>European (EU) Alta Control Center: Use the Alta Control Center on page 33, Add ACUs using Alta Control Center on page 56, Change input types in the Alta Control Center on page 48, Configure EOL in the Alta Control Center on page 50, Configure Wiegand devices in the Alta Control Center on page 49, Provisioning options on page 59</p>

Contents

- Revisions 3**
- Before you start 8**
 - Conducting site surveys 8
 - For more information 9
 - Technical support 9
 - Product documentation 9
 - Third-party documentation 9
- Installation 11**
 - Network requirements 11
 - Selecting a backup battery 11
 - Mounting options 12
 - Mount the enclosure to the wall 12
 - Install Access Control Core without mounting bracket 13
 - Install Access Control Core with mounting bracket 14
 - Install the Core Series boards in E1 enclosure 15
 - Install the Elevator Core Series boards in E1 enclosure 16
 - Install the Core Series boards in E2 enclosure 18
 - Install the Core Series boards in E4 enclosure 19
 - Install the Core Series boards in E6 enclosure 20
 - Avigilon reader wiring 22
 - Install the Smart Reader v2 23
 - Standard Reader 23
 - Mullion Reader 24
 - Install the Smart Keypad Reader 25
 - Standard Keypad Reader 25
 - Mullion Keypad Reader 26
 - Install the Embedded USB Smart Reader 27
 - Flush mount 27
 - Desktop mount for use as an enrollment reader 28
 - Wiring 28

Install the Video Reader Pro	30
Specifications	30
Prerequisites	30
Installation	30
Network security best practices	33
Install the Video Intercom Reader Pro	35
System overview	35
Specifications	35
Prerequisites	36
Installation	36
Power the Video Intercom Reader Pro	38
Provision the Video Intercom Reader Pro	38
Standard wiring	40
Wiring the 12/24V 4-Door Smart Hub	40
Wiring the 24V Elevator Smart Hub	40
Wiring the 12/24V 8-Door Smart Hub	42
Wiring the 12/24 8-Door Large Smart Hub	43
Wiring the 12/24 16-Door Large Smart Hub	44
Wiring fail-safe and fail-secure lock hardware	45
Advanced wiring	46
Wiring Wiegand readers to Avigilon readers	46
Wiring to legacy panels and mobile gateway	46
Change I/O types	48
Wire to Wiegand devices on Core Series Smart Hubs	48
End-of-line supervision	50
Provisioning	52
Prerequisites	52
Power, Relay, Status, and Board ID LEDs	52
Expansion board Status LED indicator	53
Access Control Core Status LEDs	54
Smart Reader LED indicator	54
Avigilon Pro Series Reader LED indicator	55
Add ACUs using Alta Control Center	56

Add multiple ACUs using Quick start option	56
Add one ACU	57
Disable the Static Cloud IP connection	58
Provisioning options	59
Provision the ACU using Avigilon Alta Access app (recommended)	59
Provision the ACU using Alta Control Center on a laptop	59
Test internet connection using Avigilon Alta Access app	61
Configure network settings using Avigilon Alta Access app	61
Change network settings	61
Set up Wi-Fi on the Access Control Core	61
Maintenance and troubleshooting	62
Legacy wiring	62
Resetting ACUs	62
Soft reset	62
Hard reset	62
Reset video readers and video intercom readers	63
Resolve common issues	63
Appendix: Best practices - Wiring a REX to your Avigilon Alta access control system	64
Wiring REX in series with mag lock or other fail-safe hardware	64
Wiring REX with Video Reader Pro and Video Intercom Reader Pro	64
Regulatory notice	67
UL 294	67
CAN/ULC 60839-11-1-16 GRADE 1	67
FCC	67
IEC 62368-1	68
RF Radiation Hazard Warning	68
Industry Canada Notice and Marking	69
IC RSS-102	70
Electrical specifications	71

Before you start

This installation guide explains how to install and configure Avigilon Smart Hubs (ACUs), Smart Readers (Smart Reader v2, Smart Keypad Reader, and Embedded USB Smart Reader), and Avigilon Pro series readers (Video Reader Pro and Video Intercom Reader Pro), as part of the Avigilon Alta access control system. This guide also includes information about Core Series Smart Hubs.

Conducting site surveys

Before installing Avigilon hardware, conduct a customer site survey to determine the following:

- The number of entries that need to be configured (for example, doors, gates, and elevator floors)
- The legacy wiring or new wiring to be installed
- The electronic entry mechanisms, Request to Exit (REX) mechanisms, and door contact sensors to be used and their power requirements

If your locking hardware requires 24V, either use a Smart Hub with a 24V power supply or use a separate 24V supply.

- Any backup batteries for a Smart Hub (see [Selecting a backup battery on page 11](#))
- The support of a legacy access control panel for mobile gateway (see [Wiring to legacy panels and mobile gateway on page 46](#))

For more information

Technical support

For additional support documentation, see help.openpath.com.

Product documentation

For additional product documentation, see the Avigilon Alta (Cloud Solutions) product suite on avigilon.com/product-documentation.

- [Avigilon Alta Control Center Administrator Guide](#)

Avigilon controllers, expansion boards, and Smart Hubs:

- [Avigilon Access Control Core \(OP-CR-ACC\) Datasheet](#)
- [Avigilon 4-Port and 8-Port Expansion Board \(OP-EX-4E, OP-EX-8E\) Datasheet](#)
- [Avigilon 16 I/O Elevator Board \(OP-16EM\) Datasheet](#)
- [Avigilon 12/24V 4-Door Smart Hub \(SYS-4ENT-DVE1\) Datasheet](#)
- [Avigilon 24V Elevator Smart Hub \(SYS-ELEV-SVE1\) Datasheet](#)
- [Avigilon 12/24V 8-Door Smart Hub \(SYS-8ENT-DVE2\) Datasheet](#)
- [Avigilon 12/24V 8-Door Large Smart Hub \(SYS-8ENT-DVE4\) Datasheet](#)
- [Avigilon 12/24V 16-Door Large Smart Hub \(SYS-16ENT-DVE6\) Datasheet](#)

Avigilon Smart Readers and Pro Series Readers:

- [Avigilon Standard and Mullion Smart Readers \(OP-R2X-STND, OP-R2X-MULL\) Datasheet](#)
- [Avigilon Standard and Mullion Smart Keypad Readers \(OP-RKP-STND, OP-RKP-MULL\) Datasheet](#)
- [Avigilon Embedded USB Smart Reader \(OP-R2X-EMBD\) Datasheet](#)
- [Avigilon Video Intercom Reader Pro \(OP-VID-PRO-INT\) Datasheet](#)
- [Avigilon Video Reader Pro \(OP-VID-PRO-RDR\) Datasheet](#)

Third-party documentation

For additional power supply documentation, see vendor documentation.

- [LifeSafety Power® FlexPower Vantage Standard Power System Installation Manual](#) for FPV4 and FPV6 power supplies
- [LifeSafety Power FlexPower Generation 2 DC Power System Installation Manual](#) for FP0150 and FP0250 power supplies
- [LifeSafety Power FlexPower® B100 Installation Manual](#)

- [LifeSafety Power FlexPower C4/C8 Installation Manual](#)
- [LifeSafety Power FlexPower D8/DP8 Installation Manual](#)

Installation

Network requirements

An Ethernet connection with DHCP must be used to connect the ACU to the Local Area Network (LAN). You may also need to configure firewall settings to communicate with the Avigilon Alta access control system, which uses the following outbound ports:

- TCP port 443
- UDP port 123

Note: If using an external DNS server, the outbound UDP port 53 must also be open.

To support Wi-Fi unlocking from the Avigilon Alta Open app, the inbound TCP port 443 of the ACU must be available from within the LAN. Inbound port forwarding on the router, firewall, or NAT device is not required.

The ACU also supports Wi-Fi connections. See [Configure network settings using Avigilon Alta Access app on page 61](#).

Selecting a backup battery

While not required, a backup battery is recommended in case of power outages. 12V supplies require one 12V backup battery. 24V supplies require two 12V batteries in series. The size of battery depends on your setup and how long you want to power the system.

Table 1 Example power requirements for Core Series Smart Hubs (24V)

Access Control Core	0.4A
4-Port Board	0.3A
Standard Smart Reader	0.14A
Mullion Smart Reader	
Embedded USB Smart Reader	
Locking hardware (while engaged)	0.12A – 0.25A

Assuming a 24V power supply, a Core Series Smart Hub configured with four Avigilon readers and locking hardware uses about 2 Amps. To keep the system running for 3 hours with all entries engaged, you need $2A \times 3 \text{ hours} = 6AH$, so two 12V 6AH sealed lead acid (SLA) or gel cell batteries wired in series.

Mounting options

Avigilon Smart Hubs use LifeSafety Power E1, E2, E3, E4, and E6 enclosures. Core Series Smart Hubs are shipped with power supplies pre-installed, but Avigilon boards must be installed separately.

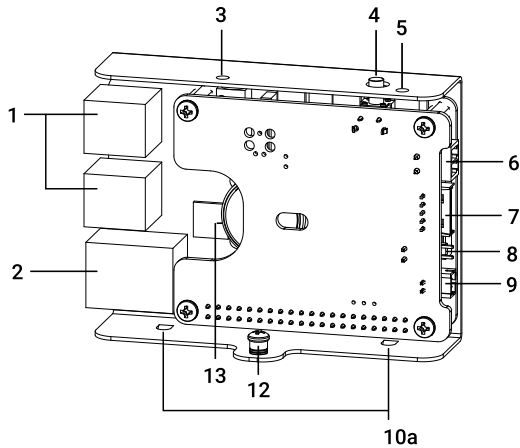
Mount the enclosure to the wall

1. (Optional) Remove the enclosure cover.
2. Locate the top keyhole mounting holes in the back of the enclosure.
3. Mark and pre-drill the locations for the keyholes in the mounting surface.
4. Partially install two fasteners appropriate for the surface on which the enclosure is being installed. Leave the heads of the fasteners approximately $\frac{1}{4}$ " out from the surface. Minimum fastener size should be #10 or larger.
5. Hang the enclosure on the two fasteners and mark the locations of the remaining mounting holes.
6. Remove the enclosure and pre-drill the locations for the remaining mounting holes.
7. Re-hang the enclosure on the top mounting fasteners, install the remaining fasteners, and tighten all fasteners.
8. Reinstall the enclosure's cover, if removed in step 1.

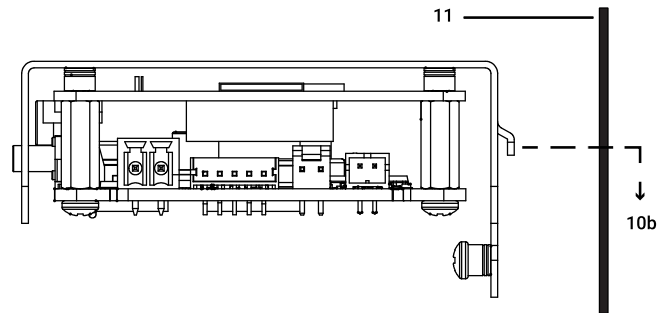
Install Access Control Core without mounting bracket

The mounting bracket is optional when installing the Access Control Core in the E1 enclosure of the 12/24V 4-Door Smart Hub or 24V Elevator Smart Hub, or the E2 enclosure of the 12/24V 8-Door Smart Hub.

Front view



Side view with enclosure



1	USB ports	8	Tamper input
2	Ethernet connector	9	LED out
3	Status LED	10a	Core board hooks
4	ADMIN button	10b	Core board installed facing down, up, left, or right, depending on the enclosure model
5	Power LED	11	Back of enclosure
6	Power input	12	Mounting screw
7	SPI Bus Link connector	13	Backup battery, CR2032

Mounting

1. Mount the Access Control Core perpendicular to the back of the enclosure, by hooking tabs into the holes in the back of the enclosure.
2. Slide the Access Control Core into the enclosure (see 10a, 10b, 11). Then gently tighten the mounting screw (12). Do not overtighten.

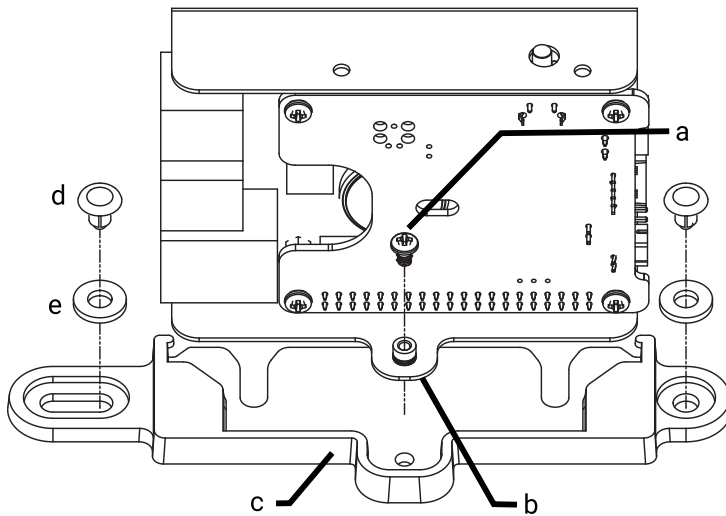
Wiring

1. Attach power connector (12/24VDC; see 6) to the input.
2. Connect the Ethernet cable (Internet connection required; see 2) prior to provisioning.

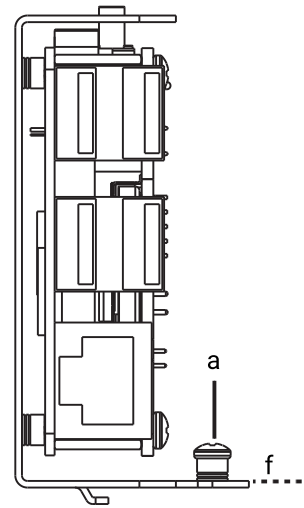
Install Access Control Core with mounting bracket

The Access Control Core must be installed with the mounting bracket in the E4 enclosure of the 12/24 8-Door Large Smart Hub or in the E6 enclosure of the 12/24 16-Door Large Smart Hub. The mounting bracket is optional in the E1 and E2 enclosures. The Access Control Core (OP-CR-ACC) must be installed with the mounting bracket in the E4 enclosure of the 12/24 8-Door Large Smart Hub or in the E6 enclosure of the 12/24 16-Door Large Smart Hub. The mounting bracket is optional in the E1 and E2 enclosures.

View with mounting bracket



Side view



To assemble the Access Control Core and mounting plate:

1. Loosen the screw (a) and ensure it is not protruding past the bottom (f).
2. Slide the Access Control Core (b) into the mounting plate (c) and secure the screw.
3. Mount the assembly into the holes of the backplate with the provided push-in rivets (d).
4. Only use washers (e) in the E1 and E2 enclosures. Washers are not needed for the backplate in the E4 and E6 enclosures.

Install the Core Series boards in E1 enclosure

The E1 board placement includes the 24V FPV4 supply, B100 secondary supply, C4 Relay Based Lock Control Module, 4-Port Board, and Access Control Core with or without the mounting bracket.

Front view

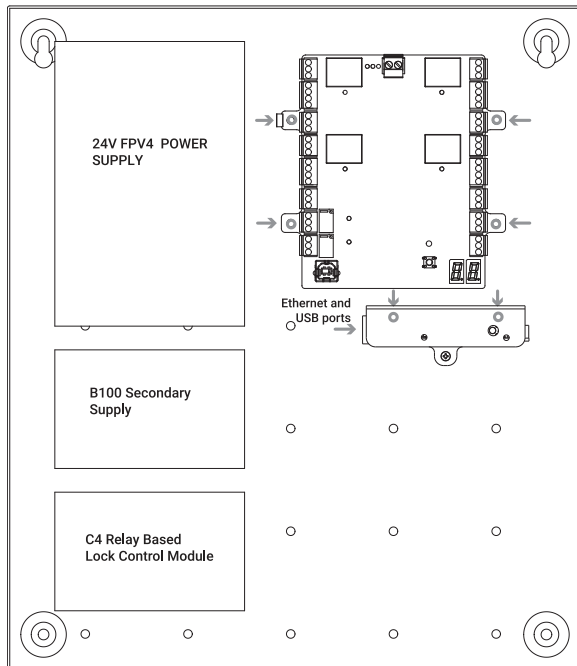


Figure 1 Access Control Core mounted without bracket (Ethernet and USB ports facing left) below 4-Port Board

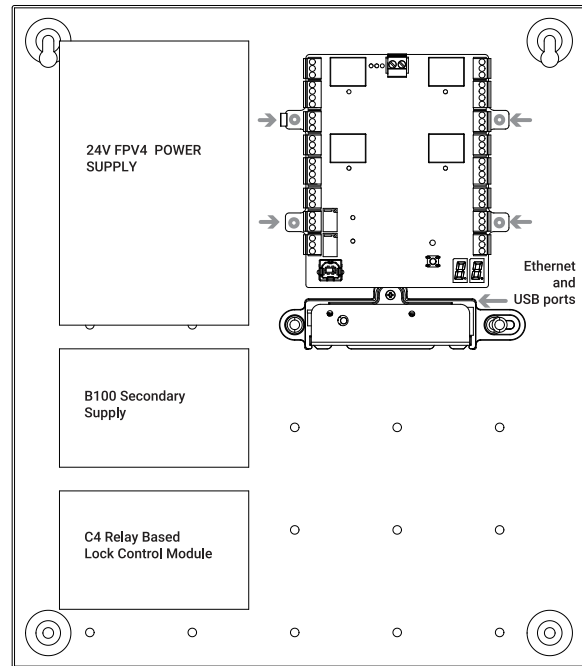


Figure 2 Access Control Core mounted with bracket (Ethernet and USB ports facing right) below 4-Port Board

Mounting

1. Mount the 4-Port Board to the right of the LifeSafety Power supply modules by snapping the board standoffs into the enclosure (see arrows).
2. If mounting the Access Control Core without the bracket, see [Install Access Control Core without mounting bracket on page 13](#). Ensure the Ethernet and USB ports face left.

If mounting the Access Control Core with the bracket, see [Install Access Control Core with mounting bracket on the previous page](#). Ensure the Ethernet and USB ports face right.

3. Connect the Access Control Core to the 4-Port Board with the included USB cable.

Note: The maximum recommended USB cable length is 6 feet (2 meters) or 10 feet (3 meters) if high quality, shielded cable.

Install the Elevator Core Series boards in E1 enclosure

The E1 board placement includes the 24V FPV4 supply, 16 I/O Elevator Board, and Access Control Core with or without the mounting bracket.

Front view

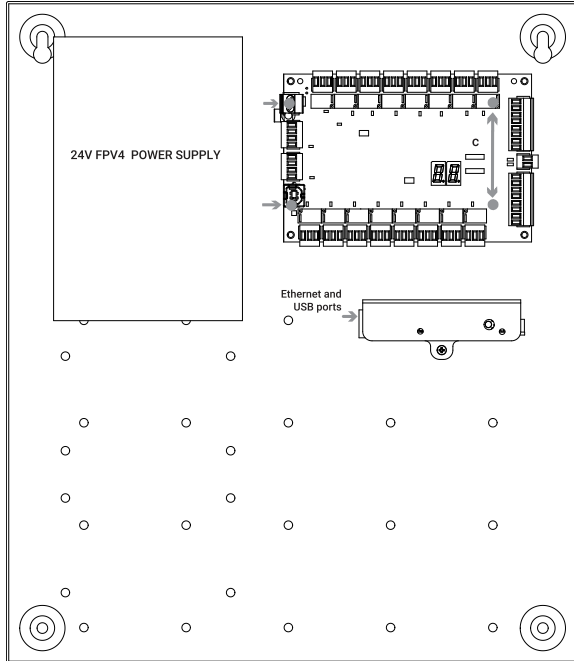


Figure 3 Access Control Core mounted without bracket (Ethernet and USB ports facing left) below 16 I/O Elevator Board

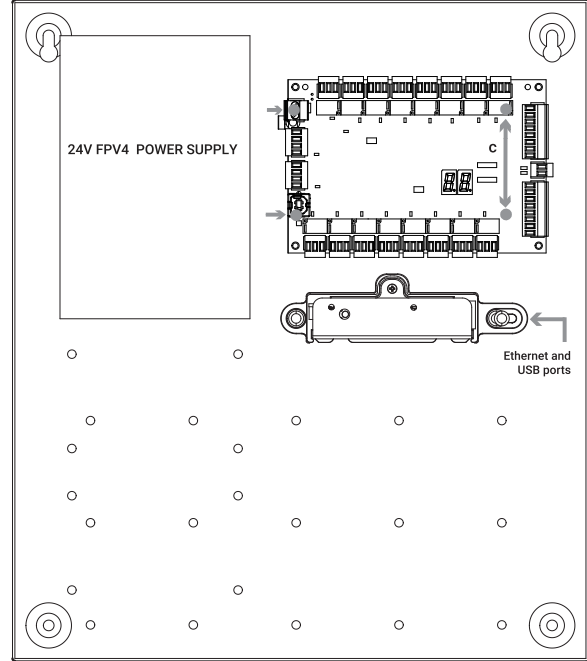
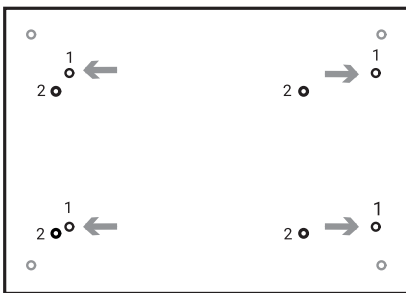


Figure 4 Access Control Core mounted with bracket (Ethernet and USB ports facing right) below 16 I/O Elevator Board


Mounting

1. Screw the four included metal standoffs into the appropriate set of holes labeled '1' on the back of the 16 I/O Elevator Board mounting plate (see below).



2. Insert the included 6-32 x 3/8" screws from the back of the enclosure, and screw into the standoffs (see arrows) to secure the 16 I/O Elevator Board assembly in place with the USB connector facing left.

3. If mounting the Access Control Core without the bracket, see [Install Access Control Core without mounting bracket on page 13](#). Ensure the Ethernet and USB ports face left.
If mounting the Access Control Core with the bracket, see [Install Access Control Core with mounting bracket on page 14](#). Ensure the Ethernet and USB ports face right.
4. Connect the Access Control Core to the 16 I/O Elevator Board with the included USB cable.

 **Note:** The maximum recommended USB cable length is 6 feet (2 meters) or 10 feet (3 meters) if high quality, shielded cable.

Install the Core Series boards in E2 enclosure

The E2 board placement includes the 24V FPV6 power supply, B100 secondary supply, C8 Relay Based Lock Control Module, 8-Port Board, and Access Control Core with or without the mounting bracket.

Front view

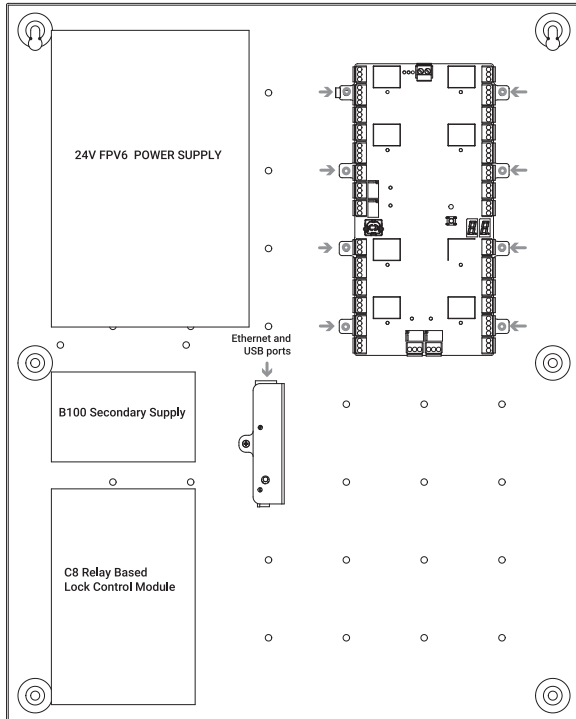


Figure 5 Access Control Core mounted without bracket (Ethernet and USB ports facing up) below 8-Port Board

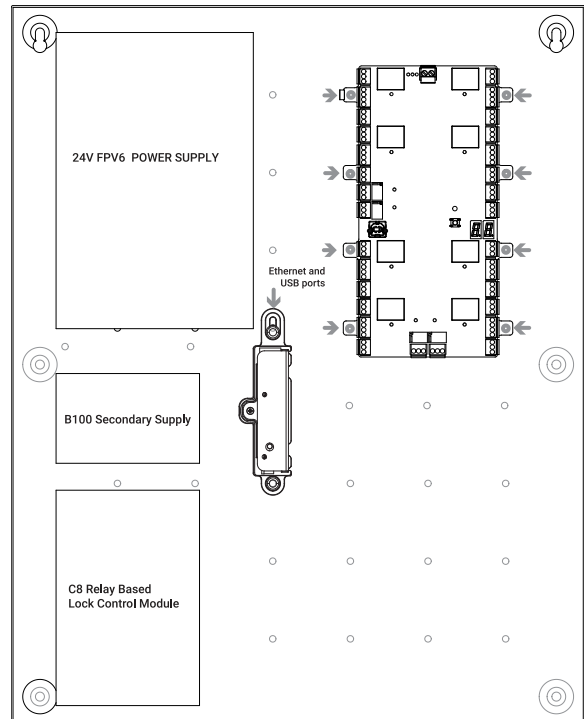


Figure 6 Access Control Core mounted with bracket (Ethernet and USB ports facing up) below 8-Port Board

Mounting

1. Mount the 8-Port Board in the upper-right corner of the enclosure by snapping the board standoffs into the holes in the backplate (see arrows).
2. If mounting the Access Control Core without the bracket, see [Install Access Control Core without mounting bracket on page 13](#). Ensure the Ethernet and USB ports face up.

If mounting the Access Control Core with the bracket, see [Install Access Control Core with mounting bracket on page 14](#). Ensure the Ethernet and USB ports face up.

3. Connect the Access Control Core to the 8-Port Board with the included USB cable.

Note: The maximum recommended USB cable length is 6 feet (2 meters) or 10 feet (3 meters) if high quality, shielded cable.

Install the Core Series boards in E4 enclosure

The E4 board placement includes the 24V FP0150 power supply, B100 secondary supply, D8P Power Distribution Module, C8 Relay Based Lock Control Module, 8-Port Board, and Access Control Core with the mounting bracket.

Front view

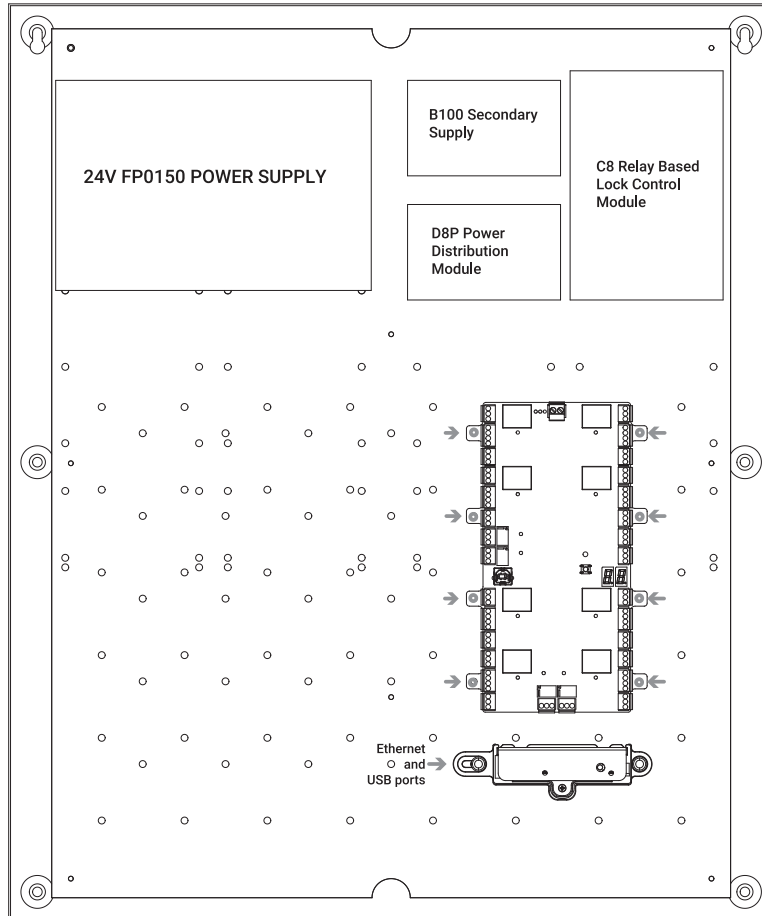


Figure 7 Access Control Core mounted with bracket (Ethernet and USB ports facing left) below the 8-Port Board

Mounting

1. Mount the 8-Port Board below the power supply modules by snapping the board standoffs into the holes in the backplate (see arrows).
2. Mount the Access Control Core with the bracket. Ensure the Ethernet and USB ports face left. For more information, see [Install Access Control Core with mounting bracket on page 14](#).
3. Connect the Access Control Core to the 8-Port Board with the included USB cable.

Note: The maximum recommended USB cable length is 6 feet (2 meters) or 10 feet (3 meters) if high quality, shielded cable.

Install the Core Series boards in E6 enclosure

The E6 board placement includes the 24V FP0150 and FP250 power supplies, D8P Power Distribution Modules, C8 Relay Based Lock Control Modules, 8-Port Boards, and Access Control Core with the mounting bracket.

Front view

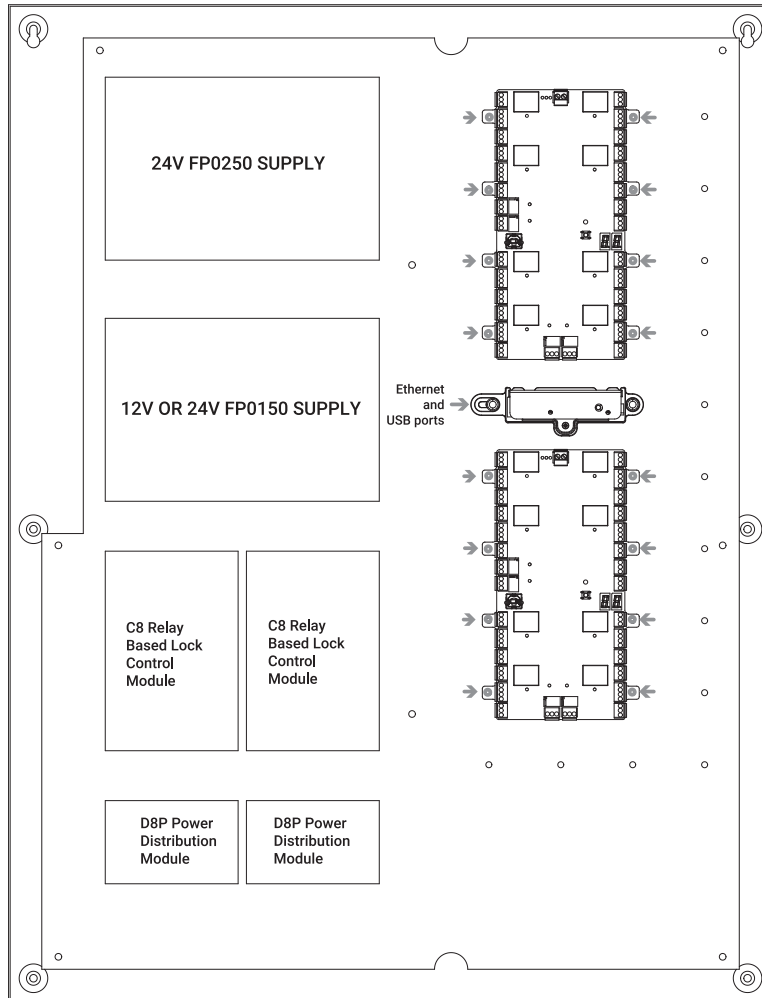



Figure 8 Access Control Core mounted with bracket between the 8-Port Boards (Ethernet and USB ports facing left)

Mounting

1. Mount the 8-Port Boards to the right of the power supply modules by snapping the board standoffs into the holes in the backplate (see arrows).
2. Mount the Access Control Core with the bracket. Ensure the Ethernet and USB ports face left. For more information, see [Install Access Control Core with mounting bracket on page 14](#).


3. Connect the Access Control Core to the 8-Port Boards with the included USB cables.

 **Note:** The maximum recommended USB cable length is 6 feet (2 meters) or 10 feet (3 meters) if high quality, shielded cable.

Avigilon reader wiring

Avigilon readers and ACUs communicate via RS-485. The compatible wire types are listed in order of preference which impacts distance.

- Shielded CAT6A (recommended; additional two pairs can be used for sensors)
- Shielded Cat 6
- Shielded RS-485 with 18-24 AWG (lower gauge, thicker wire is better)
- Shielded Cat 5
- Unshielded Cat 6
- Unshielded Cat 5
- Shielded 22/6
- Unshielded 22/6

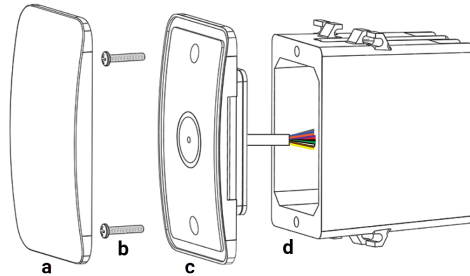
 **Note:** Use one twisted pair for GND and VIN (power) and one twisted pair for +B and -A (data).

Install the Smart Reader v2

Standard Reader

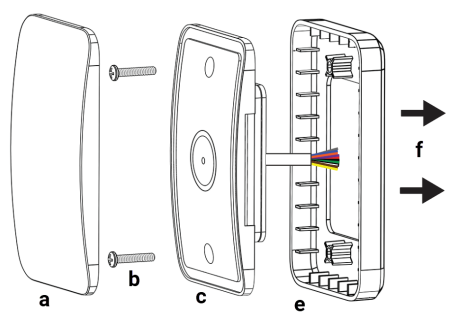
The Smart Reader v2 (OP-R2X-STND) can be flush mounted in a single gang box or surface mounted using the provided bracket.

Flush mount (recommended)



1. Install a recessed single gang box (d) into the wall.
2. Strip and connect the wires.
3. Use the provided screws (b) to attach the reader (c) to the gang box. Do not use the provided surface mount bracket for flush mount installations.
4. Snap on the front cover (a).


Surface mount



Note: The flat side of the surface mount bracket must face the wall. No adhesives are necessary.

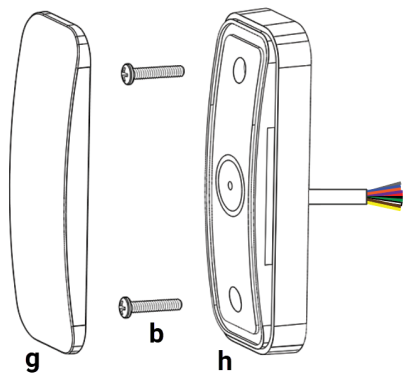
1. Place the reader (c) inside the surface mount bracket (e).
2. Strip and connect the wires.
3. Use wall anchors and the appropriate screws (not included) to attach the reader (c and e) to the wall.

4. Snap on the front cover (a).

 **Note:** Do not use adhesive.


Mullion Reader

The Mullion Smart Reader (OP-R2X-MULL) can be surface mounted where space is limited.



Surface mount

1. Strip and connect the wires.
2. If installing on a metal surface, drill and tap to use the provided #6-32 screws (b). Or, use self-tapping screws (not included). Attach the reader (g) to the wall (f).
3. Snap on the front cover (g).

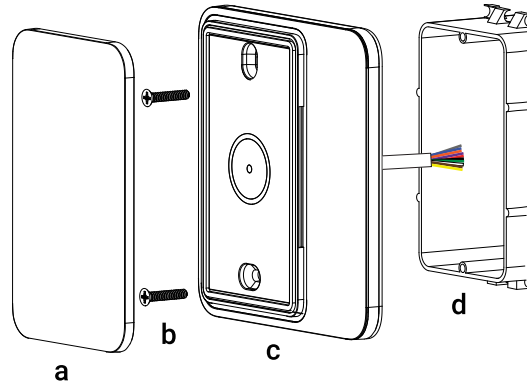
 **Note:** Do not use adhesive.

Install the Smart Keypad Reader


Standard Keypad Reader

The Smart Keypad Reader (OP-RKP-STND) can be flush mounted in a single gang box or surface mounted using the provided surface mount bracket.

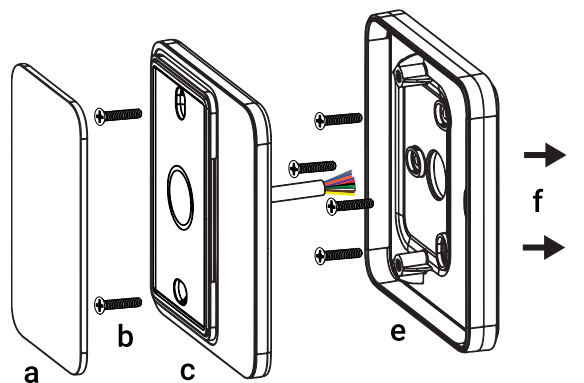
Flush mount



1. Install a recessed single gang box (d) into the wall.
2. Strip and connect the wires.
3. Use the provided screws (b) to attach the reader (c) to the wall. Do not use the provided surface mount bracket for flush mount installations.
4. Snap on the front cover (a).

 **Note:** Do not use adhesive.


Surface mount



1. Attach the surface mount bracket (e) to the wall (f) using one of these options:

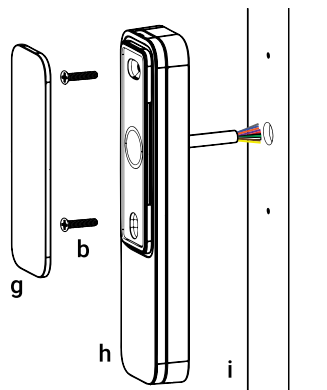
Drywall: Use wall anchors and suitable screws. **UK single gang box:** Use four machine screws (not incl). **EU single gang box:** Use two machine screws (not included) in the top and bottom holes.

2. Strip and connect the wires.
3. Use the provided #8-32 screws (b) to attach the reader (c) to the surface mount bracket (e).
4. Snap on the front cover (a).


 **Note:** Do not use adhesive.

Mullion Keypad Reader

The Mullion Smart Reader (OP-RKP-MULL) can be surface mounted where space is limited.

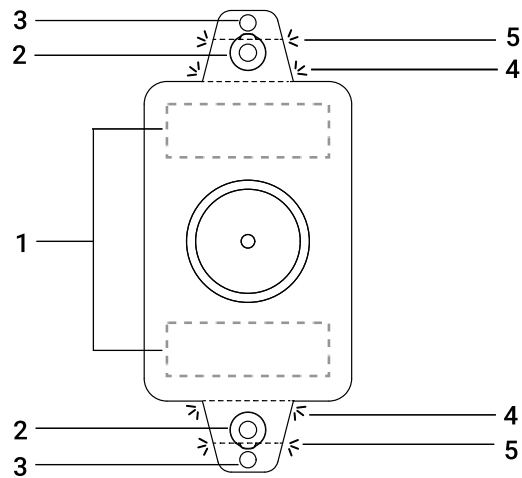


1. Strip and connect the wires.
2. If installing on a metal surface, drill and tap to use the provided #6-32 screws (b). Or, use self-tapping screws. Attach the reader (h) to the wall (i).
3. Snap on the front cover (g).


 **Note:** Do not use adhesive.

Install the Embedded USB Smart Reader

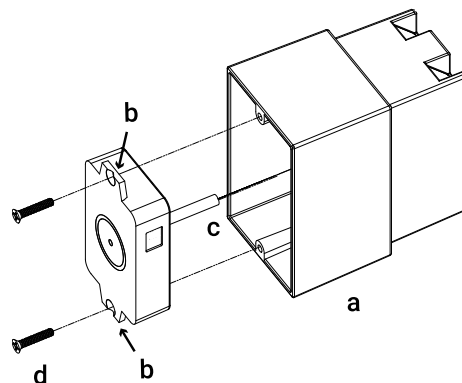
The Embedded Reader (OP-R2X-EMBD) can be flush mounted in a US gang box; installed within kiosks, turnstiles, parking systems, or other enclosures using the mounting holes; or mounted behind panels using adhesive.



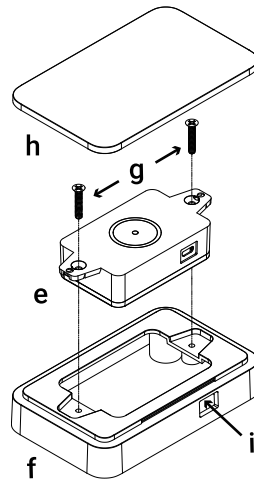
-
- 1 Recommended mounting strip location
 - 2 Mounting holes for single gang box
 - 3 Outer mounting holes
 - 4 Inner breakaway tabs for mounting using adhesive
 - 5 Outer breakaway tabs for US gang box installation
-

 **Note:** Remove tabs carefully using pliers.

Flush mount



Desktop mount for use as an enrollment reader



1. Install the reader (e) within the desktop mount bracket (f) (sold separately) with the provided screws (g).
2. Snap on the front cover (h).
3. Connect the reader to the host using the USB cable (i) provided with the desktop mount bracket.

Connector type: USB 2.0 Micro B

Wiring

Avigilon readers and ACUs communicate via RS-485. The compatible wire types are listed in order of preference which impacts distance.

- Shielded CAT6A (recommended; additional two pairs can be used for sensors)
- Shielded Cat 6
- Shielded RS-485 with 18-24 AWG (lower gauge, thicker wire is better)
- Shielded Cat 5
- Unshielded Cat 6
- Unshielded Cat 5
- Shielded 22/6
- Unshielded 22/6

Note: Use one twisted pair for GND and VIN (power) and one twisted pair for +B and -A (data).

Connector type	Description
USB 2.0 Micro B	Connect to host over USB for keyboard emulation

Table 2 Connections from Avigilon ACU to Avigilon Embedded reader

Short name	Full name
GND	Ground (RTN)
+B	RS485-B
-A	RS485-A
VIN	+12V IN

Table 3 Connections to third-party Wiegand reader (optional)

Short name	Full name
VO	Wiegand Voltage
GND	Wiegand RTN
WD0	Wiegand Data 0
WD1	Wiegand Data 1
LED	Wiegand LED
BUZZER	Wiegand Buzzer

Temperature must not exceed -22°F to 140°F (-30°C to 60°C).

Install the Video Reader Pro

The Video Reader Pro combines a built-in high-resolution camera with the form factor of a mullion door reader. The video readers are powered using PoE and do not need to be wired back to an Avigilon ACU. However, you must use an ACU or third-party panel to support locking hardware.

Specifications

For the Video Reader Pro specifications and dimensions, see the [OP-VID-PRO-RDR datasheet](#).

Prerequisites

Create the video reader in the Alta Control Center prior to installing and provisioning. For more information, see the Avigilon Alta Control Center Administrator Guide. See also [Network security best practices on page 33](#).


To install the Mobile Gateway option, see the [Installation article](#).

Installation

You can install the Video Reader Pro on a narrow surface using the mullion mount or on a single gang box using the standard mount.

Install the Video Reader Pro on the mullion mount

1. Use the provided machine screws (a) in threaded holes, or the wall mount screws and anchors (not shown) for drywall, to attach the mullion mounting plate (b) to the wall.
2. Place the cradle bracket (c) on the mounting plate, angled as desired, and secure with the provided screws (d).
3. Wire and provision the device. See the provisioning reader topic on the next pages.
4. Snap in the reader (e), and secure with the security set screw (f).

 **Note:** Do not use adhesive.

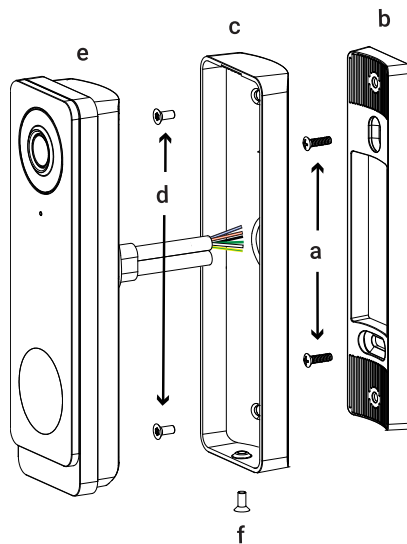


Figure 9 Installing the Video Reader Pro on the mullion mount

Install the Video Reader Pro on the standard mount

1. Install a recessed single gang box into the wall.
2. Use the provided machine screws (a) to attach the standard mounting plate (b) to the wall.
3. Place the cradle bracket (c) on the mounting plate, angle as desired, and secure with the provided screws (d).
4. Strip and connect the wires, and provision the device.
5. Snap in the reader (e) and secure with the security set screw.

Note: Do not use adhesive.

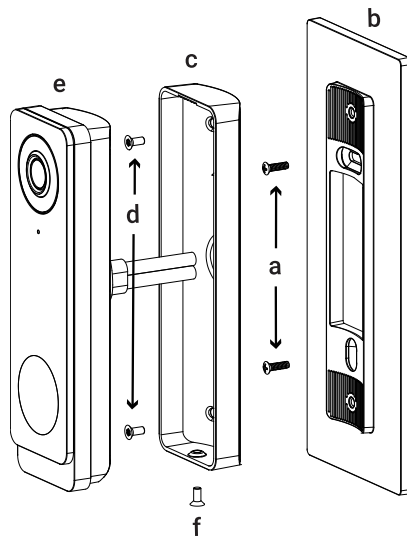


Figure 10 Installing the Video Reader Pro on the standard mount

Video Reader Pro wiring

Table 4 Connection to Avigilon cloud

Connector type	Description
Ethernet	RJ-45 connector

Table 5 Connections to third-party controller (optional)

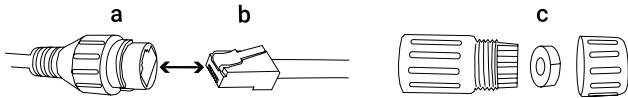
Pigtail color	Short name	Full name
Black	GND	Wiegand RTN
Green	WD0	Wiegand Data 0
White	WD1	Wiegand Data 1

Table 6 Connections to third-party device (optional)

Pigtail color	Short name	Full name
Blue and white stripe	NO	Relay Normally Open*
Orange and white stripe	COM	Relay Common*
Green and yellow stripe	GND	Ground (RTN)*

*Relay is not rated for locking hardware. To power locking hardware, use an Avigilon Smart Hub or third-party access control panel.

1. Use the provided waterproof coupling (c) to connect the RJ-45 jack (a) to an Ethernet cable (Cat 5e, 26 AWG or better), which is connected to a networked Power over Ethernet (PoE) source (b).



2. Optional. Use the NO and COM stripe wires to connect to a third-party device. Use the WD0 and WD1 wires to connect to an input on the panel of a legacy access control system.

Power up the Video Reader Pro


1. Connect the Video Reader Pro to a PoE injector or PoE-powered switch.
2. Power on the Video Reader Pro.

Provision the Video Reader Pro

You must first create a Video Reader Pro in the Alta Control Center before provisioning.


Use the Avigilon Alta Access app

1. Open the Avigilon Alta Access app.
2. Search for org name.
3. Press Admin button (see figure on the next pages) on the back of reader.

 **Note:** Remove the back cradle to expose the Admin button.

4. Tap the serial number of the reader in the Avigilon Alta Access app.
5. Tap **Provision Device** in the Avigilon Alta Access app and follow in-app instructions.

Use the Alta Control Center

1. Go to control.openpath.com/login and sign in. To access the European Alta Control Center, go to control.eu.openpath.com/login.
2. Go to  **Devices > Video readers**.
3. Press Admin button (see figure below) on back of Video Reader Pro.
4. In the Alta Control Center, click the Register button.

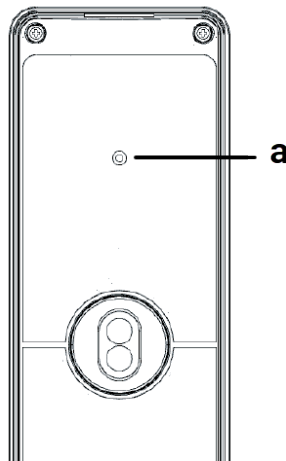


Figure 11 Admin button (a) on the back of Video Reader Pro

For next steps, return to the Alta Control Center to view the activated device.

Network security best practices

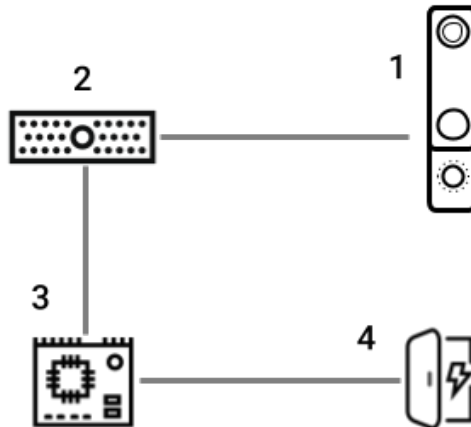
PoE access control readers, such as the Video Reader Pro and Video Intercom Reader Pro, require a wired network connection installed on the unsecured side of a door.

Important: To remove the risk of an attacker gaining access to the local network via the network connection, assuming they can remove the reader from the wall, Avigilon Alta recommends that your IT team place the exposed Ethernet port on a demilitarized zone (DMZ) or perimeter network.

Install the Video Intercom Reader Pro

The Video Intercom Reader Pro combines a built-in high-resolution camera, intercom with intelligent voice interface, and multi-technology reader into a sleek form factor.

System overview



No.	Description
1	Video Intercom Reader Pro is powered using PoE and does not need to be wired to an Avigilon ACU. However, you must use an ACU or third-party panel to support locking hardware. The device must be connected to the same local network as the ACU, control panel, or door controller that controls it.
2	PoE-powered network switch or Avigilon PoE injector
3	Avigilon ACU, legacy panel, or door controller that unlocks the door
4	Door strike

For the Gateway Mode wiring setup (not shown in the diagram), see "Appendix A: Configuring Avigilon Alta Control Center with Legacy Systems" in the Avigilon Alta Control Center Administrator Guide.

Specifications

For the Video Intercom Reader Pro specifications and dimensions, see the [OP-VID-PRO-INT datasheet](#).

Note: Higher network bandwidth is recommended for the best performance in video and audio streaming.

Prerequisites

Create the Video Intercom Reader Pro in the Alta Control Center before installing and provisioning. For more information, see the Avigilon Alta Control Center Administrator Guide. See also [Network security best practices on page 33](#). To install the Mobile Gateway option, see the [Installation article](#).

Note: You get 5 free Video Intercom Reader Pro user licenses per organization.

Installation

You can install the Video Intercom Reader Pro on a narrow surface using the mullion mount or on a single gang box using the standard mount.

Install the Video Intercom Reader Pro on the mullion mount

1. Use the provided machine screws (a) in threaded holes, or the wall mount screws and anchors (not shown) for drywall, to attach the mullion mounting plate (b) to the wall.
2. Place the cradle bracket (c) on the mounting plate, angled as desired, and secure with the provided screws (d).
3. Wire and provision the device. See the provisioning reader topic on the next pages.
4. Snap in the reader (e), and secure with the security set screw (f).

Note: Do not use adhesive.

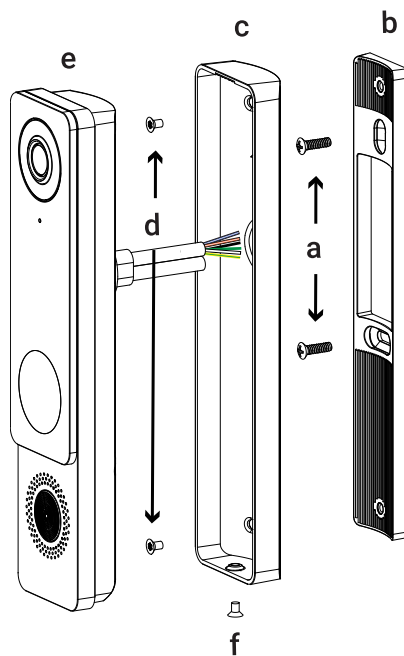


Figure 12 Installing the Video Intercom Reader Pro on the mullion mount

Install the Video Intercom Reader Pro on the standard mount

1. Install a recessed single gang box into the wall.
2. Use the provided machine screws (a) to attach the standard mounting plate (b) to the wall.
3. Place the cradle bracket (c) on the mounting plate, angle as desired, and secure with the provided screws (d).
4. Strip and connect the wires, and provision the device.
5. Snap in the reader (e) and secure with the security set screw.

Note: Do not use adhesive.

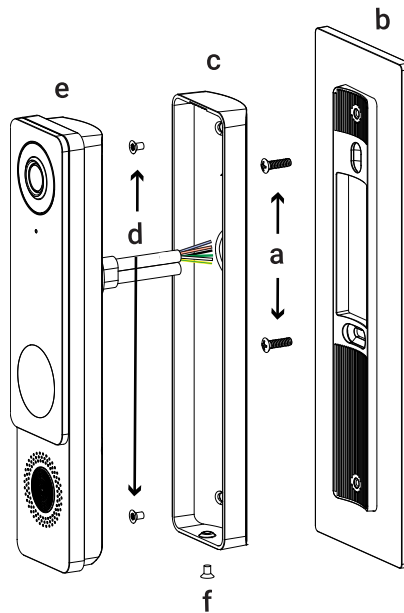


Figure 13 Installing the Video Intercom Reader Pro on the standard mount

Wiring the Video Intercom Reader Pro

Table 7 Connection to Avigilon cloud

Connector type	Description
Ethernet	RJ-45 connector

Table 8 Connections to third-party controller (optional)

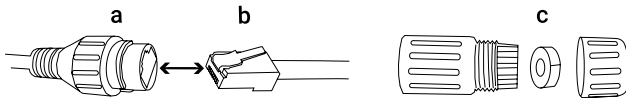
Pigtail color	Short name	Full name
Black	GND	Wiegand RTN
Green	WD0	Wiegand Data 0
White	WD1	Wiegand Data 1

Table 9 Connections to third-party device (optional)

Pigtail color	Short name	Full name
Blue and white stripe	NO	Relay Normally Open*
Orange and white stripe	COM	Relay Common*
Green and yellow stripe	GND	Ground (RTN)*

*Relay is not rated for locking hardware. To power locking hardware, use an Avigilon Smart Hub or third-party access control panel.

1. Use the provided waterproof coupling (c) to connect the RJ-45 jack (a) to an Ethernet cable (Cat 5e, 26 AWG or better), which is connected to a networked Power over Ethernet (PoE) source (b).



2. Optional. Use the NO and COM stripe wires to connect to a third-party device. Use the WD0 and WD1 wires to connect to an input on the panel of a legacy access control system.

Power the Video Intercom Reader Pro

1. Connect the Video Intercom Reader Pro to a PoE injector or PoE-powered switch.
2. Power on the Video Intercom Reader Pro.

Provision the Video Intercom Reader Pro

You must first create a Video Intercom Reader Pro in the Alta Control Center.

For more information, see *Add a Video Intercom Reader Pro* in the Avigilon Alta Control Center Administrator Guide.

Use the Avigilon Alta Access app


1. Open the Avigilon Alta Access app.
2. Search for org name.
3. Press Admin button (see figure on the next pages) on the back of reader.

 **Note:** Remove the back cradle to expose the Admin button.

4. Tap the serial number of the reader in the Avigilon Alta Access app.
5. Tap **Provision Device** in the Avigilon Alta Access app and follow in-app instructions.

Use the Alta Control Center

1. Go to control.openpath.com/login and sign in. To access the European Alta Control Center, go to control.eu.openpath.com/login.

2. Go to  **Devices** > **Video intercom readers**.
3. Press Admin button (see figure below) on back of Video Reader Pro.
4. In the Alta Control Center, click the Register button.

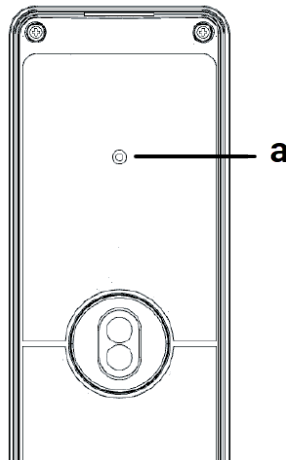


Figure 14 Admin button (a) on the back of Video Reader Pro

For next steps, return to the Alta Control Center to view the activated device.

Standard wiring

Wiring the 12/24V 4-Door Smart Hub

The 12/24V 4-Door Smart Hub (SYS-4ENT-DVE1) uses the [LifeSafety Power FPV4](#) to power the Access Control Core and 4-Port Board; a [LifeSafety Power B100](#) secondary power supply; and the [LifeSafety Power C4 Relay Based Lock Control Module](#) to power 12-24V locking hardware.

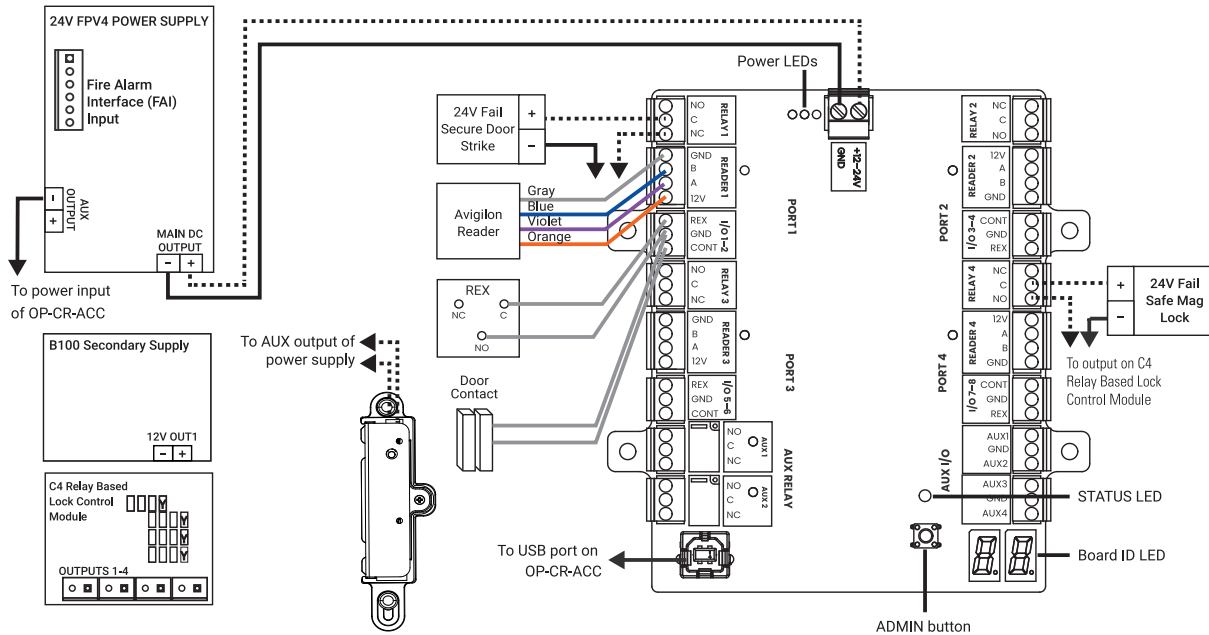


Figure 15 SYS-4ENT-DVE1 wiring diagram

24V FPV4

The main output can be switched by the Fire Alarm Interface (FAI).

Power Supply

Fail safe and fail secure are ways of configuring lock hardware:

- Fail-safe hardware *unlocks* when power is interrupted or lost.
- Fail-secure hardware *locks* when power is interrupted or lost.

For information about wiring third-party lock hardware, refer to vendor documentation.

Note: Ensure that locking hardware is connected to the required voltage by setting the jumpers on the C4 Power Control Module.

*OUTPUTS 1–4

The voltage of each C4 output can be selected individually as 12V or 24V using the yellow jumper corresponding to the output: position 1 on the jumper pins is 24V (this is the default setting) and position 2 is 12V.

Wiring the 24V Elevator Smart Hub

The 24V Elevator Smart Hub (SYS-ELEV-SVE1) uses the [LifeSafety Power FPV4](#) to power the Access Control Core, and 16 I/O Elevator Board.

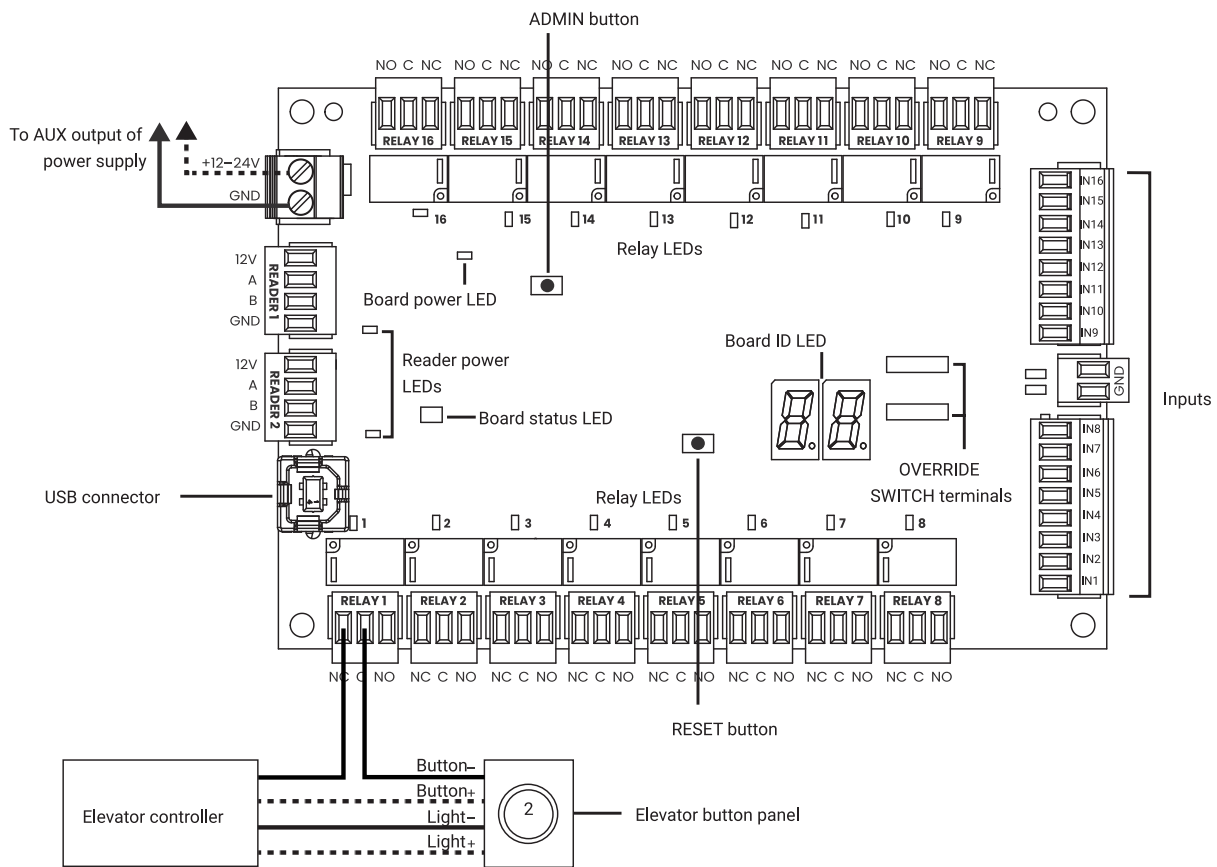


Figure 16 SYS-ELEV-SVE1 wiring diagram

USB connector	Connects to the Access Control Core board.
Relays 1–16	Output ratings: 16 relays, 60VDC maximum; 1A @ 24VDC (resistive); 0.5A @ 125VAC (resistive). The pin order is the same on both sides of the board, left to right (for example, NC, C, NO), which allows connectors to be moved without rewiring.
Inputs 1–16	General-purpose inputs require a voltage between 3V and 24V.

1. For 12V or 24V systems, connect the 16 I/O Elevator Board to an unswitched output from the main power supply (AUX output on the FPV4).
2. Use the provided USB cable to connect the 16 I/O Elevator Board to the USB connector on the Access Control Core board.
3. For elevator button wiring, interrupt one of the signal wires from each elevator floor button. Run through the C and NC contacts for the corresponding relay on the board.
4. For general-purpose input wiring, general-purpose inputs respond to voltages between 3V and 24V. The inputs will not respond directly to a switch or relay connection to ground. To use these inputs with a switch or relay, connect one side of the switch to the input and the other side of the switch to a supply voltage between 3V and 24V. Optional: Add a 1kΩ ohm resistor in series with the switch.

Wiring the 12/24V 8-Door Smart Hub

The 12/24V 8-Door Smart Hub (SYS-8ENT-DVE2) uses the [LifeSafety Power FPV6](#) to power the Access Control Core and 8-Port Board; a [LifeSafety Power B100](#) secondary power supply; and the [LifeSafety Power C8 Relay Based Lock Control Module](#) to power 12V and 24V locking hardware.

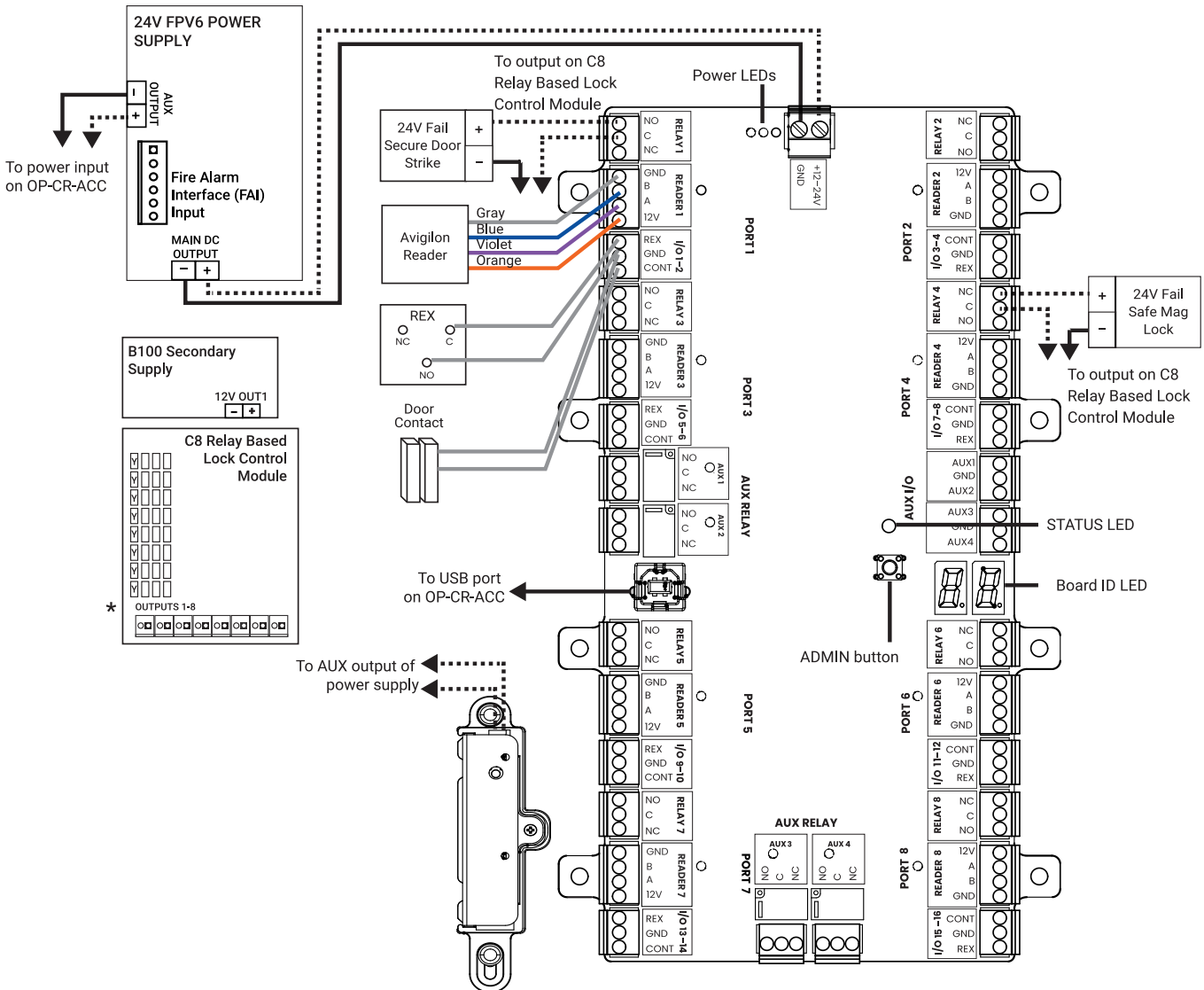


Figure 17 SYS-8ENT-DVE2 wiring diagram

24V FPV6 Power Supply

The main output can be switched by the Fire Alarm Interface (FAI).

Fail safe and fail secure are ways of configuring lock hardware:

- Fail-safe hardware *unlocks* when power is interrupted or lost.
- Fail-secure hardware *locks* when power is interrupted or lost.

For information about wiring third-party lock hardware, refer to vendor documentation.

Note: If locking hardware uses 12V, use the C8 Relay Based Lock Control Module. Ensure that appropriate jumpers are set to 12V.

***OUTPUTS 1-8** The voltage of each C8 output can be selected individually as 12V or 24V using the yellow jumper corresponding to the output: position 1 on the jumper pins is 24V (this is the default setting) and position 2 is 12V.

Wiring the 12/24 8-Door Large Smart Hub

The 12/24 8-Door Large Smart Hub (SYS-8ENT-DVE4) uses the [LifeSafety Power FP0150](#) to power the Access Control Core and 8-Port Board; a [LifeSafety Power B100](#) secondary power supply; the [LifeSafety Power C8 Relay Based Lock Control Module](#) to power 12-24V locking hardware; and the [LifeSafety Power D8P Power Distribution Module](#) to power 12V and 24V locking hardware and accessories.

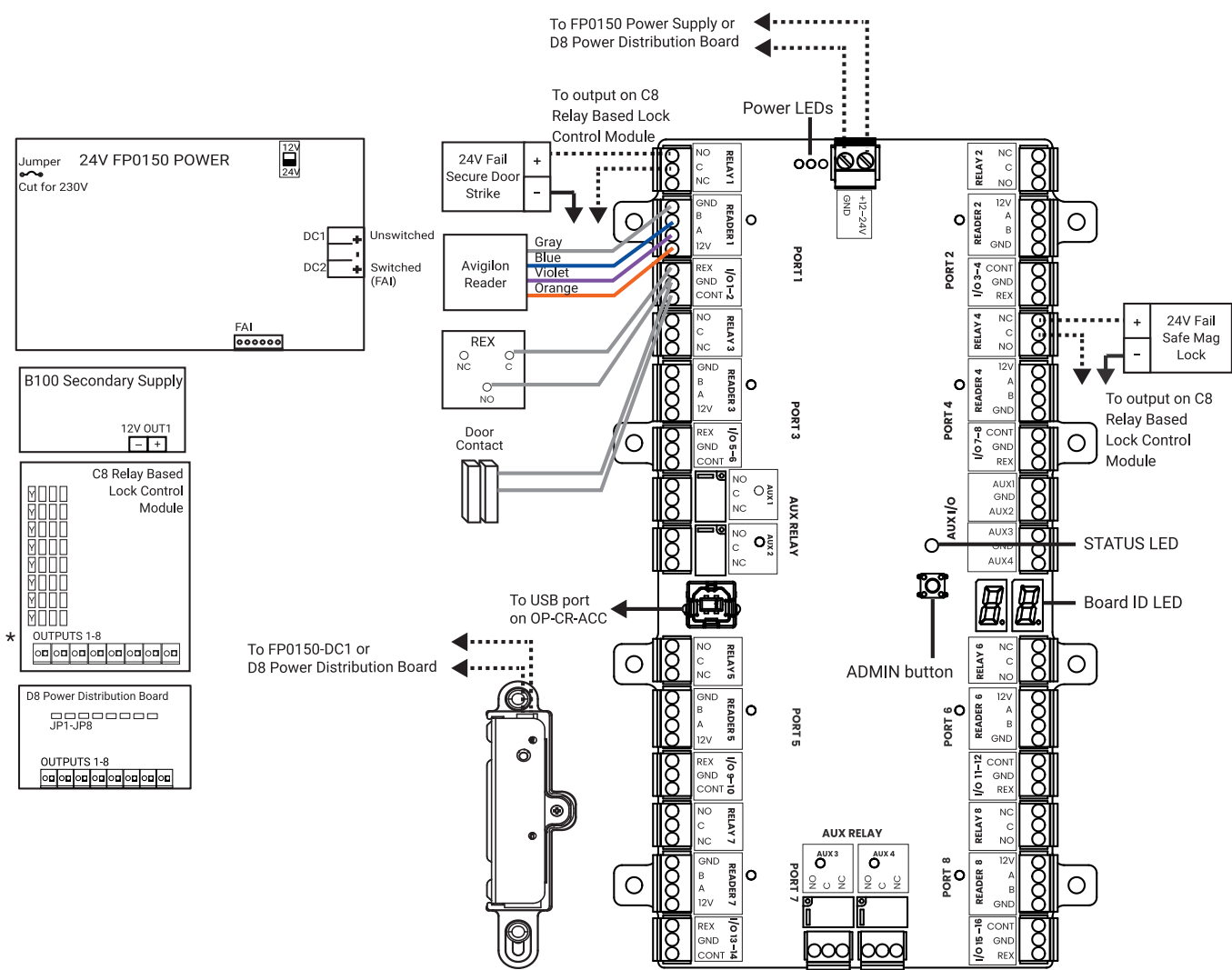



Figure 18 SYS-8ENT-DVE4 wiring diagram

24V FP0150 Power Supply The main output can be switched by the Fire Alarm Interface (FAI).
 Fail safe and fail secure are ways of configuring lock hardware:

- Fail-safe hardware *unlocks* when power is interrupted or lost.
- Fail-secure hardware *locks* when power is interrupted or lost.

For information about wiring third-party lock hardware, refer to vendor documentation.

***OUTPUTS 1–8** The voltage of each C8 or D8 output can be selected individually as 12V or 24V using the yellow jumper  corresponding to the output: position 1 on the jumper pins is 24V (this is the default setting) and position 2 is 12V.

Wiring the 12/24 16-Door Large Smart Hub

The 12/24 16-Door Large Smart Hub (SYS-16ENT-DVE6) uses the [LifeSafety Power FP0150 and FP250](#) to power the Access Control Core and 8-Port Boards; [LifeSafety Power B100](#) secondary power supplies; [LifeSafety Power C8 Relay Based Lock Control Modules](#) to power 12-24V locking hardware; and the [LifeSafety Power D8P Power Distribution Module](#) to power 12V and 24V locking hardware and accessories.

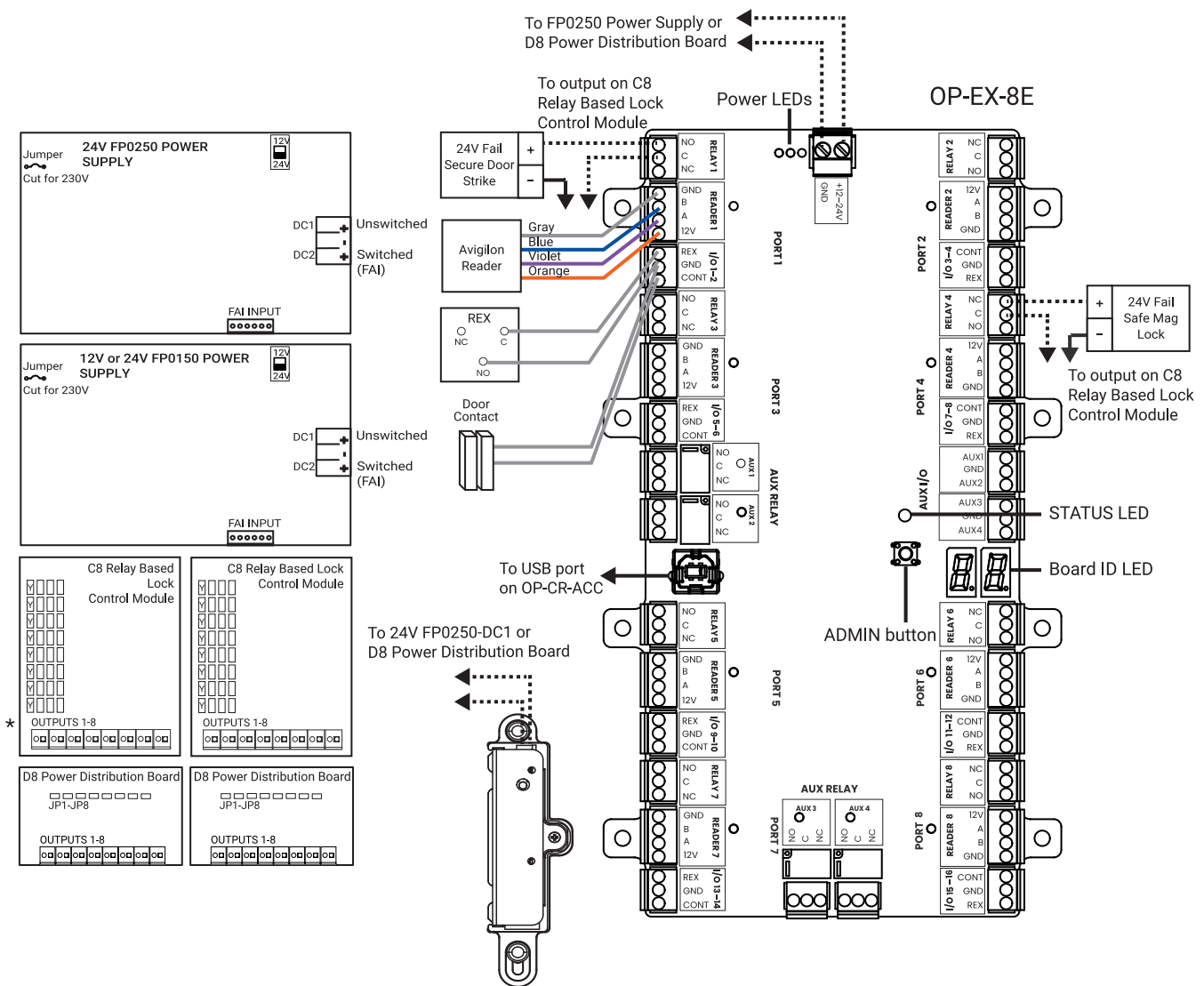


Figure 19 SYS-16ENT-DVE6 wiring diagram

**FP0150 and
FP0250 Power
Supplies**


The main output can be switched by the Fire Alarm Interface (FAI).

Fail safe and fail secure are ways of configuring lock hardware:

- Fail-safe hardware *unlocks* when power is interrupted or lost.
- Fail-secure hardware *locks* when power is interrupted or lost.

For information about wiring third-party lock hardware, refer to vendor documentation.

***OUTPUTS 1–
8**

If FPO150 is set to 12V, each C8 or D8 output can be selected individually as 12V or 24V using the yellow jumper  corresponding to the output: position 1 on the jumper pins is 24V (this is the default setting) and position 2 is 12V.

Wiring fail-safe and fail-secure lock hardware

Fail safe and fail secure are ways of configuring lock hardware:

- Fail-safe hardware *unlocks* when power is interrupted or lost.
- Fail-secure hardware *locks* when power is interrupted or lost.

For information about wiring third-party lock hardware, refer to vendor documentation.

See also [Appendix: Best practices - Wiring a REX to your Avigilon Alta access control system on page 64](#).

Advanced wiring

Wiring Wiegand readers to Avigilon readers

To support additional card credentials and biometric scanners, you can wire third-party Wiegand devices to the ACU by using the Smart Reader pigtail. Simply connect the power (red), ground (black), WD0 (green), and WD1 (white) from the Smart Reader pigtail to the Wiegand device.

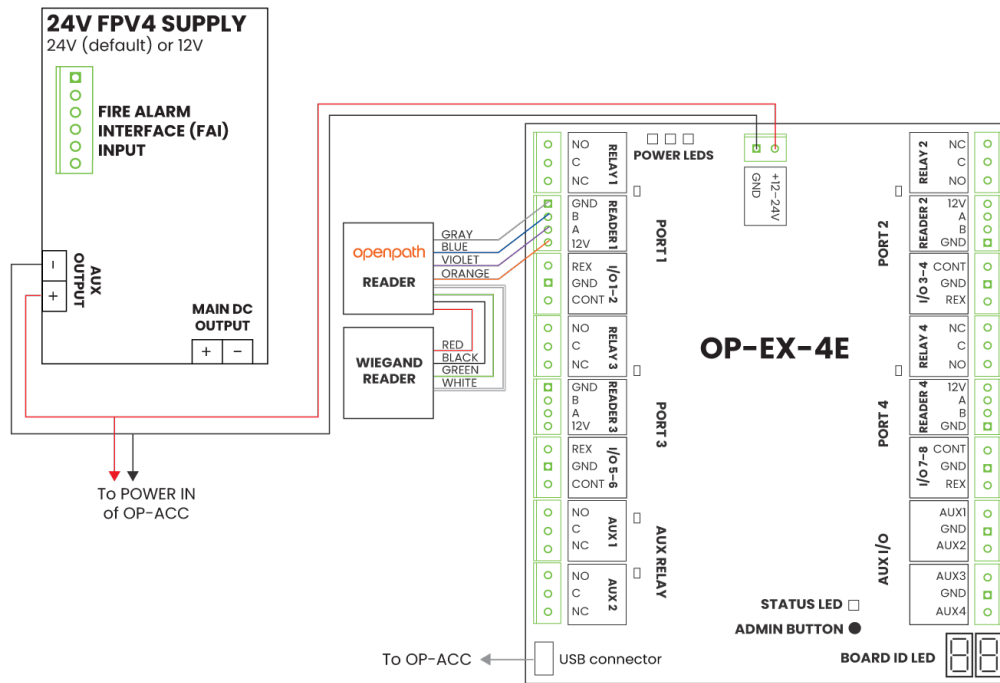


Figure 1 Wiring Wiegand readers to Avigilon readers

Wiring to legacy panels and mobile gateway

Note: The Avigilon Pro series readers (Video Reader Pro and Video Intercom Reader Pro) do not require a controller, however, a Smart Hub is required to support locking hardware.

To add mobile credential features (see 6 below) to a legacy access control system:

1. Install the Avigilon ACU (see 4) between the Avigilon Smart Readers (see 5) and the legacy panel (see 2) connected to legacy software (see 1). See [Change I/O types on page 48](#) to configure the ACU as output to the legacy panel and [Configure Wiegand devices in the Alta Control Center on page 49](#).
2. If existing Wiegand readers use a proprietary card format, they can be wired to new Avigilon Smart Readers. Otherwise, replace existing readers with Avigilon Smart Readers.

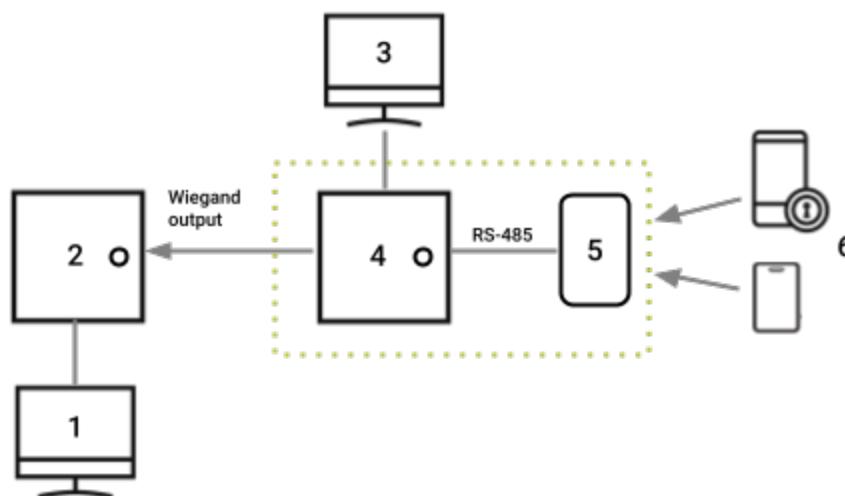


Figure 2 Wiring ACUs to legacy panels and legacy software



1	Legacy access control system software
2	Legacy access control system panel
3	Avigilon Alta Control Center
4a	Avigilon Smart Hub ACU installed between the Smart Reader and the legacy panel <ul style="list-style-type: none"> Note: The Video Intercom Reader Pro does not require a controller to be wired, however, a Smart Hub is required to support locking hardware. Note: The Video Reader Pro does not require a controller to be wired, however, a Smart Hub is required to support locking hardware. Note: The Avigilon Pro series readers (Video Reader Pro and Video Intercom Reader Pro) do not require a controller, however, a Smart Hub is required to support locking hardware.
4b	Wiegand port configured as output to the legacy panel <p>For more information, see advanced wiring in the Avigilon Alta Access Control System Installation Guide (link).</p>
5	Avigilon Smart Readers <p>If existing Wiegand readers use a proprietary card format, they can be wired to new Avigilon Smart Readers. Otherwise, replace existing readers with Avigilon Smart Readers.</p>
6	Avigilon Alta Open app, Cloud Key credentials and Wave to unlock functionality <p>Avigilon credential with default gateway number or Wiegand ID</p>

In this configuration, the legacy panel controls all locking hardware and entry mechanisms while the Avigilon system lets you use the Avigilon Alta Open app, Smart Reader, and Wave to Unlock functionality. Refer to the Avigilon Alta Control Center Administrator Guide for more information on configuring Mobile Gateway settings.

Change I/O types

While I/Os on the 4-Port Board and 8-Port Board are labeled REX and CONTACT by default, you can use these I/Os interchangeably or as generic inputs, by modifying their type in the Alta Control Center. You can also change them to Wiegand inputs, which requires a few extra steps. For more information, see the Avigilon Alta Control Center Administrator Guide.

Change input types in the Alta Control Center

1. Go to control.openpath.com/login and sign in. To access the European Alta Control Center, go to control.eu.openpath.com/login.
2. Go to  **Devices** > **ACUs** and click the ACU to edit it.
3. Click on the **Ports** tab.
4. Click  **Port** next to the input to be re-purposed.
5. Select a different type from the **Input type** dropdown, and click **Save**.

Wire to Wiegand devices on Core Series Smart Hubs

You can wire third-party Wiegand readers and panels to the ACU to support integrations or Mobile Gateway mode. The extra Auxiliary I/Os on the 4-Port Board and 8-Port Board can be used for wiring Wiegand devices, however, any I/O pair may be used including Contact and REX inputs.

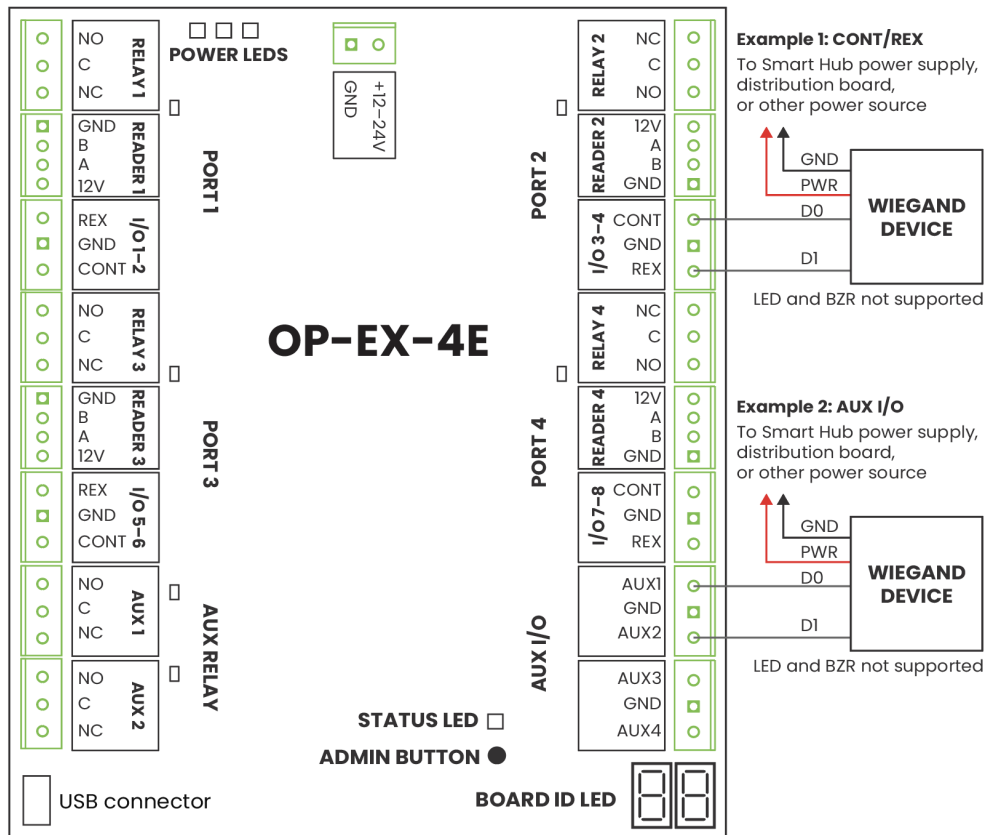
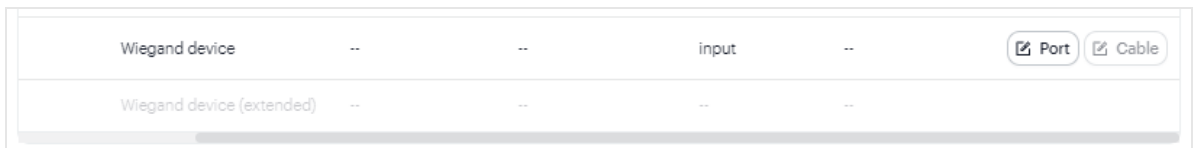


Figure 3 Wiring a Wiegand device to a Core Series Smart Hub


Configure Wiegand devices in the Alta Control Center

- Go to control.openpath.com/login and sign in. To access the European Alta Control Center, go to control.eu.openpath.com/login.
- Go to **Devices > ACUs** and click the ACU to edit it.
 - Click the **Ports** tab.
 - Click **Port** next to the first input of the I/O pair with a Wiegand device configured (in example 1, Contact2; in example 2, AUX1).
 - Select from **Input type**, and click **Save**.

This will label the subsequent input as **Wiegand device (extended)** and disable it from editing. Inputs cannot be changed if they are already assigned to an entry.



Once the Wiegand device is configured on the ACU, it can be assigned to an entry.

3. Go to  **Sites > Entries**, and create or edit an existing entry. In the Wiegand device settings, configure the following:

- **Port** – The port for the Wiegand device to which this entry is wired.
- **Mode** – The direction the card credential data is sent.
 - **Input** – Receives data from the Wiegand reader.
 - **Output (gateway)** – Sends credential data to a third-party control panel.

Enable **Gateway credential pass-through** if you do not want the Avigilon Alta system to authenticate credentials, but rather send all data to the legacy panel for authentication.

Enter a **Default gateway card number** so that all credentials (including mobile credentials) are sent to the legacy panel as a Wiegand ID.

For more information on creating entries, refer to the Avigilon Alta Control Center Administrator Guide.

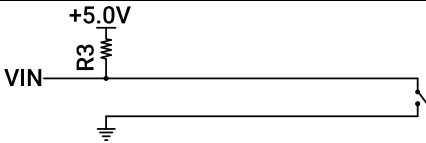
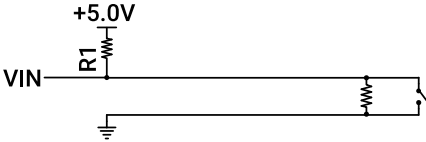
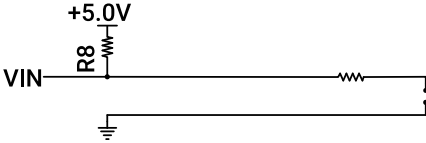
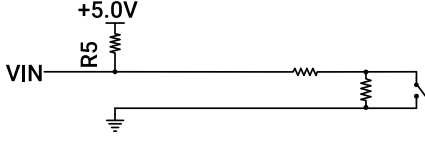
End-of-line supervision

The 4-Port Board and 8-Port Board inputs have support for user-installed single or double 1k ohm termination.



This lets you monitor cut or shorted lines, and create alerts and rules in the Alta Control Center.

Configure EOL in the Alta Control Center

The input settings in the Alta Control Center must match the physical wiring configurations.

Type	Cable →	End of line supervision setting
Smart Hub No EOL		None
Smart Hub Single EOL		Cut Line Detect
Smart Hub Single EOL		Line Shorted Detect
Smart Hub Double EOL		Both

1. Go to control.openpath.com/login and sign in. To access the European Alta Control Center, go to control.eu.openpath.com/login.

2. Go to  **Devices** > **ACUs**.
3. Select the ACU to edit it.
4. Click the **Ports** tab. Click  **Cable** next to the port with the EOL configured.
5. Select the appropriate **End of line supervision** setting — **None**, **Cut Line Detect**, **Line Shorted Detect**, or **Both**.
6. Click **Save**.

Provisioning

Provisioning the ACU means registering it in the Avigilon Alta Control Center and running the latest firmware. You will need to re-provision in the case of a hard reset, see [Resetting ACUs on page 62](#).

Note: If you are provisioning ACUs for a customer account, the customer organization needs to be created first.

Prerequisites

- Meet all [Network requirements on page 11](#).
- Connect the ACU to the internet using the Ethernet cable.
- Install the Avigilon Alta Access app.



- If you are using a laptop instead of the app, the laptop must be on the same network as the ACU. If you have a VLAN, make sure the laptop is on the same VLAN as the ACU.
- If you are using a laptop running Microsoft™ Windows or Linux®, you must download the [iTunes](#) app. The provisioning process uses Bonjour software that comes with iTunes. Optionally, you can download iTunes and use an archive utility to extract and install only the Bonjour MSI.

App Store® and the Apple logo® are trademarks of Apple Inc. Google Play and the Google Play logo are trademarks of Google LLC. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Power, Relay, Status, and Board ID LEDs

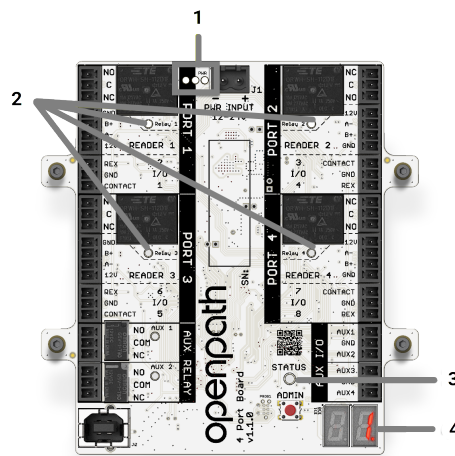


Figure 4 Expansion board LEDs – 4-Port Board example

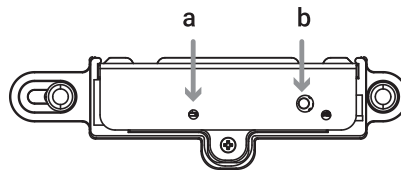







Figure 5 STATUS LED (a) and ADMIN button (b) on Access Control Core

Avigilon ACUs (Access Control Core and Expansion Boards) have several LEDs that indicate the following.

No.	Label	Description
1	PWR	Power LEDs indicate when the board is connected to power.
2	Relay 1 Relay 2 Relay 3 Relay 4	Relay LEDs indicate when the relays are activated.
3	STATUS	Status LED indicates when the ACU has been configured with firmware. See Expansion board Status LED indicator below.
4		Board ID LED matches the EXPANSION BOARD NUMBER in the Alta Control Center.

Expansion board Status LED indicator










The Status LED on the 4-Port Board or 8-Port Board board indicates the following.

Port LED	Description
 Solid green	The expansion board is connected and communicating with the Access Control Core.
 Solid red	The connection to the Access Control Core is in an error state. To resolve the issue, try: <ul style="list-style-type: none"> • Power cycle the 4-Port Board or 8-Port Board. • Unplug and replug the USB cable. • Restart the device in Alta Control Center. Go to  Dashboards > Device , and choose Restart device communicator from the REMOTE DIAGNOSTICS column.
 Blinking red	The expansion board firmware is being updated.

The Status LED on the Access Control Core has several states, see [Access Control Core Status LEDs on the next page](#).



Access Control Core Status LEDs








The Status LED on the Access Control Core controller indicates the following.

Status LED	Description
 Solid green	The Access Control Core is provisioned and operating as expected.
 Solid cyan	The Access Control Core is booting up.
 Solid yellow	The Access Control Core is restoring software. Appears when you power on the Access Control Core for the first time or perform a hard reset.
 Blinking yellow	<p>The Access Control Core is updating software. Indicates when the Access Control Core has been online for less than 24 hours.</p> <p>If the device is stuck in this state after 3.5 hours, an unexpected issue may have occurred. Contact Avigilon Alta Support before power cycling the device.</p>
 Solid blue	The Access Control Core is in an unprovisioned state. Indicates the Access Control Core has finished booting and is ready for provisioning.
 Solid purple	The Access Control Core is connected to the Avigilon Alta Access app.
 Blinking purple	The Access Control Core is ready to connect to the Avigilon Alta Access app.
 Blinking red	<p>The Access Control Core is not connected to the internet.</p> <p>The Access Control Core configuration is being updated and saved in the Alta Control Center. The device continues to operate as expected.</p> <p>The blinking red indicator is expected to be temporary and change back to the solid green indicator. If the device is stuck in this state after 5 seconds, contact Avigilon Alta Support.</p>
 Solid red	<p>The Access Control Core is in an error state.</p> <p>Go to the Devices dashboard in Alta Control Center for more information.</p>

Smart Reader LED indicator




The Avigilon Smart Reader LED indicates the following:







Status LED	Description
	The entry or door is locked.
	The entry or door is unlocked.

Status LED	Description
	The reader has just received power.
	The reader is not connected to power. Check if power wires are swapped. The reader firmware is being updated.
	The reader is connected to power, but cannot communicate with the ACU. Check if the +B (blue) and -A (violet) lines are swapped. An expansion board issue has occurred, expansion board firmware is being updated, or a general communication error has occurred between the reader and expansion board.
	The reader is connected to power and can communicate with the ACU. The reader is not configured as an entry in the Alta Control Center.
	The reader is identified by the Alta Control Center.
	The reader might not be receiving enough voltage or current, potentially due to a break in wiring. Try connecting the reader directly to the ACU, bypassing any wire runs.
	The wires might be swapped. Check that +12V IN (orange) is not swapped with +B (blue) or -A (violet).

Avigilon Pro Series Reader LED indicator

The Video Reader Pro and Video Intercom Reader Pro status LEDs indicate the following:


Status LED	Description
	The entry is locked.
	The entry is unlocked.
	The reader is not connected to power. Check to see if power wires are swapped.

Status LED	Description
	The reader firmware is being updated.
	Center dot is blinking blue. The reader is booting.
	Center dot is solid yellow. The reader is restoring software to factory default.
	Center dot is solid blue. The reader is ready to be provisioned or has not been configured as an entry in the Alta Control Center.
	Center dot is solid purple. The reader is ready to connect to Avigilon Alta Access app.
	Center dot is solid green and the outer ring is solid white. The reader has been identified in the Alta Control Center.
	Center dot is blinking red. The reader is connected to power, but cannot communicate with the ACU.
	An expansion board issue has occurred, expansion board firmware is being updated, or a general communication error has occurred between the reader and expansion board.

Add ACUs using Alta Control Center

Before you can provision an ACU using the Avigilon Alta Access app, you must first create an ACU in the Alta Control Center.

Add multiple ACUs using Quick start option


1. Go to control.openpath.com/login and sign in. To access the European Alta Control Center, go to control.eu.openpath.com/login.
2. Go to  **Administration** > **Quick start**.
3. Enter a **Site name** and any other relevant site information.
 - a. In **Site language**, select the preferred language for the site-wide emails sent by the system.
 - b. Click **Next**.
4. Enter the number of controllers located at your site and:
 - a. Enter names for the controllers.
 - b. In **Controller type**, select the type used:


- **First generation - Red Board (OP-AS-01)** – For first generation Smart Hubs.
 - **Core series ACU** – For Core Series Smart Hubs.
- c. If your ACU also connects to an expansion board, add the appropriate types in EXPANSION BOARDS:


 **Tip:** The Openpath boards are most common with the Core Series Smart Hub.

- **Openpath 4-Port Expansion**
 - **Openpath 8-Port Expansion**
 - **Openpath 16-Port Elevator**
5. Enter the number of readers connected to the controllers. Enter their names and click **Next**.
 6. Review your site details and click **Confirm & submit**. It may take a few minutes for setup to complete.

Add one ACU

1. Go to  **Devices > ACUs**.
2. To add a new ACU, click the **+** button in the upper-right corner.
3. Enter a unique name for the ACU.
4. In **Controller type**, select the type used:
 - **First generation - Red Board (OP-AS-01)** – For first generation Smart Hubs.
 - **Core series ACU** – For Core Series Smart Hubs.
5. If your ACU also connects to an expansion board, add the appropriate types in EXPANSION BOARDS:

 **Tip:** The Openpath boards are most common with the Core Series Smart Hub.

- **Openpath 4-Port Expansion**
 - **Openpath 8-Port Expansion**
 - **Openpath 16-Port Elevator**
6. Click **Add board**.
 7. Optional. To connect your network to the Cloud using a static IP address and port on an allowlist, select the **Enable Static Cloud IP** toggle. Default port is 443. An Enterprise plan is required to use Static Cloud IP.
 - a. Go to  **App marketplace** and ensure the **Static Cloud IP** app is installed.
 - b. After the toggle is enabled in the Alta Control Center, open the Avigilon Alta Access app and select **Provision with Static Cloud IP** to provision the devices.
 8. Click **Save**.

Example: Avigilon expansion board connection to an ACU

× Create ACU

ACU

Controller name*
ACU 001

Controller type*
ACU der Core-Serie

EXPANSION BOARDS

Add expansion board
Openpath 4-Port Expansion

Add board

EXPANSION BOARD NUMBER	EXPANSION BOARD NAME	ACTION	ENABLE
1	Openpath 4-Port Expansion	To be added	--

CLOUD CONNECTION METHOD

Enable Static Cloud IP

NOTES

Enter notes about this ACU...

Reset Save

Disable the Static Cloud IP connection

If it is necessary to disable the Static Cloud IP connection:

- Go to the Edit ACU page, and deselect the **Enable Static Cloud IP** toggle.

Normal cloud operation resumes after the Static Cloud IP connection is disabled.

Provisioning options

Provision the ACU using Avigilon Alta Access app (recommended)

1. Log in to the Avigilon Alta Access app with your Alta Control Center credentials.
2. Locate the organization to which you're provisioning hardware, either on the list or using search, and then tap on the organization name.
3. Press the Admin button on the controller board or Access Control Core.
4. In the Avigilon Alta Access app, tap on the last four digits of the serial number for the ACU.
5. Tap **Test Internet Connection** and wait for a green YES to appear before proceeding with the next step.

 **Note:** This checks if the ACU or SDC can ping <https://api.openpath.com/health>.





6. Tap **Provision Device**.
7. Tap on the ACU Name that you want to provision to (this is the name of the ACU you created in the Alta Control Center), and then tap **Yes** to proceed.
8. The app will send notifications when ACU provision state changes from **Unprovisioned** to **Provisioning in progress** to **Provisioning complete**.

 **Note:** The ACU will disconnect from the Avigilon Alta Access app app 5 minutes after first pressing the Admin button.

Provision the ACU using Alta Control Center on a laptop

1. Go to control.openpath.com/login and sign in. To access the European Alta Control Center, go to control.eu.openpath.com/login.

 **Note:** The laptop must be connected to the same network as the ACU.

2. Go to  **Devices > ACUs**.
 - a. Locate your ACU on the list.
 - b. If you don't see your ACU listed, create a new one:
 - i. Click the  button in the upper-right corner.
 - i. Go to  **Devices > ACUs**.
 - ii. To add a new ACU, click the  button in the upper-right corner.
 - iii. Enter a unique name for the ACU.

- iv. In **Controller type**, select the type used:
 - **First generation - Red Board (OP-AS-01)** – For first generation Smart Hubs.
 - **Core series ACU** – For Core Series Smart Hubs.
- v. If your ACU also connects to an expansion board, add the appropriate types in EXPANSION BOARDS:

 **Tip:** The Openpath boards are most common with the Core Series Smart Hub.

- **Openpath 4-Port Expansion**
- **Openpath 8-Port Expansion**
- **Openpath 16-Port Elevator**

- vi. Click **Add board**.
- ii. Click **Save**.

3. On the ACU, press the ADMIN button.

4. In the Alta Control Center, click the  Register button next to the name of your ACU.

a. Click **Yes** to proceed. A new window will open.

b. Click **Provision**.

c. If you see a "This Site Cannot be Reached" error, you need to ping the ACU using the command line:

i. Open a command prompt and run:

- On Windows: `ping oppi.local`
- On Mac or Linux: `ping -c4 oppi.local`

- If nothing returns, check your network requirements. See [Network requirements on page 11](#).

ii. You should see the ACU's IP address, either in IPv4 or IPv6 format. Copy the address and return to the error page.

iii. In the URL, delete everything before `:8080`.

- If using an IPv4 address, paste before `:8080`. For example: `192.0.2.0:8080`
- If using an IPv6 address, delete the last two digits and the percentage sign, put square brackets outside the address, and paste before `:8080`.

- **Correct:** a123::b456:5a18:eb8f:7fd6:8080
- **Incorrect:** a123::b456:5a18:eb8f:7fd6%29:8080
- Press **Enter** and then click the **Provision** button.
- If the Provision button still doesn't appear, contact Avigilon Alta Support at (844) 673-6728 Ext 2 or support@openpath.com.

Test internet connection using Avigilon Alta Access app

In the Avigilon Alta Access app, you can tap **Test Internet Connection** to check if the ACU can ping api.openpath.com/health.

Configure network settings using Avigilon Alta Access app

In the Avigilon Alta Access app, you can configure network settings for the ACU. While wired internet connections are preferred, you can configure the Access Control Core to use Wi-Fi instead. The default interface for the Access Control Core is Ethernet/wired connection. Ethernet and Wi-Fi connections can be DHCP (default) or can have a static IP address.

The Access Control Core supports 2.4 GHz and 5 GHz Wi-Fi connections.

Change network settings

1. Connect to the Access Control Core by pressing the Admin button again, if needed.
2. Tap on **Network Settings**.
3. Select **Configure network manually**.
4. Configure the network settings as needed. Set a static IP address or set a preferred DNS server.
5. Tap **Save** in the top-right corner.

Set up Wi-Fi on the Access Control Core

1. Connect to the Access Control Core by pressing the Admin button again, if needed.
2. Tap on **Network Settings**.
3. Tap on **Wi-Fi IP Settings**.
4. Enable **Default Interface**.
5. Tap on **Pick Wi-Fi Network**.
6. Choose your network, enter your password, and then tap **Connect**.

Maintenance and troubleshooting

Warning:

- Disconnect power before servicing.
- Do not plug into an outlet controlled by an on/off switch.
- Powering the power supply with 230V requires jumper modification. See the power supply datasheet for more information.

Legacy wiring

Sometimes legacy wiring (unshielded and straight through, rather than shielded twisted pair, often 22-6) results in slower connections and dropped packets between the Avigilon reader and ACU. To remedy this, you can switch GND and VIN with +B and -A connections on the ACU and readers to ensure the data pair (+B and -A) are using the alternate pair of legacy wires.

Resetting ACUs

Soft reset

To soft reset the ACU, disconnect power from the ACU, wait 10 seconds, and then reconnect the power.

Hard reset

- Warning:** Only hard reset the ACU if absolutely necessary and if instructed by Avigilon Alta Support. This will clear all of the data off of the ACU and will require reprovisioning.

1. Disconnect power from the ACU.
2. Press the Admin button (see b).

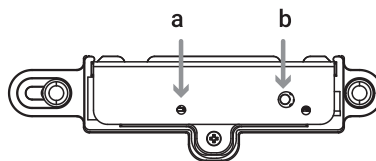


Figure 1 STATUS LED (a) and ADMIN button (b) on Access Control Core

3. While still pressing the Admin button, reconnect the power. Continue to hold the button for another 15 seconds until the status LED (see a) turns yellow ●, and then release.
4. Wait 15 minutes or until the status LED turns blue ● before provisioning. See [Provisioning on page 52](#).

Reset video readers and video intercom readers

 **Warning:** A hard reset will erase all data on the device. Only reset if instructed by Avigilon Alta Support.

1. Disconnect power from the device.
2. Press and hold the Admin button.
3. Reconnect power to the device.
4. Continue pressing the Admin button until the LED turns solid yellow (about 10 seconds), and then release.

Resolve common issues

To resolve common issues in the Video Intercom Reader Pro , see this Alta [support article](#).

Appendix: Best practices - Wiring a REX to your Avigilon Alta access control system

For fire and safety reasons, and in accordance with building code in many jurisdictions, a Request to Exit (REX) device is used to ensure free egress.

Important: Always defer to the Authority Having Jurisdiction (AHJ) for all building code requirements, including code requirements for REX devices and how they should connect to an access control system, such as Avigilon Alta.

Wiring REX in series with mag lock or other fail-safe hardware

Although you can wire a REX directly to the Avigilon Alta (formerly Openpath) access control unit (ACU) like other access control systems, the best practice would be to wire the REX device in series with electromagnetic (mag lock) or other fail-safe hardware. This prevents any points of failure in the egress path. If the REX device is wired directly to the REX input on an ACU, then the Avigilon Alta access control system can simply shunt forced-open alarms only, or shunt forced-open alarms and trigger the relay to unlock. In the event of complete power loss, the lock hardware specified by the AHJ would be fail-safe or fail-secure.

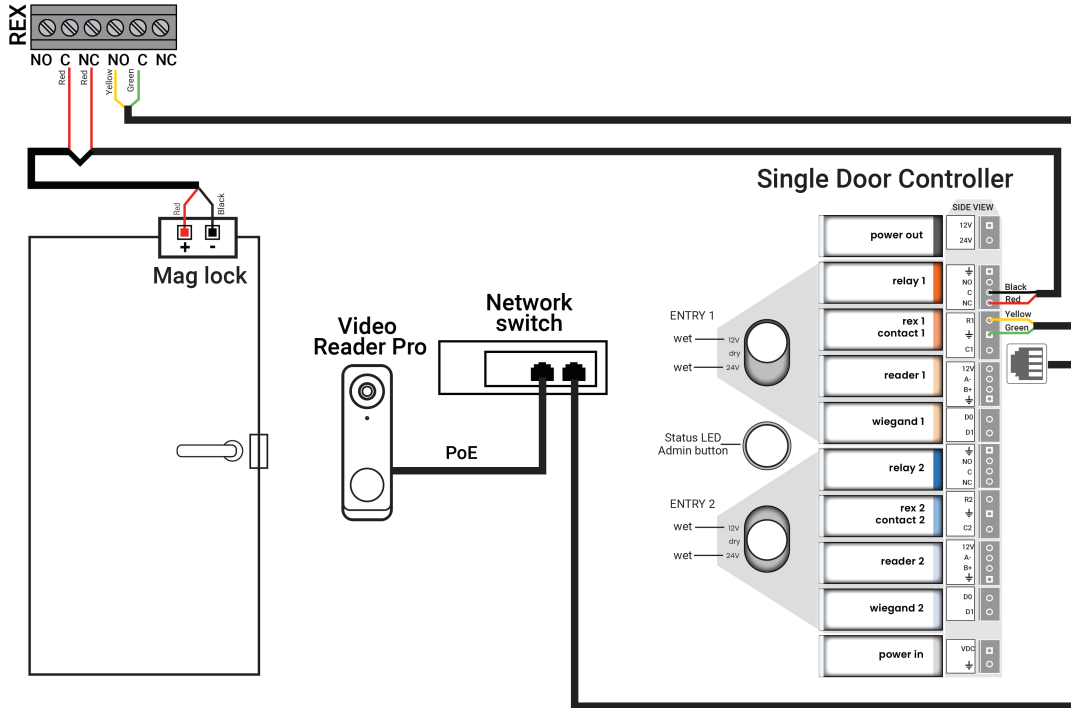
- Fail-safe hardware *unlocks* when power is interrupted or lost.
- Fail-secure hardware *locks* when power is interrupted or lost.

Wiring REX with Video Reader Pro and Video Intercom Reader Pro

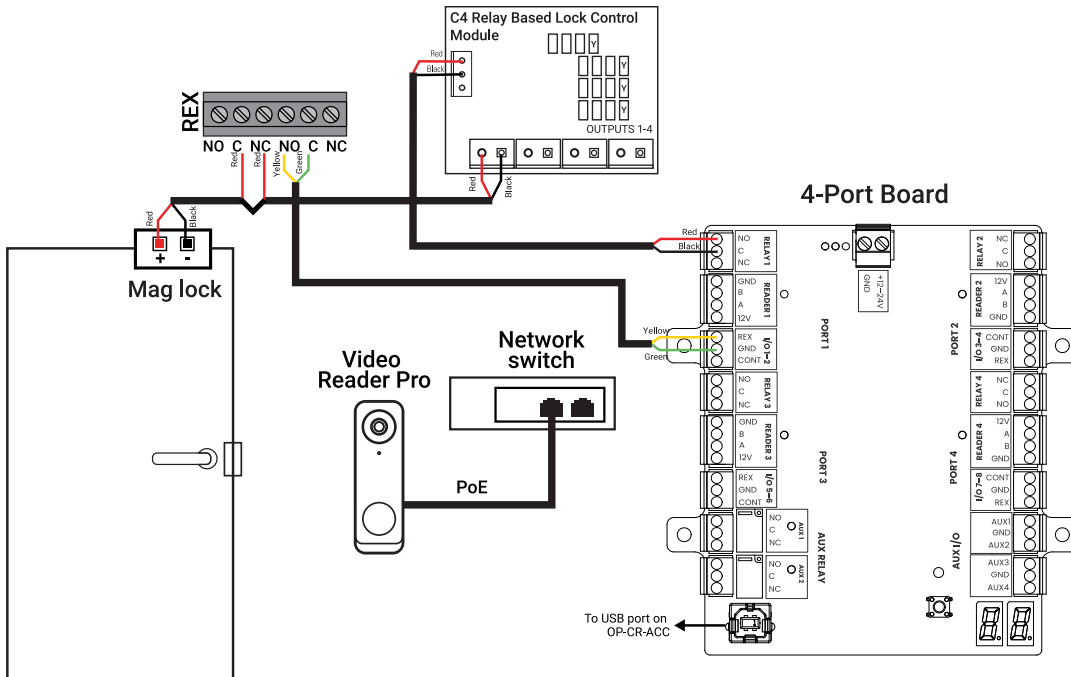
Because these devices do not include a REX input or door relay, you must use a remote ACU to manage door peripherals, such as a door lock relay, door contact, and a REX device. A LAN connection to the remote ACU is required to control all door peripherals that are assigned to the Video Reader Pro or Video Intercom Reader Pro entry. If the Video Reader Pro and the Video Intercom Reader Pro go offline, and if the REX is not wired in a series with the lock hardware, the REX on the entry does not engage the remote relay. It is important to follow the best practices outlined here and the diagrams below to ensure a reliable experience when the Video Reader Pro or Video Intercom Reader Pro is inaccessible due to a network interruption, maintenance, or firmware update.

Tip: The following wiring diagrams are examples. Make sure you follow the installation instructions of third-party hardware for cable type, power requirements, and manufacturer-specific configurations (for example, DIP switch configuration).


Example: Remote REX on Single Door Controller with Video Reader Pro or Video Intercom Reader Pro



Example: Remote REX on 4-Port Board with Video Reader Pro or Video Intercom Reader Pro



To further improve reliability, Avigilon Alta will be implementing changes that will engage the remote relay for the entry when the REX is triggered even if the associated video device is unavailable. The controller for this relay should have a battery backup or be wired in a fail-safe configuration for maximum reliability.

 **Tip:** In Alta Control Center reporting, a REX event on Video Reader Pro and Video Intercom Reader Pro entries will appear twice due to these changes. This duplicate can be safely ignored.

Regulatory notice

All national and local electrical codes apply.

UL 294

The following performance levels are defined for the Core Series Smart Hub, Smart Reader v2, Smart Keypad Reader, Embedded USB Smart Reader, Video Intercom Reader Pro, and Video Reader Pro as per UL 294:

Attack:	Level I
Endurance:	Level I
Line Security:	Level I
Standby:	Level I

CAN/ULC 60839-11-1-16 GRADE 1

For C-UL Listed applications, the unit shall be installed in accordance with Part 1 of the Canadian Electrical Code.

FCC

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm should be maintained between the antenna of Openpath Smart Reader(s) and persons during operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the User will be required to correct the interference at his own expense.

OP-ACC: Contains FCC ID:2ABCB-RPI3B

OP-CR-ACC:Contains FCC ID:2ABCB-RPI4B

OP-R2X-EMBD: FCC ID:2APJVOPR2LHF

OP-R2X-MULL: FCC ID:2APJVOPR2LHF

OP-R2X-STND: FCC ID:2APJVOPR2LHF

OP-RKP-MULL: FCC ID:2APJVOPR2LHF

OP-RKP-STND: FCC ID:2APJVOPR2LHF

OP-VID-PRO-INT: FCC ID:2APJVOPVNRC
OP-VID-PRO-RDR: FCC ID:2APJVOPVRC
OP-2ESH-POE: FCC ID:2APJV2ESH
OP-4ESH-24V; FCC ID:2ABCB-RPI3B
SYS-4ENT-DVE1: FCC ID:2ABCB-RPI4B
SYS-8ENT-DVE2: FCC ID:2ABCB-RPI4B
SYS-8ENT-DVE4: FCC ID:2ABCB-RPI4B
SYS-16ENT-DVE6: FCC ID:2ABCB-RPI4B
SYS-ELEV-SVE1: FCC ID:2ABCB-RPI4B
4ENT-SYS-1224V: Contains FCC ID:2ABCB-RPI3B
4ENT-SYS-24V: Contains FCC ID:2ABCB-RPI3B
8ENT-SYS-1224V: Contains FCC ID:2ABCB-RPI3B
20ENT-SYS-24V: Contains FCC ID:2ABCB-RPI3B

IEC 62368-1

- This equipment is intended only for use in a restricted access area.
- Securely fasten the equipment according to LifeSafety Power mounting instructions. See [FlexPower Vantage Standard Power System - Installation Manual](#)¹.
- PROTECTIVE EARTHING: For safety, the Smart Hub must only be plugged into a grounded 3-prong outlet, wired with a minimum of 16 gauge wire to ground.

RF Radiation Hazard Warning

To ensure compliance with FCC and Industry Canada RF exposure requirements, Smart Hubs device must be installed in a location where the antennas of the device will have a minimum distance of at least 20 cm from all persons. Using higher gain antennas and types of antennas not certified for use with this product is not allowed. The device shall not be co-located with another transmitter.

Installez l'appareil en veillant à conserver une distance d'au moins 20 cm entre les éléments rayonnants et les personnes. Cet avertissement de sécurité est conforme aux limites d'exposition définies par la norme CNR-102 at relative aux fréquences radio.

¹See https://lifesafetypower.com/docs/im_fpv-standard.pdf.

Industry Canada Notice and Marking

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other Users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

IC Company Number: 25142

OP-4ESH-24V; IC ID: 25142-OP2ESH

OP-CR-ACC: Contains IC ID: 20953-RPI4B

OP-R2X-EMBD: IC ID: 25142-OPR2LHF

OP-R2X-MULL: IC ID: 25142-OPR2LHF

OP-R2X-STND: IC ID: 25142-OPR2LHF

OP-RKP-MULL: IC ID: 25142-OPRKPM

OP-RKP-STND: IC ID: 25142-OPRKP

SYS-4ENT-DVE1: Contains IC ID: 20953-RPI4B

SYS-8ENT-DVE2: Contains IC ID: 20953-RPI4B

SYS-8ENT-DVE4: Contains IC ID: 20953-RPI4B

SYS-16ENT-DVE6: Contains IC ID: 20953-RPI4B

SYS-ELEV-SVE1: Contains IC ID: 20953-RPI4B

4ENT-SYS-1224V: Contains IC: 20953-RPI3B

4ENT-SYS-24V: Contains IC: 20953-RPI3B

8ENT-SYS-1224V: Contains IC: 20953-RPI3B

20ENT-SYS-24V: Contains IC: 20953-RPI3B

IC RSS-102

This equipment complies with the IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 5mm between the radiator and the body.

OP-RKP-STND

OP-RKP-MULL

 **Warning:**

- Disconnect power before servicing.
- Do not plug into an outlet controlled by an on/off switch.
- Powering the power supply with 230V requires jumper modification. See the power supply datasheet for more information.

Electrical specifications

For the hardware specifications, see the datasheets [on page 9](#).

16 I/O Elevator Board (OP-16EM)	12-24VDC, 0.35A @ 12V, 0.2A @ 24V
4-Port Board (OP-EX-4E)	12-24VDC, 0.5A @ 12V, 0.3A @ 24V
8-Port Board (OP-EX-8E)	12-24VDC, 0.6A @ 12V, 0.3A @ 24V
Smart Reader v2 (OP-R2X-STND, OP-R2X-MULL)	12-24VDC, 0.25A @ 12V, 0.12A @ 24V
Embedded USB Smart Reader (OP-R2X-EMBD)	12-24VDC, 0.25A @ 12V, 0.12A @ 24V, 5V USB
Smart Keypad Reader (OP-RKP-STND, OP-RKP-MULL)	12-24VDC, 0.25A @ 12V, 0.12A @ 24V
Access Control Core (OP-ACC)	Operating Voltage: 12-24VDC Operating Current: 0.7A @ 12VDC, 0.4A @ 24VDC
Access Control Core (OP-CR-ACC)	Operating Voltage: 12-24VDC Operating Current: 0.7A @ 12VDC, 0.4A @ 24VDC
Video Intercom Reader Pro (OP-VID-PRO-INT)	Input Voltage: 802.3af PoE (48VDC, 0.27A) Power Consumption: 10.8W
Video Reader Pro (OP-VID-PRO-RDR)	Input Voltage: 802.3af PoE (48VDC, 0.27A) Power Consumption: 7.8W
12/24V 4-Door Smart Hub (SYS-4ENT-DVE1)	Input Voltage: 120VAC, 208/230VAC with cuttable jumper Input Current: 1.8Amp max. Operating Voltage: 12VDC and 24VDC Operating Current: 1.2A @ 24V with 4 Smart Readers, 0.7A @ 24V with no Smart Readers
12/24V 8-Door Smart Hub (SYS-8ENT-DVE2)	Input Voltage: 120VAC, 208/230VAC with cuttable jumper Input Current: 3.7Amp max. Operating Voltage: 12VDC and 24VDC Operating Current: 1.8A @ 24V with 8 Smart Readers, 0.7A @ 24V with no Smart Readers
12/24 8-Door Large Smart Hub (SYS-8ENT-DVE4)	Input Voltage: 120VAC, 208/230VAC with cuttable jumper Input Current: 2.5Amp max. Operating Voltage: 12VDC and 24VDC

	Operating Current: 1.8A @ 24VDC with 8 Smart Readers; 0.7 @ 24VDC with no Smart Readers
12/24 16-Door Large Smart Hub (SYS-16ENT-DVE6)	<p>Input Voltage: 120VAC, 208/230VAC with cuttable jumper</p> <p>Input Current: 2.5Amp/3.2A max. (two supplies)</p> <p>Operating Voltage: 12VDC and 24VDC</p> <p>Operating Current: 3.2A @ 24VDC with 16 Smart Readers; 1A @ 24VDC with no Smart Readers</p>
24V Elevator Smart Hub (SYS-ELEV-SVE1)	<p>Input Voltage: 120VAC, 208/230VAC with cuttable jumper</p> <p>Input Current: 1.8Amp max.</p> <p>Operating Voltage: 12VDC and 24VDC</p> <p>Operating Current: 1.1A @ 12VDC, 1.6A with 2 Smart Readers; 0.6A @ 24VDC, 0.9A with 2 Smart Readers</p>
Smart Hub with 12/24V Supply (OP-4ESH-24V)	120V, 0.7A or 230V, 0.3A, 50/60 Hz