AVIGILON™

Access Control Core

Installation Guide

OP-CR-ACC

Avigilon Corporation
avigilon.com

20241122-en

Revisions

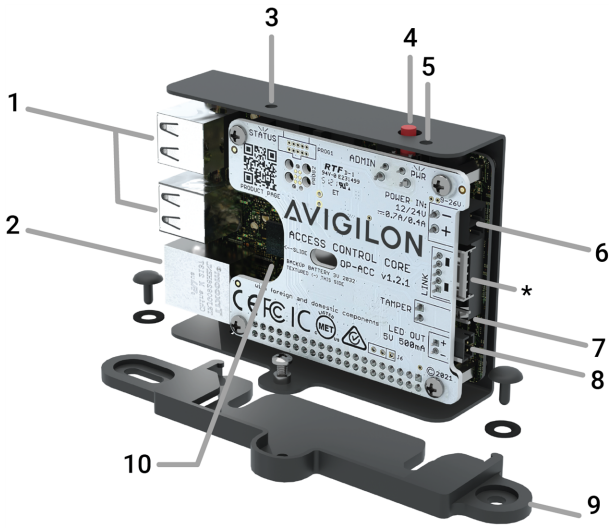
Guide	Description
November 2024	Mercury™ MP Series intelligent controller support: Mercury device installation on page 12, Add one ACU on page 22
September 2024	Control Center portal renamed to Alta Access Tip about using Avigilon Alta Access mobile app: Add ACUs using Alta Access on page 21
August 2024	Initial release of guide

Contents

Before you start

The Avigilon Access Control Core is an access control unit (ACU) that controls up to 8, 12, or 16 entries through two expansion board connections. This installation guide explains how to install and configure the Access Control Core, as part of the Alta access control system, including expansion board connections to Mercury™ hardware connected to third-party Wiegand and OSDP readers.

Overview



1	USB ports	**6**	Power input
2	Ethernet connector	**7**	Tamper switch
3	Status LED	**8**	LED output (future use)
4	Admin button	**9**	The Access Control Core is installed with the ports facing down, up, left, or right, depending on the enclosure model. Use of the bracket is recommended for added stability in SYS-4ENT-DVE1, SYS-8ENT-DVE2, and SYS-ELEV-SVE1 models. Use of the bracket is required in SYS-8ENT-DVE4 and SYS-16ENT-DVE6 models.
5	Power LED indicator	**10**	Backup battery, CR2032

*Not used

What's included

Access Control Core

Power cable

Bracket and push-in fasteners

Tamper sensor wire (optional)

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 32)
- The support of a legacy access control panel for mobile gateway (see Wiring to legacy panels and mobile gateway on page 19)

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 Alta Access, 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.

Enclosure requirements

- The Access Control Core and Avigilon expansion boards are installed in an Avigilon Smart Hub with pre-installed power supply.

  The Avigilon 4-Door Smart Hub (SYS-4ENT-DVE1) is used as an example throughout this guide. For other Smart Hubs, see For more information on page 33.

- The Access Control Core, and Mercury controller and subpanels, are installed in a LifeSafety Power® enclosure.

  For more information about third-party enclosures, refer to vendor documentation.

Installation

Specifications

For the Access Control Core specifications and dimensions, see the OP-CR-ACC datasheet.

Note: All national and local electrical codes apply when installing this device.

Avigilon reader wiring requirements

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).

ACU and Wiegand reader wiring requirements

Table 1 Connections from Avigilon ACU to Avigilon reader

Pigtail color	Short name	Full name
Gray	GND	Ground (RTN)
Blue	+B	RS485-B
Violet	-A	RS485-A
Orange	VIN	+12V IN

Table 2 Connections to third-party Wiegand reader (optional)

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

Pigtail color	Short name	Full name
Brown	LED	Wiegand LED
Yellow	BUZZER	Wiegand Buzzer

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

Recommended maximum cable length: 300 ft (91 m) with CAT6 or 500 ft (152 m) if two wire pairs are used for GND and VIN (power).

For shielded wiring: Connect one side of the drain wire (the shield around the wires) to the GND terminal on the ACU. Both the shield and the GND wire can share the same GND terminal. Do not connect the other side of the shield to anything.

> **Note:** For elevators, all relays and readers must be connected to the same ACU. If you need more than four access controlled floors or readers, add the 16 I/O Elevator Board.

> **Warning:** Always remove power from the ACU and locking hardware when wiring Avigilon readers and other devices. Failure to do so can damage the ACU.

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.

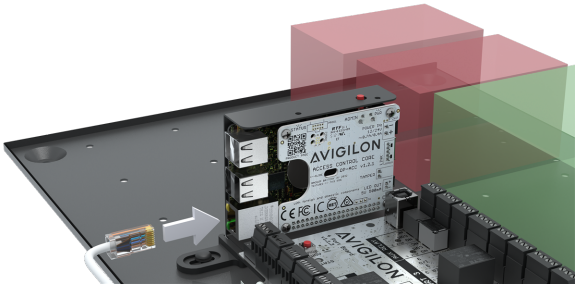
Standard configuration

Wiring the Access Control Core in a Smart Hub

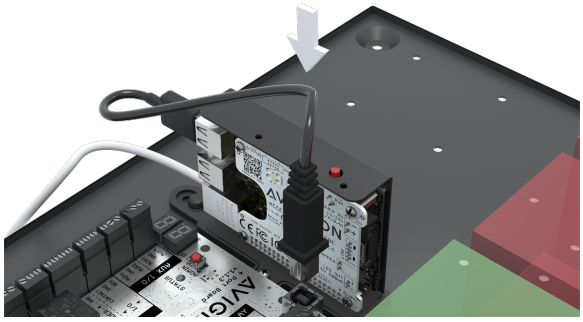
Smart Hubs are shipped with power supplies pre-installed, but the Avigilon boards must be installed separately.

Example: 4-Door Smart Hub

1. Connect the Access Control Core to an Ethernet cable with internet access.

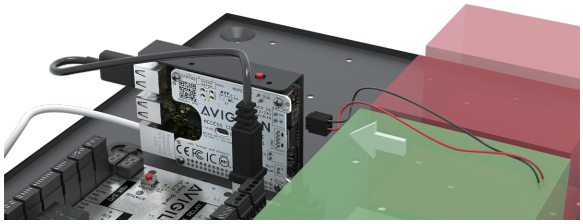


2. Connect the Access Control Core to an Avigilon expansion board using the USB cable.

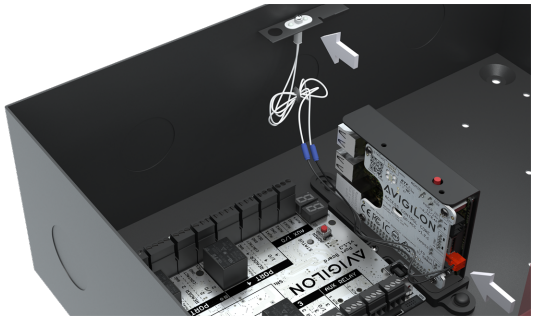


3. Connect the Access Control Core to a power supply using the included power cable.

> **Warning:** Do not apply power during wiring. Ensure the power supply is unplugged until all wiring is complete.



4. Optional. To monitor tamper events, attach the included tamper wire to the tamper switch on the enclosure and plug into the Access Control Core.



Advanced configuration

Mercury device installation

Mercury devices can be installed to manage entries where third-party Wiegand and OSDP readers are installed.

- Up to 8 entries for the MP Series MP1501 and LP Series LP1501 intelligent controller models
- Up to 32 entries for the MP Series MP1502 and MP2500, and LP Series LP1502 and LP2500 intelligent controller models

Prerequisites

Before you start, see:

- Enclosure requirements on page 8
- Mercury device installation in Third-party documentation on page 33

> **Note:** Avigilon Alta Access supports only the Mercury devices below. Other device models might not operate as described in this guide.

Supported devices

Mercury devices are added in Alta Access as follows.

- Mercury MP Series or LP Series controllers are added as expansion boards and must connect to the Access Control Core.
  - MP1501, MP1502, MP2500, LP1501, LP1502, LP2500
- Mercury Series 3 subpanels are added as expansion boards and must connect to the MP Series or LP Series controller.
  - MR50-S3, MR52-S3B, MR16IN-S3, MR16OUT-S3
- Third-party Wiegand and OSDP readers are added as inputs.
  - One expansion board port supports one Wiegand reader.
  - One expansion board port supports two OSDP readers.
- Door contact sensors that report open/close status are added as contact sensors.
- REX inputs that report events to our system are added as REX inputs.

> **Note:** Alta mobile credentials can be issued to users in Alta Access and used to unlock their entries using the Avigilon Alta Open mobile app.

System requirements

- Ensure the SIO baud rate is set to 38400 or higher on the board, and matches the baud rate in Alta Access for TLS support.

  This is required if you are connecting a Mercury Series 3 subpanel to an MP Series or LP Series controller.

- Ensure the bit raw read on the Wiegand or OSDP reader is set to 64-bit for accurate DESFire® card reads.
- Custom reader wiring is needed to support BZR and LED. The Wiegand reader LED control requires:
  - Wiring the Green LED output to the LED input
  - Wiring the Red LED output to the BZR input on a Mercury reader port

  If the LED wires are not wired as specified, you will hear a single beep and see a Green LED blink for any card scans that result in a grant or denial.

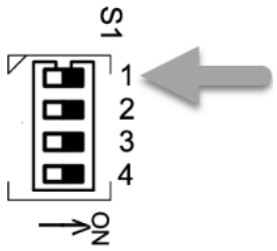
Installing and configuring controllers and subpanels

> **Tip:** A subpanel can be pre-configured before installing the controller. For information about installing a subpanel and using two-conductor RS-485 wiring to connect to Wiegand and OSDP devices, see Mercury device installation in Third-party documentation on page 33.

1. Connect the controller to a power supply using a power cable (not included).

   For the power selector details, see vendor documentation.

2. Connect the controller to the LAN using an Ethernet cable (not included).
3. Move the S1 (or SW1) DIP switch on the controller to the ON position. Example: LP1502



   This operating mode allows you to log in to the web interface of the controller.

   > **Note:** You can skip this step for a previously provisioned controller.

4. Log in to a computer on the same network as the Alta Access network.

   The default IP address for controllers and panels is `192.168.0.251`. For more information, see the factory settings of the device model in vendor documentation.

   > **Important:** Assigning unique IP addresses to controllers is recommended during initial setup.

5. Open a web browser and type `192.168.0.251` in the address bar to access the Configuration Manager.

Or, type the unique IP address for a previously provisioned controller.

6. In the **Username** field, type `admin`. In the **Password** field, type `password`. Click the **Login** button.

   > **Important:** Creating user accounts in the Users menu is recommended during initial setup.

7. When logged in, select **Network** in the left menubar.

   a. Select **Use Static IP configuration** to ensure the IP address doesn't change at a later time.

   Set the **IP Address**, **Subnet Mask**, and **Default Gateway**.

   b. Select **DNS Settings** to set the appropriate settings for communication on the LAN.

   > **Note:** The controller or subpanel must be on the same subnet and LAN segment as the ACU it will connect to. Document the IP address for Alta Access setup.

8. Select **Host Comm** in the left menubar.

   a. Change **Communication Address** to **2**.

   b. Leave the default **Port Number** as **3001**.

   c. Set **Data Security** to **TLS Required**.

   > **Note:** Adding the **Network port** and enabling the **TLS Enabled (Recommended)** checkbox in Alta Access are required when you create the ACU in later steps.

9. Ensure the **Allow All** button is selected.
10. Select **Apply Settings** in the left menubar to save the changes to the controller.
11. Select **Log Out** in the left menubar to close the web interface.
12. Return the S1 (or SW1) DIP switch to the OFF position on the controller.

Assign Wiegand or OSDP readers to entries

1. Go to control.openpath.com/login and sign in. For access in the EU, go to control.eu.openpath.com/login.
2. Go to **Sites** > **Entries**, and create or edit an existing entry.

   For more information on creating entries, see the Avigilon Alta Access Administrator Guide .
3. In the **Controller** field, select the Access Control Core.
4. Assign the contact sensor, REX device, or reader to the entry.

   - In **CONTACT SENSOR**, select the Mercury controller or subpanel expansion board in **Port** and other relevant settings.

- In **ENTRY/EXIT DEVICES**, select the Mercury controller or subpanel expansion board in **Port** and other relevant settings.
- In **REQUEST TO EXIT**, select the Mercury controller or subpanel expansion board in **Port** and other relevant settings.
- In **THIRD PARTY READER - WIEGAND**, select the Wiegand reader in **Port**, and enter the **OSDP address** and **Baud rate**.
- In **THIRD PARTY READER - OSDP**, select the OSDP reader in **Port** and enter the **OSDP address** and **Baud rate**.

5. Click **Save**.

Change input and output types

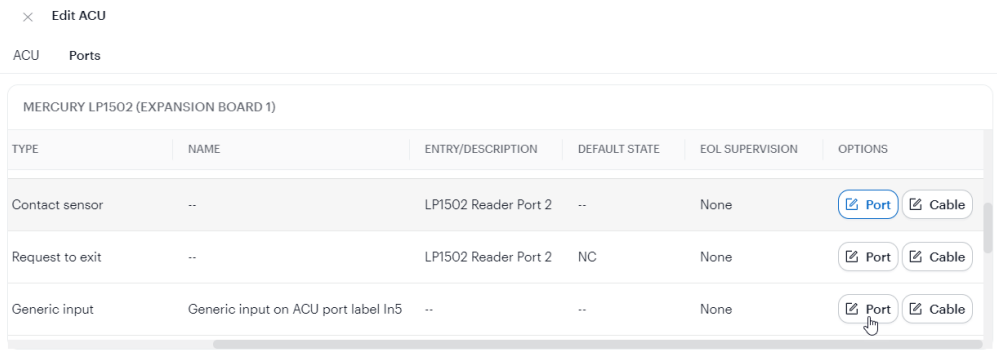
While inputs and outputs (I/O) on the 4-Port Board and 8-Port Board are labeled REX and CONTACT by default, you can use these I/Os interchangeably or as generic inputs, by configuring their type in Alta Access. You can also change them to Wiegand inputs, which requires a few extra steps. For more information, see Wiring to Wiegand devices on Smart Hubs on page 18.

Reader and input ports on the Mercury boards can be configured in Alta Access to support third-party Wiegand or OSDP readers. See the examples below.

Change input types in Alta Access

1. Go to control.openpath.com/login and sign in. For access in the EU, go to control.eu.openpath.com/login.
2. Go to **Devices** > **ACUs** and click the ACU to edit it.
3. Click the **Ports** tab.
4. Scroll to the right and click **Port** next to the input to be configured.

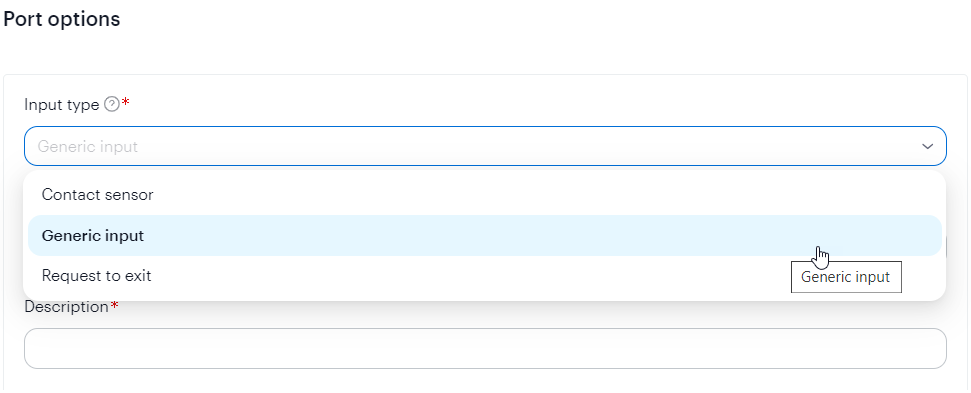
   Example: Mercury board



5. Select a different type from **Input type**.

   For an Avigilon board, click **Input type** to change a **Contact sensor**, **Openpath reader**, **Request to exit** device, **Wiegand device**, or **Generic input** to a different input type.

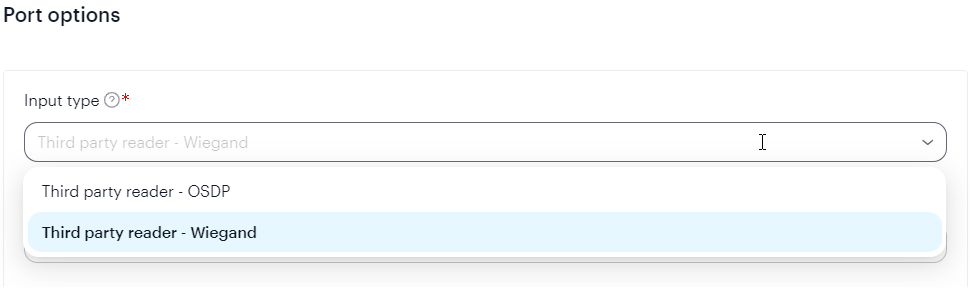
   For a Mercury board, click **Input type** to select **Contact sensor**, **Generic input**, or **Request to exit** device.



Note: Inputs cannot be changed if they are already assigned to an entry.

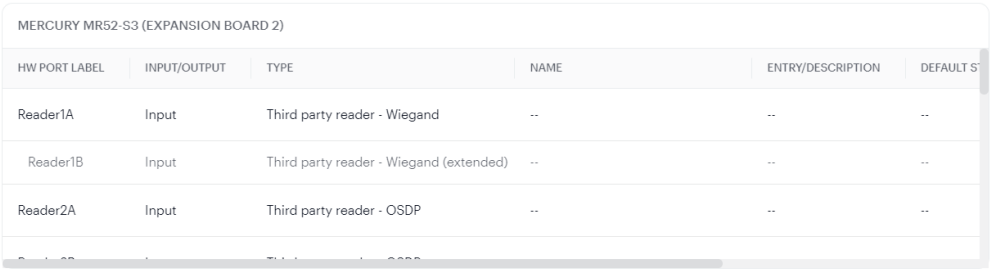
6. *For a Mercury board.* In the reader expansion board section, scroll to the right and click **Port** .

   In **Input type**, select **Third party reader - OSDP** or **Third party reader - Wiegand**.



Note: After the reader port is set to OSDP, ensure the reader is also set up for OSDP communication. For more information about reader configuration, see vendor documentation.

7. Click **Save**.

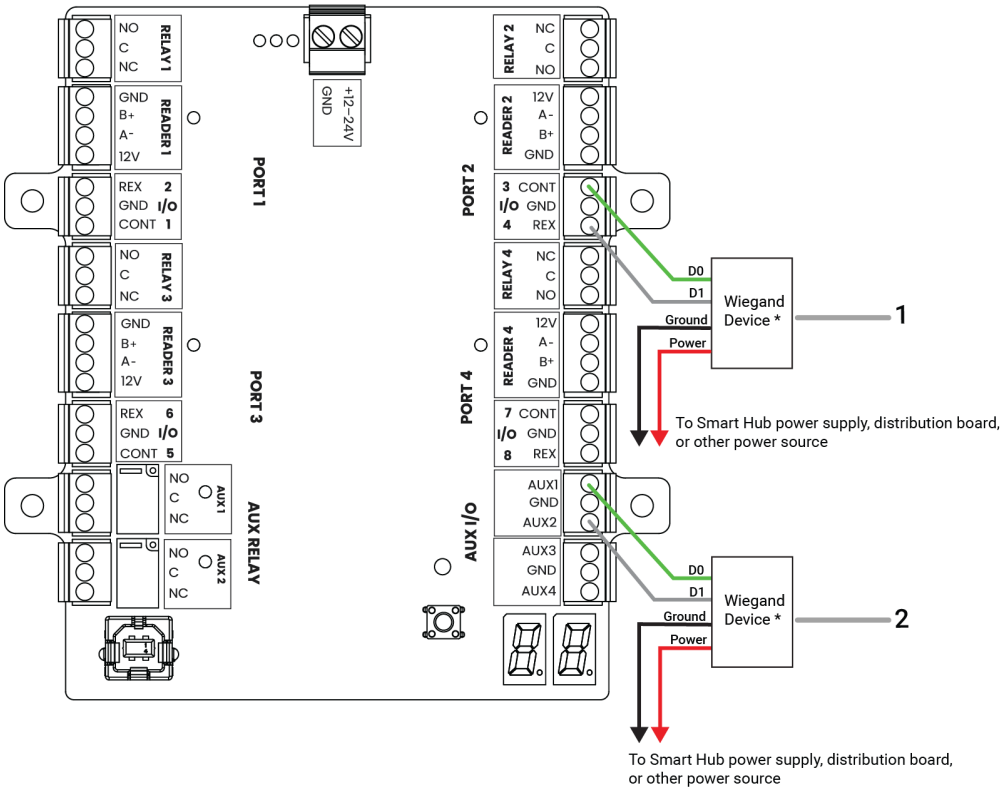


The **Third party reader - Wiegand (extended)** setting (read-only) represents a second Wiegand reader port which is never used.

For the next step, see Provision the ACU using Alta Access on a laptop on page 27.

Wiring to Wiegand devices on 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 (shown below) and 8-Port Board can be used for wiring Wiegand devices (see 2 below), however, any I/O pair may be used including Contact and REX inputs (see 1 below).



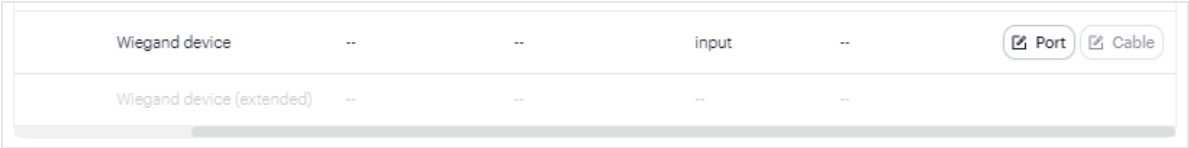
*LED and BZR connections are not supported.

Configure Wiegand devices in Alta Access

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

      This will label the subsequent input as **Wiegand device (extended)** and disable it from editing.

      > **Note:** 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 Alta Access 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 Access Administrator Guide.

Wiring to legacy panels and mobile gateway

Example: Avigilon boards

In this configuration, the legacy panel controls all locking hardware and entry mechanisms while the Alta access control system lets you use the Alta Open mobile app, Smart Reader, and Wave to Unlock functionality.

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 input and output types on page 1 to configure the ACU as output to the legacy panel and Configure Wiegand devices in Alta Access on the previous page.
2. If existing Wiegand readers use a proprietary card format, they can be wired to new Smart Readers. Otherwise, replace existing readers with Smart Readers.

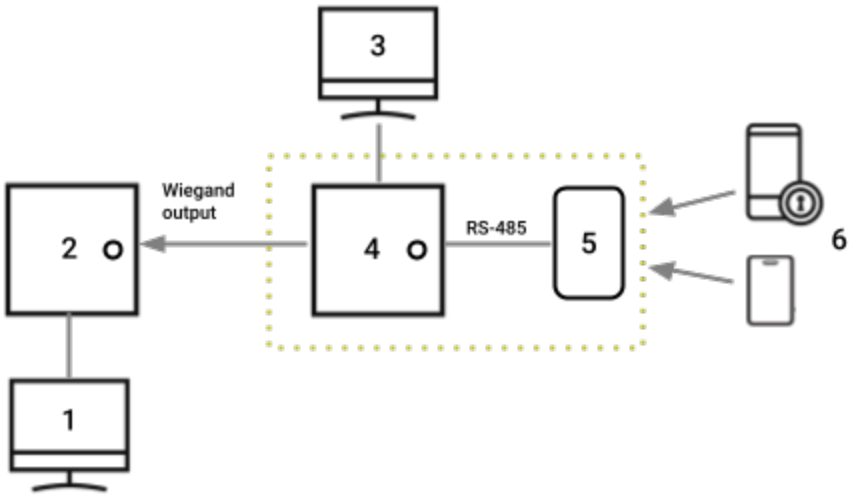


Figure 1 Wiring ACUs to legacy panels and legacy software

1	Legacy access control system software
2	Legacy access control system panel
3	Alta Access
4a	Smart Hub ACU installed between the Smart Reader and the legacy panel **Note:** The Pro series reader does not require a controller, however, a Smart Hub is required to support locking hardware.
4b	Wiegand port configured as output to the legacy panel For more information, see advanced wiring configuration.
5	Smart Readers If existing Wiegand readers use a proprietary card format, they can be wired to new Smart Readers. Otherwise, replace existing readers with Smart Readers.
6	Avigilon Alta Open mobile app, Cloud Key credentials and Wave to unlock functionality Avigilon credential with default gateway number or Wiegand ID

Provisioning

Provisioning the ACU means registering it in Alta Access and running the latest firmware. You will need to re-provision in the case of a hard reset, see Resetting ACUs on page 31.

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

Prerequisites

- Connect the ACU to a power supply using the included power cable.

  Meet all Network requirements on page 7.

- Connect the ACU to the internet using the Ethernet cable.

  > **Note:** The expansion boards must be on the same subnet and LAN as the ACU it connects to.

- Install the Alta Access mobile 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.

Add ACUs using Alta Access

> **Tip:** You can choose to add ACUs using the Alta Access mobile app.
>
> 
>
> 
>

For more information, see this Alta Access article.

Add multiple ACUs using Quick start option

> **Note:** Bulk ACU creation is not supported for the Access Control Core that connects to Mercury expansion boards. These ACUs must be created one at a time.

1. Go to control.openpath.com/login and sign in. For access in the EU, 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:
        - **Openpath 4-Port Expansion**
        - **Openpath 8-Port Expansion**
        - **Openpath 16-Port Elevator**

    > **Tip:** The Avigilon (formerly, Openpath) boards are most common with the Core Series Smart Hub.
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 Avigilon (formerly, Openpath) boards are most common with the Core Series Smart Hub.

   - **Openpath 4-Port Expansion**
   - **Openpath 8-Port Expansion**
   - **Openpath 16-Port Elevator**
   - **Mercury LP1501**
   - **Mercury LP1501 (With Downstream)**
   - **Mercury LP1502**
   - **Mercury LP2500**
   - **Mercury MP1501**
   - **Mercury MP1501 (With Downstream)**
   - **Mercury MP1502**
   - **Mercury MP2500**

> **Note:** For the Mercury controller board, enter also their unique **IP address** and **Network port** (default is `3001`). **TLS Enabled (Recommended)** is enabled by default.
>
> If you select **Mercury MP1501 (With Downstream)** or **Mercury LP1501 (With Downstream)**, ensure the baud rate matches the baud rate on the physical board (default is `38400`).

6. Click **Add board**. The Mercury board is disabled by default.
   a. When you are ready to open communication to the Mercury board, ensure it is disconnected from any previous access control system.
   b. In the ENABLE column, select **Enabled** for the selected board.

> **Caution:** The previous configuration on the legacy access control system will be overwritten.

7. If you have additional subpanels, click **Add board** again and add the appropriate types.
   - **Mercury MR16IN-S3**
   - **Mercury MR16OUT-S3**

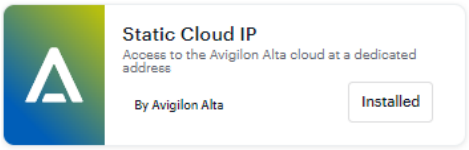
- **Mercury MR50-S3**
- **Mercury MR52-S3**

> **Note:** For the Mercury readers and panels, enter also the **Port** and **RS-485 address** (supported range is `0 – 31`).

8. 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.

   > **Note:** An Enterprise plan is required to use Static Cloud IP.

   a. Go to **App marketplace** and ensure the **Static Cloud IP** app is installed.

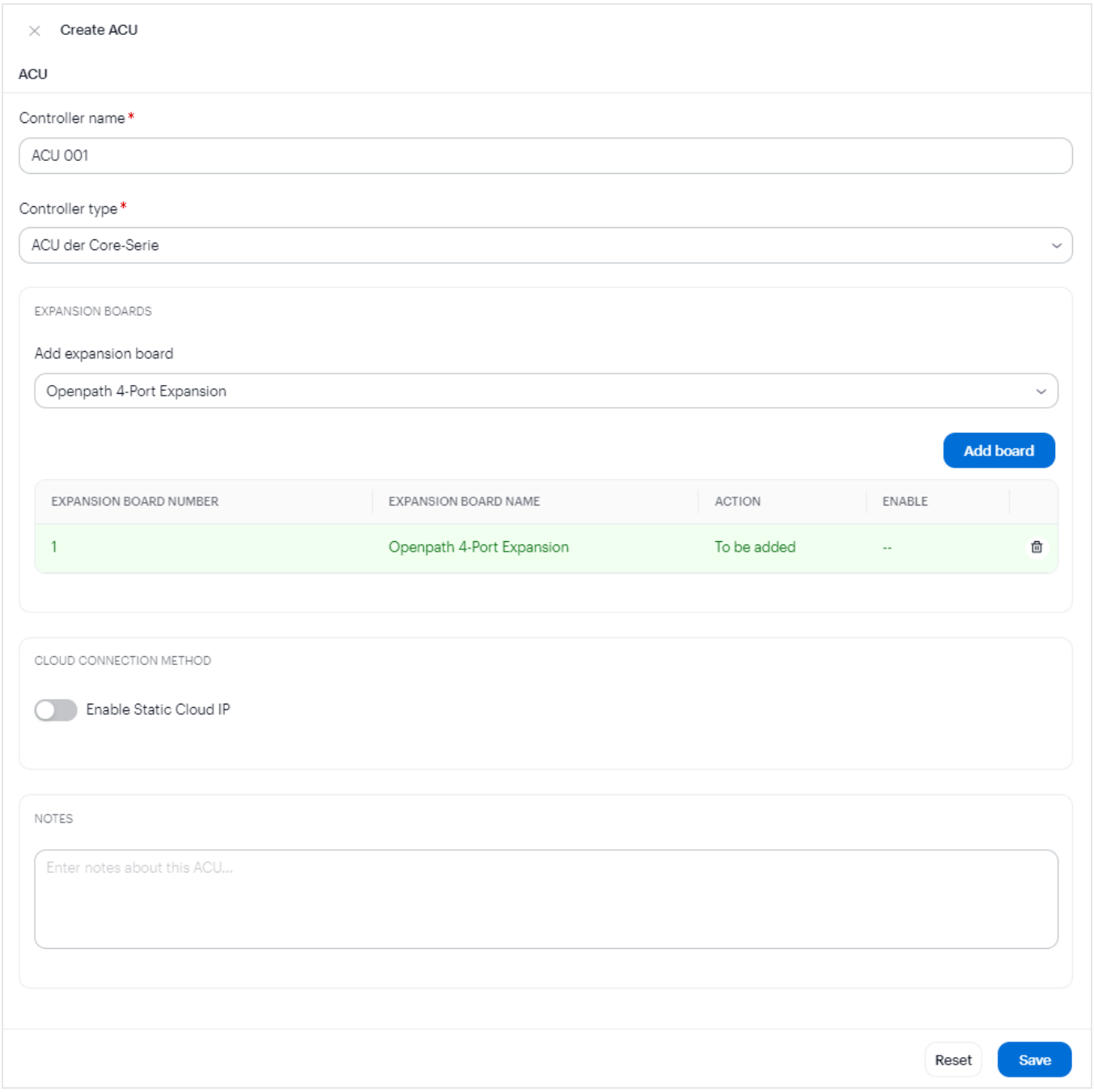
   

   b. After the toggle is enabled in Alta Access, open the Alta Access mobile app and select **Provision with Static Cloud IP** to provision the devices.

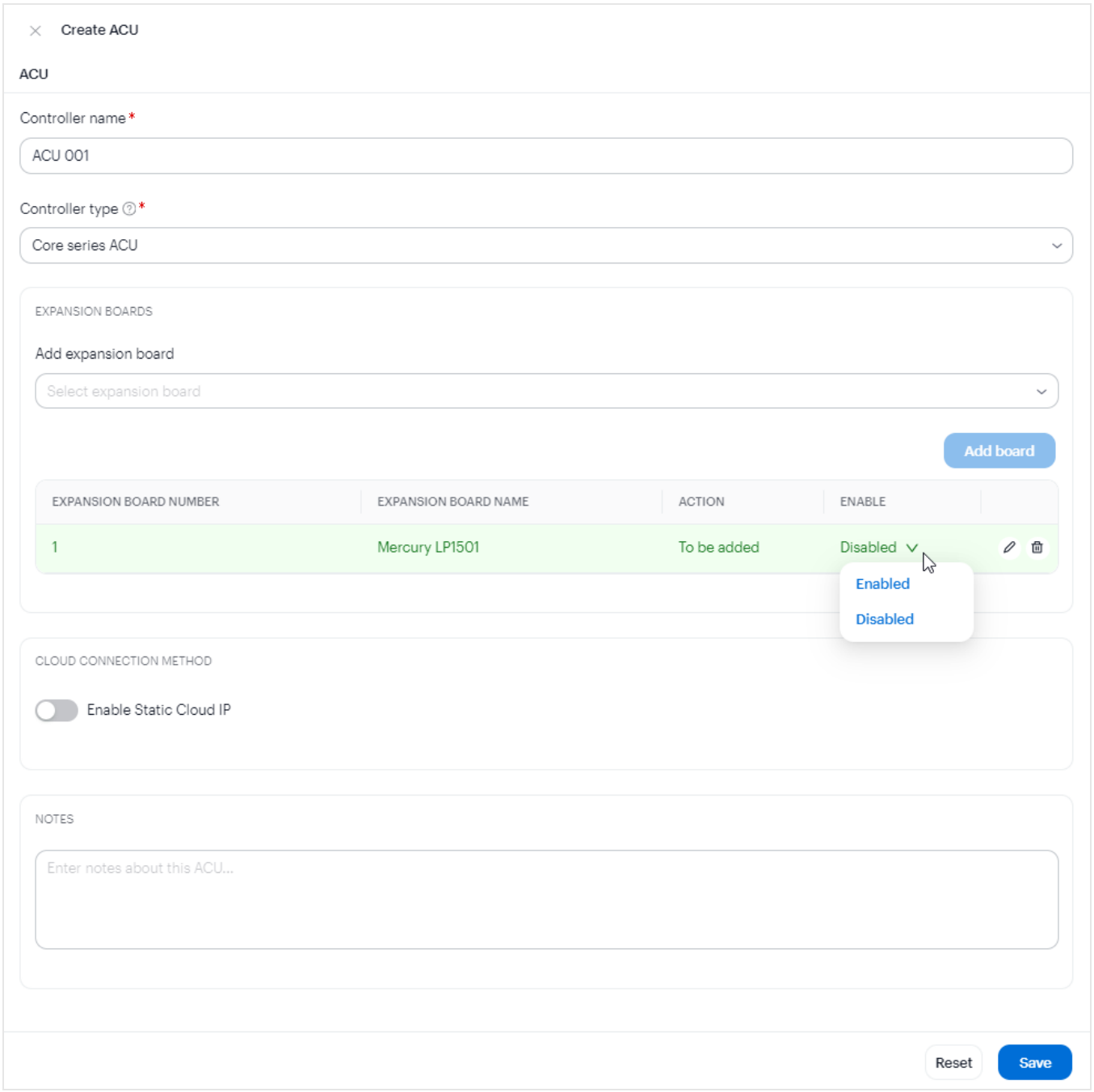
9. Click **Save**.

> **Note:** If you are saving a new Mercury expansion board, Access Control Core firmware will automatically download and install for up to 30 minutes, depending on network speed.

Example: Avigilon expansion board connected to an ACU



Example: Mercury expansion board connected to an ACU



Provision the ACU using Alta Access mobile app (recommended)

> **Note:** Mobile app provisioning is not applicable to the Access Control Core that connects to Mercury boards and subpanels.

1. Log in to the Alta Access mobile app using your mobile credential.
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 Access Control Core.
4. In the Alta Access mobile 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 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 Alta Access), and then tap **Yes** to proceed.
8. The app will send notifications when the ACU provision state changes from **Unprovisioned** to **Provisioning in progress**, and then to **Provisioning complete**.

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

Provision the ACU using Alta Access on a laptop

1. Go to control.openpath.com/login and sign in. For access in the EU, go to control.eu.openpath.com/login.

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

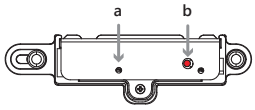
2. Go to **Devices** > **ACUs**.
3. Locate your ACU on the list.
4. If you don't see your ACU listed, create a new one:
   a. Click the + button in the upper-right corner.
   b. Enter a unique name for the ACU.

c. In **Controller type**, select the controller and any appropriate expansion boards in the other fields.

d. Click **Save**.

> **Note:** If you are saving a new Mercury expansion board, Access Control Core firmware will automatically download and install for up to 30 minutes, depending on network speed.

5. On the ACU, press the Admin button.



6. In Alta Access, 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 7.

      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 doesn't appear, contact Avigilon Alta Support at (844) 673-6728 Ext 2 or support@openpath.com.

Test internet connection using Alta Access mobile app

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

Configure network settings using Alta Access mobile app

In the Alta Access mobile app, you can configure network settings for the ACU. Ethernet connections can be DHCP (default) or can have a static IP address.

> **Note:** Setting DHCP reservation and a static IP address are recommended to support allowlisting or safelisting of the same address during a reboot of the Access Control Core (when new IP addresses are assigned).

Change network settings

1. Connect to the Access Control Core device 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.

Status LED indicator

The Status LED on the Access Control Core 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	The Access Control Core is updating software. Indicates when the Access Control Core has been online for less than 24 hours. 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.
	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 Alta Access mobile app.
	Blinking purple	The Access Control Core is ready to connect to the Alta Access mobile app.
	Blinking red	The Access Control Core is not connected to the internet.
		The Access Control Core configuration is being updated and saved in Alta Access. The device continues to operate as expected. 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.
	Solid red	The Access Control Core is in an error state. Go to the  Devices dashboard in Alta Access for more information.

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.

Resetting ACUs

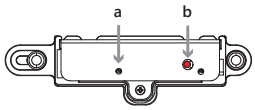
Soft reset

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).



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 21.

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 Mullion Smart Reader Embedded USB Smart Reader	0.14A
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 x 3 hours = 6AH, so two 12V 6AH sealed lead acid (SLA) or gel cell batteries wired in series.

Mercury device installation

Note: For Mercury subpanels and third-party Wiegand and OSDP readers, you need to calculate the power draw to obtain the applicable battery size.

For more information

Technical support

For additional support documentation, see support.avigilon.com.

Product documentation

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

Third-party documentation

Mercury hardware:

- MP1501 Installation Manual, MP1502 Installation Manual, MP2500 Installation Manual
- LP1501 Installation Manual, LP1502 Installation Manual, LP2500 Installation Manual
- MR50-S3 Installation Manual, MR52-S3B Installation Manual, MR16IN-S3 Installation Manual, MR16-OUT-S3 Installation Manual

Avigilon warranty

Warranty terms for Avigilon products are provided at avigilon.com/support/warranty.

Regulatory notice

All national and local electrical codes apply.

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

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.
- 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.

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.

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

Electrical specification

Electrical	
Operating Voltage	12-24VDC
Operating Current	0.7A @ 12VDC 0.4A @ 24VDC