

AVIGILON™

Single Door Controller

Installation guide | OP-CR-SDC

Contents

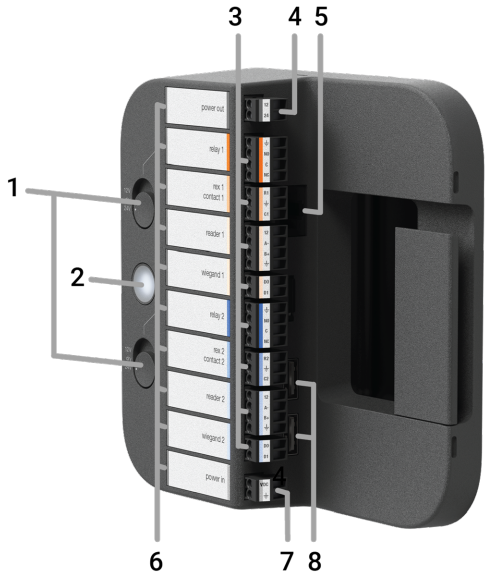
Before you start 4
Overview 4
What's included 5
Conducting site surveys 5
Network requirements for Alta Access devices 5
Ethernet connection and firewall configuration 5
Wi-Fi unlocking configuration 6
Installation 7
Specifications and dimensions 7
Mounting 10
Standard SDC wiring configuration 12
Avigilon reader wiring requirements 13
ACU and Wiegand reader wiring requirements 14
Wiring fail-safe and fail-secure lock hardware 15
Tamper alert setup 15
Advanced configuration 16
Legacy wiring 16
Voltage switches 16
Provisioning 17
Prerequisites 17
Add SDCs using Alta Access 18
Add multiple SDCs using Quick start option 18
Add one SDC 18
Static Cloud IP 20
Provision the SDC using Alta Access mobile app 23
Create and provision the SDC using Alta Access mobile app (recommended) 25
Test internet connection using Alta Access mobile app 25

Configure network settings using Alta Access mobile app 26
Change network settings 26
Set up Wi-Fi on the SDC 26
LED indicators 28
Status LED indicator 28
Port LED indicators 29
Maintenance 30
Selecting a backup battery 30
Troubleshooting the Avigilon Single Door Controller 31
Faulty reader or port 31
SDC offline 32
Typical causes and recommended solutions 32
Appendix 34
Best practices - Wiring a REX to your Alta access control system 34
Wiring REX in series with mag lock or other fail-safe hardware 34
Wiring REX with Video Reader Pro and Video Intercom Reader Pro 34
Regulatory notice 36
More information 38
Technical support 38
Product documentation 38
Avigilon warranty 38
Revisions 39

Before you start

The Avigilon Single Door Controller is a compact access control unit (ACU) that controls up to two entries and two Avigilon readers. This installation guide explains how to install and configure the Single Door Controller as part of the Alta access control system.

Overview



1	2 x Wet/Dry relay selections
2	Admin button, Status LED indicator
3	2 x ports for Avigilon readers 2 x ports for Wiegand readers 2 x ports for REX sensors 2 x ports for relays 2 x ports for contact sensors
4	Power output
5	Ethernet port
6	Port LED indicators
7	Power input
8	USB ports (future use)

What's included

Single Door Controller



Cover



Mounting backplate



Drywall anchors



Electrical box screws



Set screw for securing SDC to backplate

Self-tapping screws



Hex key for set screw



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
- Any backup batteries for the Single Door Controller (see Selecting a backup battery on page 30)
- The support of a legacy access control panel for mobile gateway

Network requirements for Alta Access devices

Ethernet connection and firewall configuration

Connection to LAN

- Use an Ethernet connection with DHCP to connect the Single Door Controller to the local area network (LAN).

Firewall settings

- Configure firewall settings to communicate with Alta Access.
- Required outbound ports:

- TCP port 443
- UDP port 123 - Add pool.ntp.org to the allow list for the NTP port

Additional firewall considerations

- Fortinet firewalls have anti-virus software that blocks AWS traffic by default. AWS must be on an allowlist.
- If using an external DNS, outbound UDP 53 must be open.
- Inbound port forwarding on the router, firewall, or NAT device is unnecessary.
- HTTPS certificate rewriting or TLS/SSL inspection is not allowed.

IP address and network segregation

- Alta Access does not provide an IP range or FQDN list of hostnames for Basic and Premium licenses. Most hostnames resolve to dynamic IPs and change during provisioning and configuration updates.
- To segregate traffic from Alta Access controllers, enable a DMZ for the controllers.

Static Cloud IPsetting — for Enterprise licenses

- Alta Access offers Static Cloud IP for organizations with strict firewall network policies. This simplifies opening a few IP addresses to allow the SDC to connect to the cloud.

  For more information about Static Cloud IP, see the Alta Access web app guide.
- The latest version of the Alta Access mobile app supports provisioning SDC devices behind restricted firewalls.

Wi-Fi unlocking configuration

To support Wi-Fi unlocking using the Alta Open mobile app:

- The inbound TCP port 443 of the SDC must be available from within the LAN. Inbound port forwarding on the router, firewall, or NAT device is not required.

The SDC also supports Wi-Fi connections. See Configure network settings using Alta Access mobile app on page 26.

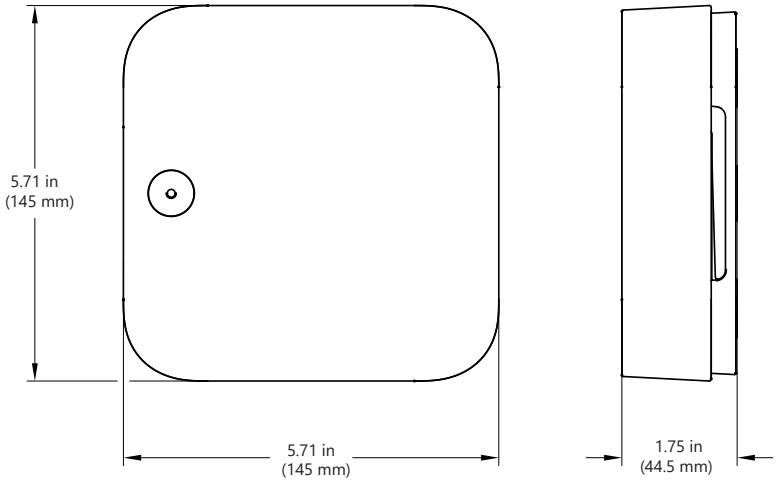
Installation

Specifications and dimensions

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

System	
Access Control	Up to 2 entries and 2 Avigilon Smart Readers
Relays	2 relays, 2A @ 24VDC (resistive)
Avigilon Readers	Up to 2 Avigilon Smart Readers
Wiegand Readers	Up to 2 Wiegand readers
REX Sensors	2 REX sensors, nominal 5VDC, 1kohm to each input (resistors built into controller)
Contact Sensors	2 contact sensors, nominal 5VDC, 1kohm to each input (resistors built into controller)
Tamper Sensor	Detects tamper events when front cover is removed
Backup Battery	May be added to PoE injector or optional external supply
Communications	10/100 baseT Ethernet port, or 2.4 GHz and 5 GHz WiFi, for connection to access control cloud service Encryption to access control cloud service uses TLS 1.2+ 2 USB ports (future use) RS-485 for connection for readers
Display	Port LED indicator: Avigilon Smart Reader in expected or error state; sensor in active state, or EOL shorted or cut; lock hardware including relay in energized or fault detected state Status LED indicator: Internet connection status, software update status,

System	
	provisioning status in access control system

Mechanical	
Dimensions	
Weight	12.7 oz (360 g)
Mounting	Wall-mounted or installed on US single-gang or double-gang box, or EU-standard gang-box
Wiring	Industry standard RS-485 signaling to communicate with readers over standard wiring Removable contact terminal blocks for convenient wiring Physical switches to select relays to be dry or wet (12V or 24V) EOL monitoring with single or double termination on all REX and Contact inputs

Electrical	
Supply Requirement	PoE, PoE+, or external 12-24VDC **Note:** When using an external supply, if 24V wet relay output is required a 24V external supply must be used. ⚠ Certified external power source (complies with LPS) must be used.

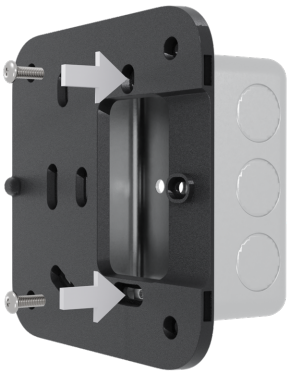
Electrical	
	Tip: When using PoE or PoE+, simplify cabling by using one cable for both power and data. Use the POWER IN on the SDC for a backup battery.
External Supply Rating	12V @ 2.2A min. or 24V @ 1.1A min.
Output Ratings	Power Out can supply up to 100mA @ 12V or 50mA @ 24V
	2 reader ports, max power output: 250mA @ 12V each
	2 relays, max power output: PoE: Max 3W combined output (250mA @ 12V, 125mA @ 24V) PoE+: Max 9W combined output (750mA @ 12V, 375mA @ 24V)

Environmental	
Operating Temperature	0°C to 50°C (32°F to 122°F)
Operating Humidity	5% to 85% relative, non-condensing

Regulatory	
Certifications	CE (Europe), IC (Canada), FCC (United States), NOM (Mexico), RCM (Australia, New Zealand), RoHS, UKCA (United Kingdom), ANATEL (Brazil), UL 294* *Performance Levels: Attack Level I, Endurance Level I, Line Security Level I, Standby Power Level I

Mounting

1. Attach the backplate to a US single-gang or double gang box using the included electrical box screws (two or four screws, respectively), or EU-standard gang box.



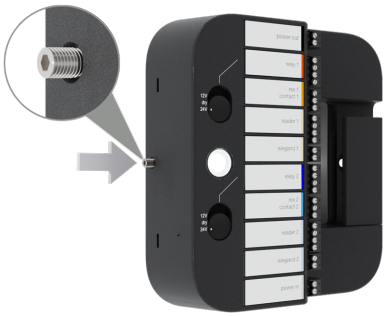
> **TIP:** Use the included drywall anchors and self-tapping screws on drywall for added stability.

2. Snap the Single Door Controller onto the backplate. Ensure the side clips on the backplate (a) fit into their notches on the back of the controller (b).

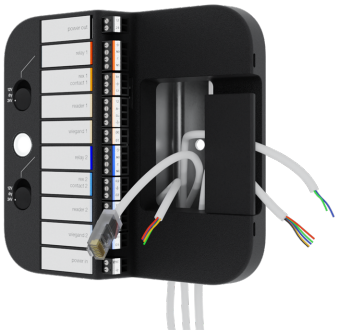




3. Use the included hex key to tighten the pre-installed set screw on the Single Door Controller to secure it to the backplate.



4. Wire the Single Door Controller. Use the cable slot to hold cables while wiring.



> **WARNING:** Do not apply power during wiring to prevent injury. Ensure the power supply is unplugged until all wiring is complete.

5. Snap on the cover.



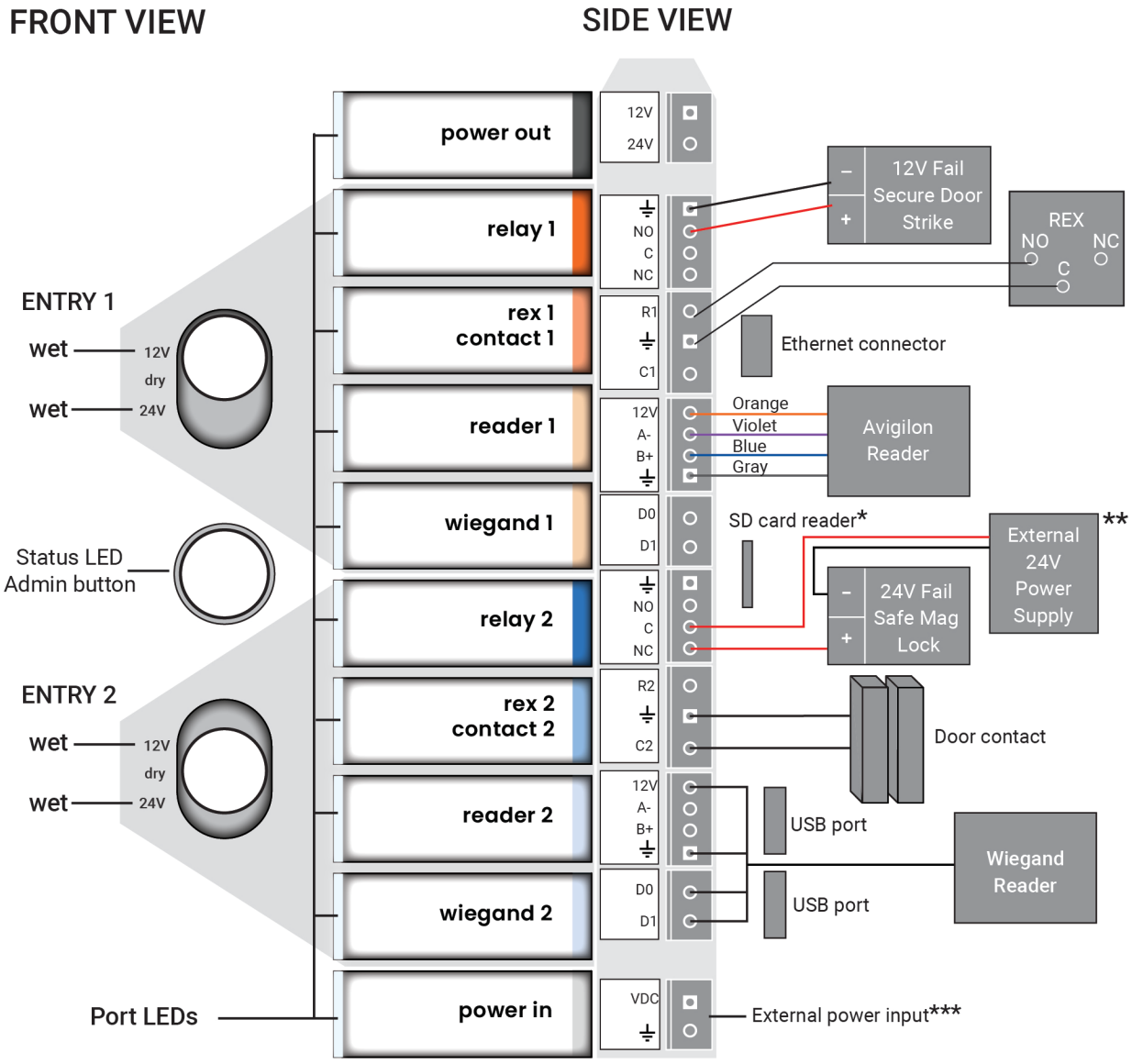
> **NOTE:** Removal of the front cover will trigger tamper detection during normal operation.

6. Apply power using either DC or PoE.



Example: North American power cord and outlet

Standard SDC wiring configuration



* SD card must not be removed unless instructed by Avigilon Alta Support.

** 24V locking hardware requires PoE or a 24V power supply.

*** For backup or if PoE not available. 12V @ 2.2A (min) or 24V @ 1.1A (min). 24V required if locking hardware requires 24V.

> ⚠ **CAUTION:** Certified external power source (complies with LPS) must be used.

Avigilon reader wiring requirements

Compatible wire types

Avigilon readers and the Single Door Controller 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).

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)

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.

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.

ACU and Wiegand reader wiring requirements

Table 1 Connections from Avigilon Single Door Controller 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

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 Single Door Controller. 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 Single Door Controller. If you need more than two access controlled floors or readers, add the 16 I/O Elevator Board.

WARNING: Always remove power from the Single Door Controller and locking hardware when wiring Avigilon readers and other devices. Failure to do so can damage the Single Door Controller.

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 Best practices - Wiring a REX to your Alta access control system on page 34.

Tamper alert setup

The front cover of the Single Door Controller has a built-in tamper sensor and will report tamper events when the cover is removed. You can monitor tamper events using the Tamper detector state changed alert, which is configured in Alta Access. For more information, see the Alta Access web app guide.

Advanced configuration

Legacy wiring

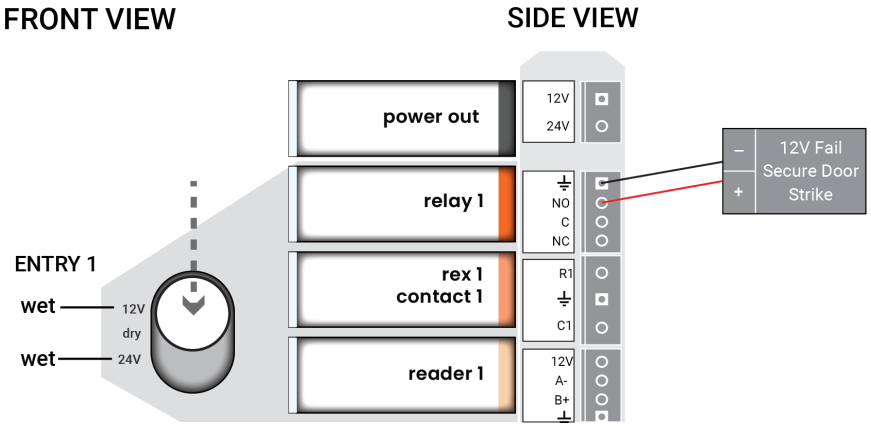
Sometimes legacy wiring (unshielded and straight through, rather than shielded twisted pair, often 22-6) results in slower connections and dropped packets between the Avigilon reader and Single Door Controller. To remedy this, you can switch GND and VIN with +B and -A connections on the SDC and readers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

Voltage switches

WARNING: Remove the DC input power and PoE before changing the voltage of the relays.

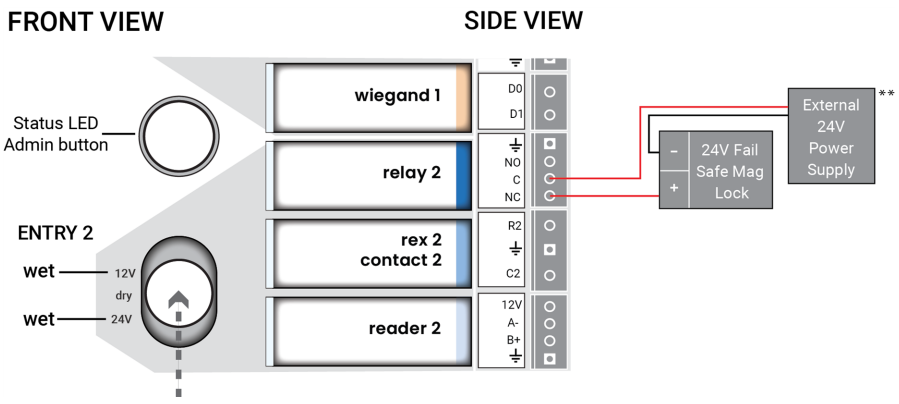
Wet relay example

To power locking hardware without an external supply (Wet Relay), select 12V or 24V, and connect locking hardware to NO and GND for fail-secure locks, or NC and GND for fail-safe locks.



Dry relay example

To use external power, select DRY and use NO or NC and C, and wire to external supply.



** 24V locking hardware requires PoE or a 24V power supply.

Provisioning

Provisioning the Single Door Controller 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 Hard reset on page 1.

> **NOTE:** If you are provisioning Single Door Controllers for a customer account, the customer organization needs to be created first.

> **TIP:** Using the Alta Access mobile app is recommended, which automatically creates and provisions the ACU in Alta Access and adds any connected devices.

Prerequisites

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

  Meet all Network requirements for Alta Access devices on page 5.

- Connect the Single Door Controller to the internet using the Ethernet cable.

  > **NOTE:** The expansion boards must be on the same subnet and LAN as the Single Door Controller 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 Single Door Controller. If you have a VLAN, make sure the laptop is on the same VLAN as the Single Door Controller.
- 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 SDCs using Alta Access

TIP: Using the Alta Access mobile app is recommended, which automatically creates and provisions the ACU in Alta Access and adds any connected devices. If you choose this method, see Create and provision the SDC using Alta Access mobile app (recommended) on page 25.

Add multiple SDCs using Quick start option

1. Sign in to alta.avigilon.com/signin and select the organization in your region.
2. Go to **Admin** > **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 **Single Door Controller (SDC)**.

   NOTE: Expansion board connections are not applicable to SDCs.
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 SDC

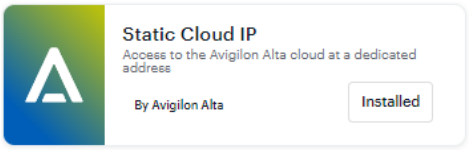
1. Go to **Devices** > **ACUs**.
2. To add a new SDC, click the + button in the upper-right corner.
3. Enter a unique name for the SDC.
4. In **Controller type**, select **Single Door Controller (SDC)**.

   NOTE: Expansion board connections are not applicable to SDCs.

5. Optional. To connect your network to the Cloud using a static IP address and port on an allowlist or safelist, select the **Enable Static Cloud IP** toggle in CLOUD CONNECTION METHOD on the Edit ACU page. Default port is 443.

   > **NOTE:** An Enterprise license is required to use Static Cloud IP for ACU and SDC devices. Static Cloud IP is not supported for video intercom readers and video readers.

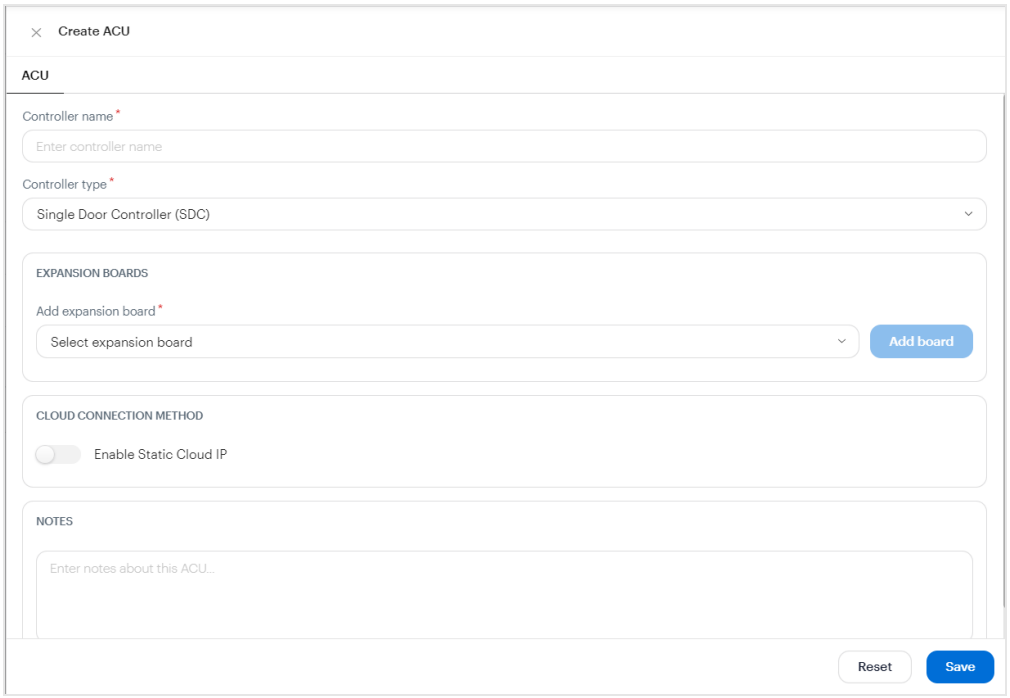
   a. Go to **Apps** and ensure the **Static Cloud IP** app is installed.

   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.

   For more information including network setup, see Static Cloud IP on the next page.

6. Click **Save**.



Static Cloud IP

Static Cloud IP offers a direct connection to the Cloud using permanent IP addresses. This significantly simplifies the configuration and management of network firewall rules, providing a straightforward solution for high-security network needs.

System requirements

- Enterprise license for Alta Access

  > **NOTE:** An Enterprise license is required to use Static Cloud IP for ACU and SDC devices. Static Cloud IP is not supported for video intercom readers and video readers.

- Static Cloud IP app installed from App marketplace
- Alta Access mobile app to provision the SDC device

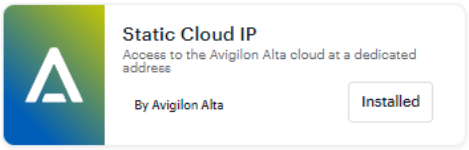
Workflow — Provision SDC devices with Static Cloud IP

1. Obtain an Enterprise license for Alta Access from your integrator.

   The Alta Access Admin requires an Organization created at the Enterprise software level.

2. Create and enable the devices in Alta Access.

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

   b. To connect your network to the Cloud using a static IP address and port on an allowlist or safelist, select the **Enable Static Cloud IP** toggle in CLOUD CONNECTION METHOD on the Edit ACU page. Default port is 443.

   c. Click **Save**.

3. Complete network configuration.

   The customer's network administrator allows the required IP addresses on their site's network firewall.

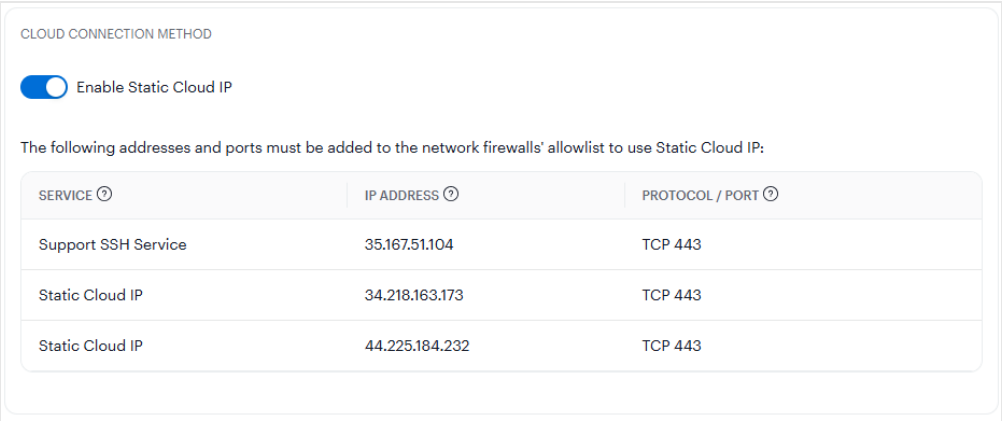
4. Provision the SDC for the first time using the Alta Access mobile app, **Provision with Static Cloud IP** option.

Each controller uses the mobile app internet connection for initial configuration and connection to the Cloud, and then completes normal provisioning through Static Cloud IP.

For more information, see Provision the SDC using Alta Access mobile app on page 23.

Switch provisioned SDC devices to Static Cloud IP

If you already have provisioned the devices, you can switch their connections to use Static Cloud IP.



Important: If your SDC was shipped before July 5, 2023, the Provision with Static Cloud IP option in the Alta Access mobile app will not work. You will need to provision the device as usual, and then go to the Edit ACU page to enable the Static Cloud IP toggle. This will provide the IP addresses you need to add to your network firewall's allowlist.

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.

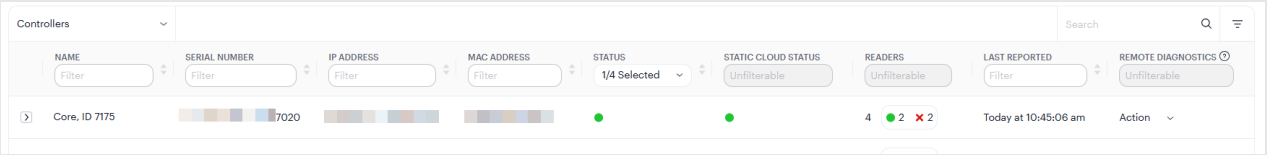
Verify your controllers are using the Static Cloud IP

To find the status of a controller in Alta Access, display the Device dashboard:

1. Go to **Home** and select **Device** in the top-right corner.

   Or, select your custom dashboard.

2. Look in the STATIC CLOUD STATUS column. For example:



Color	Status	Description
●	Connected	The controller or reader is online and communicating as expected.
✕	Disconnected	The controller or reader is offline. The last message received from the controller is more than 20 minutes old.
!	Warning	The last message received from the controller is more than 12 minutes old.
○	Muted	The controller or reader status is undetermined, or is muted in the Device dashboard.

Provision the SDC using Alta Access mobile app

1. If powering using PoE, plug in the Ethernet cable (a). If powering using an external power supply, plug in the Ethernet cable and connect power to the **power in** port (b).



   The Status LED indicator is solid cyan .

2. In the Alta Access mobile app, locate the org to which you're provisioning hardware, either on the list or using search, and then tap on the org name.

3. Wait until the Status LED indicator is solid blue and then press the Admin button on the Single Door Controller.



   NOTE: The Single Door Controller will disconnect from the Alta Access mobile app after 5 minutes of inactivity. Press the Admin button again to reset the timer.

4. When the Status LED indicator is blinking purple , tap on the ACU ending in the last five digits of the serial number in the Alta Access mobile app.

5. When the Status LED indicator changes to solid purple , tap **Test Internet Connection** and wait for a green **YES** to appear before proceeding to the next step.

   NOTE: This checks if the Single Door Controller can ping api.openpath.com.

   If this step fails, see Troubleshooting the Avigilon Single Door Controller on page 31.

6. If the internet connection test is successful, tap **Provision Device** in the app.
7. Tap the ACU name that you want to provision to (this is the name of the SDC you created in Alta Access), and then tap **Yes** to proceed.
8. Optional. Tap **Provision with Static Cloud IP**, if the Static Cloud IP toggle is enabled in Alta Access.
9. When setup is complete, the Status LED indicator will change to solid white .

Create and provision the SDC using Alta Access mobile app (recommended)

1. Install the Alta Access mobile app.

   > **NOTE:** Alta Access mobile app version 2.4.0 or newer is required on iOS 16 or newer, or Android™ 5 or newer.

2. Open the Alta Access mobile app.
3. Tap the + icon in the top-right corner.
4. Fill in the required information.
5. Tap **Create and provision** in the lower-right corner and follow in-app instructions.

For more information about app use, see the Alta Access Mobile App Admin Guide.

When processing is complete, any connected expansion boards are created in Alta Access and the SDC becomes registered on the **Devices** > **ACUs** page.

App Store and the Apple logo are trademarks of Apple Inc. Google Play and the Google Play logo are trademarks of Google LLC.

Test internet connection using Alta Access mobile app

In the Alta Access mobile app, you can tap **Test Internet Connection** to check if the Single Door Controller 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 Single Door Controller. While wired internet connections are preferred, you can configure the Single Door Controller to use Wi-Fi instead. The default interface for the Single Door Controller is Ethernet/wired connection. Ethernet and Wi-Fi connections can be DHCP (default) or can have a static IP address.

The SDC supports 2.4 GHz and 5 GHz Wi-Fi connections.

Change network settings

1. Connect to the Single Door Controller 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 SDC

1. Connect to the Single Door Controller 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**.

TIP: Alta Access Tabletop Demo Display (OP-DEMO2-SDC-RKP) testing

To test your network connection to a Smart Reader on the Tabletop Demo Display, do any of the following:

- Bluetooth test: Disable Wi-Fi on the phone, close the mobile app, touch the reader, and then unlock the reader using the mobile app.
- Wi-Fi test: Disable Bluetooth on the phone and then unlock the reader using the mobile app.

To test without a network connection:

- Disconnect the Ethernet cable and then test the reader using Bluetooth.

To conduct an RTC (Real-Time Clock) module test:

1. Unplug the power supply, wait 10 seconds, and then apply power to the Tabletop Demo Display.
2. Without the Ethernet cable connected, test the reader using Bluetooth.
3. If the reader does not unlock, an issue may have occurred with your RTC. To resolve this issue, contact Avigilon Alta Support.

LED indicators

Status LED indicator

The status LED on the Single Door Controller indicates the following.

Status LED		Description
	Solid white	The SDC is provisioned and functioning normally.
	Solid cyan	The SDC is booting.
	Solid yellow	The SDC is restoring software. Displays when you turn on the SDC for the first time or perform software updates.
	Blinking yellow	The SDC is updating software. Displays when the SDC has been online for less than 24 hours. The duration depends on the type of update and number of devices. For more information, see best practices for successful upgrades in the Alta Access web app guide. **NOTE:** 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	Unprovisioned state. The SDC has finished booting and is ready for provisioning.
	Solid purple	The SDC is connected to the Alta Access mobile app.
	Blinking purple	The SDC is ready to connect to the Alta Access mobile app.

Status LED		Description
☀	Blinking red	No internet. There is a problem with the internet connection. If attempting to set up a device using Wi-Fi, try switching to an Ethernet connection. See Network requirements for Alta Access devices on page 5.
		The SDC configuration is being updated and saved in Alta Access. The device continues to operate as expected. **NOTE:** 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 SDC is in an error state. Go to **Home** > **Device**, and choose **Restart device communicator** from the REMOTE DIAGNOSTICS column. If this doesn't resolve the error, power cycle the SDC, remove power, wait 10 seconds, and reapply power. **NOTE:** If the error persists, contact Avigilon Alta Support.

Port LED indicators

The Single Door Controller has eight port LEDs and two power LEDs. The port LEDs indicate the following.

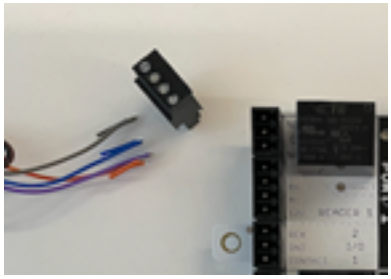
Port LED		Description
Avigilon readers or Wiegand Readers	Solid	Normal operation
	Blinking	Error state
Sensors, including REX and Contact Sensors	Solid	Active
	Blinking	EOL shorted or cut
Lock hardware including relays	Solid	Relay is energized
	Blinking	Fault detection

Maintenance

TIP: To prevent damage to your Avigilon equipment, follow these guidelines:

- Always disconnect power. Whenever possible, turn off the power to the expansion board before connecting or disconnecting any wires. This is the safest way to prevent electrical shorts.
- If power cannot be disconnected:
  - Instead of removing individual wires, detach the entire terminal block from the board.
  - Connect or disconnect wires from the terminal block's screw connectors while it's detached.
  - Once wiring is complete, plug the terminal block back onto the board.

  For example:



Selecting a backup battery

While not required, a backup battery is recommended in case of power outages. For PoE power backup, refer to the manufacturer's instructions for your PoE injector or switch. When using an external supply, 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 3 Example power requirements (24V)

Single Door Controller	.3A
Smart Reader (2)	0.25A
Locking hardware (while engaged)	0.125A – 0.25A

Assuming an external 24V power supply and an SDC configured with two Avigilon readers and locking hardware using about 1.1 Amps, Tto keep the system running for 3 hours with all entries powered, you need 1.1A x 3 hours = 3.3 AH, so two 12V 4AH sealed lead acid (SLA) or gel cell batteries in series.

Troubleshooting the Avigilon Single Door Controller

> **WARNING:**
> Disconnect power before servicing.

If your Avigilon controller or Smart Reader is experiencing issues, go to the Alta Access web app to diagnose the issue and restart the device, if necessary. For information on using the Device dashboard, see the Alta Access web app guide.

Faulty reader or port 31

SDC offline 32

Faulty reader or port

> **NOTE:** Try the steps in the sequence listed.

1. **Check voltage**: Using a voltmeter verify the voltage at the reader port, it should be reading 12V DC. Voltage inconsistencies are frequently the root cause of reader problems.

   > **NOTE:** Smart Readers do not experience a fault unless it is a whole voltage more or less.

2. **Check wiring**: Loose wiring is also a cause of reader faults.
3. **Power down**: Turn off the power to the expansion board.
4. **Disconnect the problem reader**: Locate the reader that is not working correctly. Disconnect it from its port by carefully pulling out the terminal block (the plug-in connector with the wires).
5. **Swap terminal blocks**: Find a reader that is working correctly. Disconnect its terminal block. Then, plug the terminal block from the non-working reader into the working reader port.
6. **Power up**: Turn the power back on to the expansion board.
7. **Test the problem reader**: Check if the reader that was originally not working is now functioning.

   > **NOTE:** If you don't have another reader set up you will need to make adjustments in Alta Access and create one using another port.

8. **Determine the fault**:

a. If the previously non-working reader now works, the original port on the expansion board is faulty.

b. If the reader still does not work, the problem is most likely with the reader itself, or its wiring.

9. After determining the fault contact Avigilon Alta Support

SDC offline

If your device appears offline, it usually means it is not connected to the Avigilon Alta VPN. As a result, no activity is visible in Alta Access.

NOTE: To resolve this issue, try a soft reset first:

1. Disconnect the device from power and battery, if applicable, for 30 seconds.
2. Reboot your router/modem and wait another 30 seconds.

If the device is still offline, see Typical causes and recommended solutions below.

If the device is still offline, see Hard reset on the next page.

Typical causes and recommended solutions

Power or ISP outages affecting the router/modem

Complete the soft reset above. If your network frequently loses power, consider using a UPS, such as battery backup, for your modem and router. This will keep both the device and network online during outages, preventing the need for reboots

IP assignment issue

Expand the IP range (subnet) or assign a static IP address to the device.

See Configure network settings using Alta Access mobile app on page 26.

Firewall issue

Review if Outbound ports 443 and 123 are set to open. You may also need port 53 if using an external DNS.

See Network requirements for Alta Access devices on page 5.

Bad patch cable or switchboard

Test by changing the patch cable and/or connecting the device directly to the modem to see if the issue goes away.

Too much power is drawn from the relays

If the device goes offline when multiple doors are in use, the total power draw may be exceeding the board or power supply's capacity. If this happens, refer to the data sheets to check your device's power rating.

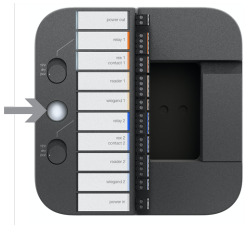
If issues persist, we recommend contacting your installer to inspect the hardware. If any network changes have been made, your installer should also be notified. As a **last resort**, the installer can attempt the next step.

Hard reset

> **WARNING: For installers only:** Only hard reset the Single Door Controller if absolutely necessary and if instructed by Avigilon Alta Support. This will clear all of the data on the Single Door Controller and will require reprovisioning.

A hard reset takes about 3-5 minutes, or longer if firmware and software updates are needed. Follow these steps:

1. Disconnect power from the Single Door Controller.
2. Press the Admin button.



3. While still pressing the Admin button, reconnect the power.
4. Continue to hold the button for another 15 seconds until the status LED turns yellow , and then release.
5. Wait until the status LED turns blue before reprovisioning the ACU to the same slot and name on the account. See Provisioning on page 17.

Appendix

Best practices - Wiring a REX to your 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 Alta Access.

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

Although you can wire a REX directly to the Alta 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 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.

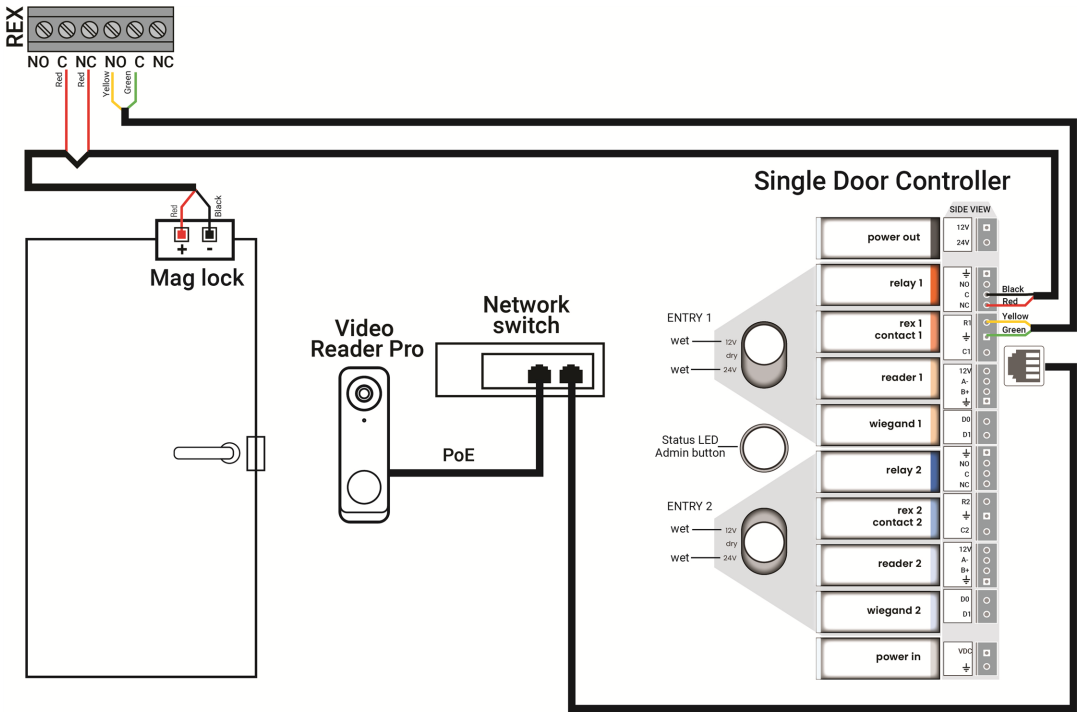
- Fail-safe hardware *unlocks* when power is interrupted or lost.
- Fail-secure hardware *locks* when power is interrupted or lost.

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 diagram is an example. 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



To further improve reliability, Alta Access 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 Access 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

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

UL 294

The following performance levels are defined for the Single Door Controller, as per UL 294:

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

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 Avigilon 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.

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

OP-CR-SDC: Contains FCC ID:2ABCB-RPICM4

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.

IC Company Number: 25142

OP-CR-SDC: Contains IC ID: 20953-RPICM4

More information

Technical support

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

Product documentation

For the cloud-native Avigilon Alta product documentation, see docs.avigilon.com.

Avigilon warranty

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

© 2025, Avigilon Corporation. All rights reserved. MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. Unless stated explicitly and in writing, no license is granted with respect to any copyright, industrial design, trademark, patent or other intellectual property rights of Avigilon Corporation or its licensors.

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

20250617-en

Revisions

Guide	Description
May 2025	Duration reference in blinking yellow indicator: LED indicators on page 28
January 2025	Domain change from control.openpath.com/login and control.eu.openpath.com/login to alta.avigilon.com/signin: Add SDCs using Alta Access on page 18 New navigation bar in Alta Access
December 2024	Tip about using Alta Access mobile app to create and provision: Add SDCs using Alta Access on page 18
September 2024	Control Center portal renamed to Alta Access
August 2024	Tip about using Alta Access mobile app to provision: Add SDCs using Alta Access on page 18
July 2024	Power rating updates: Standard SDC wiring configuration on page 12, Specifications and dimensions on page 7 Software updates (blinking yellow, blinking red): Status LED indicator on page 28 Overview diagram, package contents, mounting, and provisioning updates: Overview on page 4, What's included on page 5, Mounting on page 10, Provision the SDC using Alta Access mobile app on page 23
April 2024	App name updates: Alta Open mobile app (formerly, Openpath Mobile Access app), Alta Access mobile app (formerly, Open Admin app)