

User Guide

Avigilon ACC™ ES Rugged 8-Port Appliance

VMA-RPA-RGD-8P2 and VMA-RPA-RGD-8P4

© 2020, Avigilon Corporation. All rights reserved. AVIGILON, the AVIGILON logo, AVIGILON CONTROL CENTER, ACC, and AVIGILON APPEARANCE SEARCH are trademarks of Avigilon Corporation. MAC, MacOS, FINDER and MACINTOSH are registered trademarks of Apple Inc. FIREFOX is a registered trademark of Mozilla Foundation. Android is a trademark of Google LLC. Other names or logos mentioned herein may be the trademarks of their respective owners. The absence of the symbols ™ and ® in proximity to each trademark in this document or at all is not a disclaimer of ownership of the related trademark. Avigilon Corporation protects its innovations with patents issued in the United States of America and other jurisdictions worldwide (see [avigilon.com/patents](https://www.avigilon.com/patents)). 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 of 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

PDF-8PortRuggedAnalytics-A

Revision: 1 - EN

20200406

Table of Contents

Introduction	5
Package Contents	6
Tools Required	6
Overview	7
Front View	7
Rear View	8
System Requirements	9
Camera Frame Rate	9
Web Browser	9
Supported Network Configurations	10
Mounting an ACC ES Rugged 8-Port Appliance	11
Connecting an ACC ES Rugged 8-Port Appliance to a Power Supply	14
Configuring and Connecting the Hardware	15
Configuring the Appliance	17
Launching the ACC ES Admin Web UI	17
Viewing PoE Port Status	19
Managing ACC Services and Storage	20
Providing Service Logs for Support	21
Rebooting the Device and Managing Device Settings	21
Monitoring and Disconnecting the Storage SSD	22
Connecting the Device to Users and Cameras	24
Assigning a PoE Power Budget	24
Providing Device Logs for Support	25
Installing and Starting the ACC Client	27
Activating and Configuring ACC Software	28
Connecting to External Devices	29
LED Indicators	30
Budgeting PoE Power	31
Managing Certificates	32
Replacing the Web Certificate	32
Upload a Trusted CA Certificate	34

Upgrading the Firmware	35
Using the Software Reset Button	37
Restoring Factory Default Settings	39
Replacing the Storage SSD	40
Troubleshooting	43
Cannot Discover the Device	43
Network Configuration	43
Checking System Health	43
For More Information	44

Introduction

The Avigilon ACC ES Rugged 8-Port Appliance is an all-in-one solution for network video recording incorporating server side video analytics, ruggedly built for installation and use in harsh environments and remote locations. The appliance features:

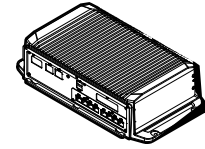
- A PoE switch to connect and power IP cameras.
- Built-in server to run the Avigilon Control Center Server Software.
- Video analytics engine to enable classified object detection on connected non-analytic cameras.

This guide describes how to install the appliance in various locations, with unique power requirements and how to configure the system after the appliance has been powered on.

Package Contents

Ensure the ACC ES Rugged 8-Port Appliance package contains the following:

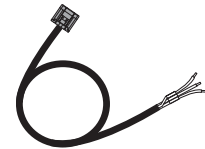
ACC ES Rugged 8-Port Appliance



Front panel key



Power supply cable (to connect to user-supplied 9-32VDC 100W (min) power supply)



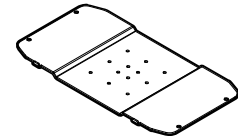
Digital input/output cable



DIN bracket



Mounting plate for the DIN bracket



4 (four) flat-head screws to attach the DIN bracket to the mounting plate in a plastic bag labeled DIN rail #1



4 (four) round-head screws to attach the the ACC ES Rugged 8-Port Appliance to the mounting plate in a plastic bag labeled DIN rail #2



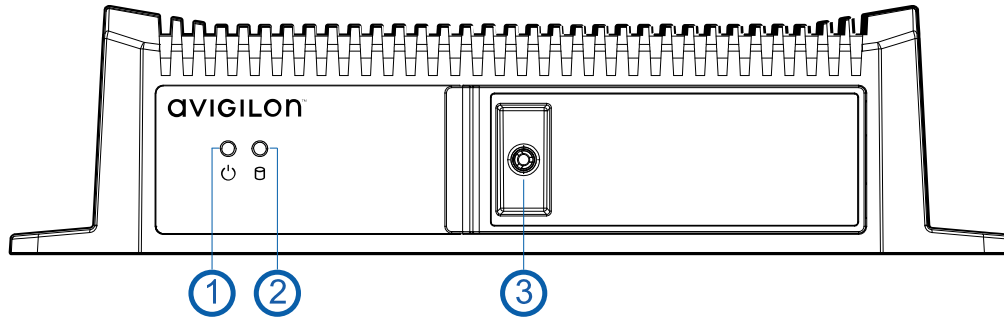
Important: For compliance to UL 60950-1, if the ACC ES Rugged 8-Port Appliance is powered by an external power adapter, it must be a UL Listed power adapter suitable for use at Tma is 40C whose output meets ES1 (or SELV) and is rated 9-32Vdc, 100W minimum. Please contact Avigilon for further information.

Tools Required

A Phillips #2 screwdriver is all that is required to attach the ACC ES Rugged 8-Port Appliance and the DIN bracket to the mounting plate.

Overview

Front View



1. **Power LED Indicator**
2. **Disk Activity LED Indicator**

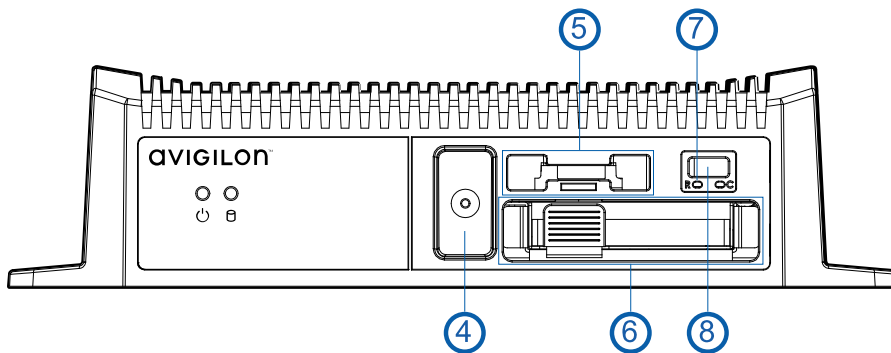
See *LED Indicators* on page 30

3. **Lock (locked position)**

The front panel is normally locked to protect and prevent access to internal components, as shown above.

4. **Lock (unlocked position)**

Use the key to unlock the front panel and open it to access the internal components, as shown below.



5. **CMOS Battery Holder**

The power from the battery in the holder maintains the appliance's internal time and date settings, and BIOS settings in the CMOS memory. If the time and date settings on the appliance become unreliable, the battery must be replaced by a trained technician only.



Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions

6. SSD Tray

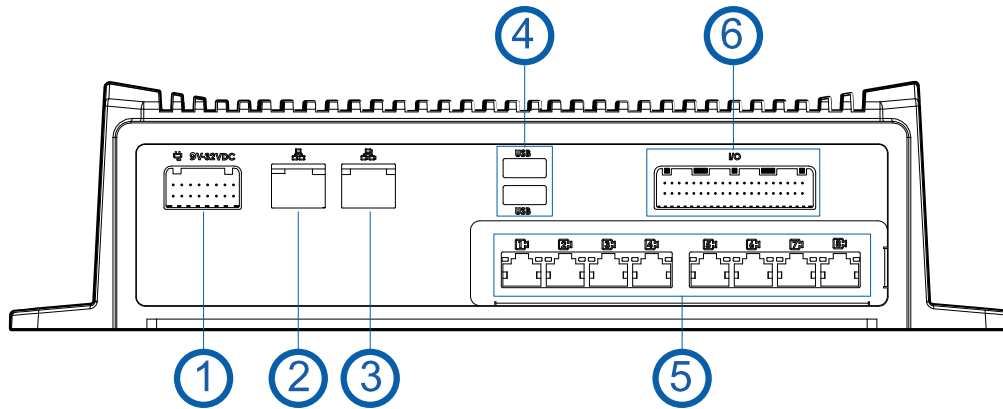
Slide the tray in and out to access the storage SSD. See *Replacing the Storage SSD* on page 40.

7. Reset button

Use this button to physically restart the appliance.

8. USB 3.0 port

Rear View



1. Power connector

2. Corporate network uplink port

Accepts a 1GbE Ethernet connection to the general network to allow users access to the web interface and connected camera video.

3. Camera network uplink port

Accepts a 1GbE Ethernet connection to link to other PoE switches and cameras.

4. USB 2.0 ports

5. PoE switch component

Connect cameras to the 10/100 speed PoE switch component to power the cameras and record video. The switch is capable of providing a total of 60 watts of power shared across all the PoE ports.

6. I/O connector

Provides connections to external input/output devices. The two cable ends are labeled for digital input and digital output. For more information, see *Connecting to External Devices* on page 29.

System Requirements

Camera Frame Rate

The ACC ES Rugged 8-Port Appliance can provide analytics for non-analytics cameras. For optimal analytics performance, the source camera should stream a minimum of 10 images per second (ips).

Web Browser

Administrative settings for the appliance are managed through a web interface, accessed from any Windows, Mac or mobile device using any of the following web browsers:

- Mozilla Firefox browser version 3.6 or later
- Google Chrome browser 8.0 or later
- Microsoft Edge browser 25 or later
- Safari 5.0 or later
- Chrome on Android 2.2 or later
- Safari on Apple iOS 5 or later.
- Windows Internet Explorer browser version 7.0 or later

Note: Your web browser must be configured to accept cookies or the web interface will not function correctly.

Supported Network Configurations

Note: The Camera Uplink Port does not support dynamically switching DHCP servers.

Network Connections	Camera Web Interface Access	Supported IP Configurations		Notes
		Corporate LAN Uplink	Camera LAN Uplink	
Corporate LAN Uplink only	No	Static or DHCP assigned	Unconnected (leave as DHCP)	Camera LAN Uplink and connected cameras will use Zeroconf IP addresses.
Camera LAN Uplink only	Yes	Unconnected (leave as DHCP)	Static, DHCP-assigned, DHCP-Zeroconf	
Corporate and Camera LAN Uplink	via Camera LAN Uplink only	Static, DHCP-assigned, DHCP-Zeroconf	Static, DHCP-assigned, DHCP-Zeroconf	Corporate and Camera LAN Uplinks must be on different subnets.

Mounting an ACC ES Rugged 8-Port Appliance

You can mount the ACC ES Rugged 8-Port Appliance to almost any flat surface capable of bearing its weight in any orientation, or to a DIN rail in any of four orientations. With the exception of mounting to a DIN rail using the provided mounting plate and DIN rail bracket and screws, you must provide screws and anchors, or nuts and bolts suitable for the surface on which you are mounting the appliance.

Tip: Mount the appliance to any surface or to a DIN rail before you permanently power on the appliance, connect cameras to it, and start recording. If you want to set up your appliance before mounting it, we recommend you turn off the power supply to the appliance and disconnect all cables after set up is complete and before you mount the appliance.

To mount the appliance on a flat surface:

The base of the appliance incorporates mounting holes at each corner for mounting the appliance to any flat surface at any angle or orientation:

1. Position the appliance with the rear panel facing in the direction for easiest access to the power and cable connectors.
2. Mark the locations of the screw holes on the surface.
3. Drill holes for the anchors and insert the anchors into the wall. If you are using wood, concrete or masonry screws, drill holes as appropriate.
4. Attach the appliance to the surface using the fasteners you provide.

To mount the DIN rail bracket and mounting plate to the appliance:

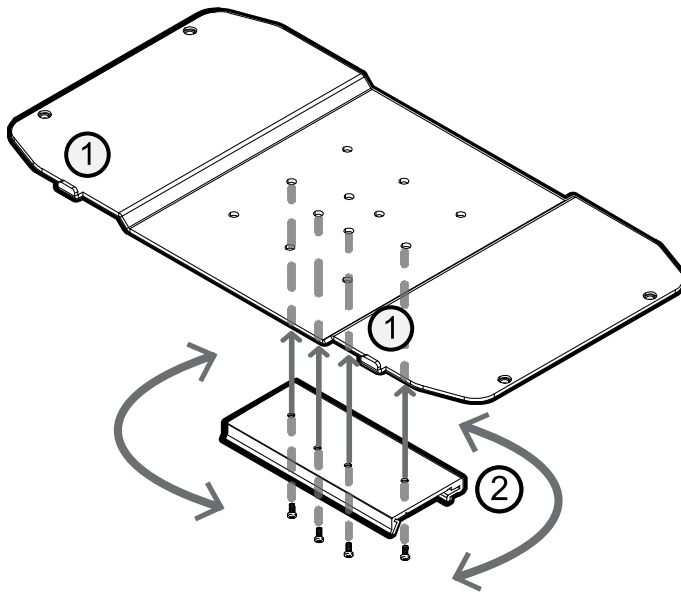
A mounting plate, bracket, and screws to attach the bracket to the plate are provided. The DIN rail bracket clips to a DIN rail with the curved part to the top. The ACC ES Rugged 8-Port Appliance has metal tabs on the rear side that fit into matching slots in the mounting plate.

The bracket can be attached to the mounting plate in one of four positions. This gives you options to mount the appliance to the rail in a variety of positions to give you the best access to the front and rear panels:

- Front or rear facing up or down
- Front or rear facing right or left

Tip: If you are mounting the ACC ES Rugged 8-Port Appliance to a DIN rail, determine the correct orientation of the bracket to the mounting plate and install the bracket on the mounting plate before attaching the mounting plate to the appliance. This makes it easier to ensure that the appliance will be installed in an optimal position.

1. Determine the position you want the DIN rail bracket attached to the mounting plate.
2. Align the DIN rail bracket to the pre-drilled threaded holes at the correct orientation on the mounting plate and attach using the 4 (four) flat-head screws provided in the plastic bag labeled **DIN rail#1**. The tabs on the back of the of the appliance fit into the slots on one side of the bracket only.

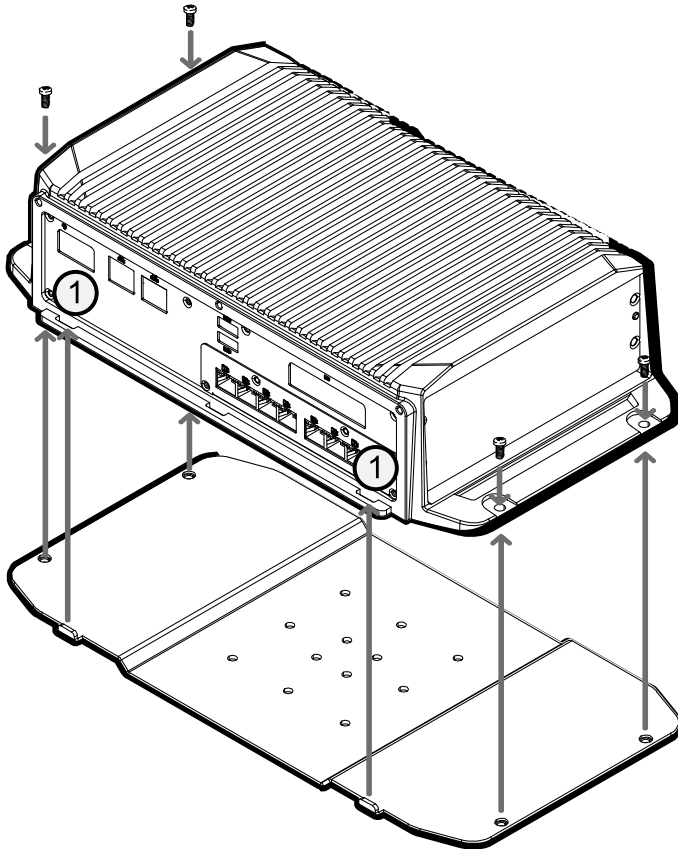


① Indicates the tabs on the mounting plate which fit in to the slots on the rear of the appliance.

② Indicates the top edge of the DIN mounting bracket.

The example orientation places the appliance on the mounting bracket so that the front of the appliance is facing up.

3. Mount the appliance on the mounting plate with the front and rear correctly oriented with the DIN rail bracket using the 4 (four) round-head screws provided in the plastic bag labeled **DIN rail#2**, as shown below.



① Indicates the slots on the rear of the appliance into which the tabs on the mounting plate fit.

4. Clip the appliance to the DIN rail with the DIN rail bracket on the mounting plate correctly aligned so the front panel LED indicators are visible and the rear panel connections are accessible.

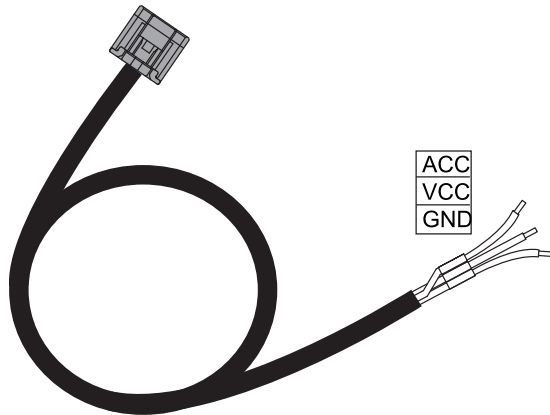


CAUTION — The device must be mounted as instructed or any issues that arise will not be covered by the warranty.

Connecting an ACC ES Rugged 8-Port Appliance to a Power Supply

The ACC ES Rugged 8-Port Appliance can be powered by any suitable 9–32 volt DC 100W (min) power supply using the provided power cable.

The provided power cable has a connector at one end that plugs into the power connector on the rear of the appliance, and three wires at the tail end labeled ACC (accessory), VCC, and GND.



To make a permanent power connection (unswitched), connect both the ACC and VCC wire to the positive side of the power source. Connect the ground wire to the ground side of the power source.

The ACC wire is provided if you want to connect to a switched power signal, such as to the vehicle accessory signal in a vehicle. When the ACC wire is connected to a switched power signal, the system will turn ON when the ACC wire is connected to the positive side of the power source, and the system will go into low-power standby mode when the ACC wire is disconnected from the positive side of the power source.

Configuring and Connecting the Hardware

You must configure the device for the first time before connecting it to your security network.

Important: If static IPs are required, a laptop computer is required to manually configure the IP address for the device.

Complete the recommended procedure for configuring the device and connecting it to your security network:

1. Connect power and wait for the device to start up.

Do not connect any other cables until instructed in this procedure.

2. If you are configuring the device with a static IP address, connect a DHCP enabled port on your configuring laptop with an Ethernet cable directly to the *camera network* port on the device. Otherwise, connect the device to the corporate network using the *corporate network* port.
3. On the laptop or network workstation, open the Network tab in File Explorer (Windows) or Finder (Macintosh) to locate the device.

You are looking for a network device labeled "VMA-RPA-RGD-8Px-<serial number>".

If you cannot locate the device, see *Troubleshooting* on page 43.

4. You will see a security warning from the browser informing you that the connection between the Web UI and the device is untrusted because the device is using a self-signed Web Certificate. This is expected and you can safely ignore the warning and proceed to the ACC ES Admin Web UI.

The level of security provided by the certificates included with the device should be sufficient for any organization that does not deploy a Public Key Infrastructure (PKI) on its internal servers.

Important: For organizations that deploy their own PKI, the device's certificates can be managed from the ACC ES Admin Web UI after the device is installed and powered. The default self-signed Web Certificate can be replaced, signed certificates from Certificate Authorities (CAs) that are not provided with the device can be added, and the signed certificates from CAs for public servers such as Google Mail that are provided with device can be disabled. For more information, see *Managing Certificates* on page 32

6. Right click and select **View Device Webpage** to open the device sign in page in your default web browser.

7. When you are prompted by the ACC ES Admin Web UI, enter a new password for the administrator username.

The Strength meter measures the complexity of your password: Red is too simple, yellow is reasonably complex, and green is complex. Complexity measures the difficulty to discover your password, not how secure your password is. A complex password is recommended.

The page refreshes and you are prompted to log in.

8. Enter `administrator` as the username and your new password.

The ACC ES Admin Web UI launch page is displayed.

9. Set the language for the ACC ES Admin Web UI, a user-friendly hostname, and the time zone. In the navigation sidebar, click **Device** to open the Device panel. In the:
 - a. General pane, select the Language from the drop-down.
 - b. Hostname pane, optionally replace the serial number of the appliance with a descriptive hostname for the appliance.
 - c. Time pane, specify the Time Zone and identify the time source in the NTP drop-down and Servers list.

For more information see *Rebooting the Device and Managing Device Settings* on page 21.

10. Select how the appliance obtains IP addresses from the network. On the navigation sidebar, click **Network** to open the Network panel. For each network port used, select Automatic or manually enter the settings.

For more information, see *Connecting the Device to Users and Cameras* on page 24.

11. If a laptop was used to configure the device:
 - a. Connect an Ethernet cable from the device to the *corporate network* port.
 - b. Disconnect the configuring laptop from the *camera network* port.

Configuring the Appliance

The ACC ES Rugged 8-Port Appliance can be configured through the ACC ES Admin Web UI that is accessible from any compatible browser on the network. The ACC ES Admin Web UI allows you to configure the ACC ES Rugged 8-Port Appliance server settings, set how the server keeps time, and allows you to remotely restart or upgrade the server. It also allows you to download the ACC Client software to the workstation you are using to access the ACC ES Admin Web UI.

Start backing up the system settings for the recorder after you configure it. These settings include the ACC password, and the settings for the camera connections. For more information on backing up the site and server configurations, see the *Avigilon ACC Client User Guide*.

Throughout this section, the term device is used to identify the appliance.

Launching the ACC ES Admin Web UI

You can access the ACC ES Admin Web UI from a network workstation with network access to the device.

The first time you access the ACC ES Admin Web UI of your device, use one of the following methods:

- **Discovering the Device**

1. Open the Network tab in File Explorer (Windows) or Finder (Macintosh) to locate the device.
You are looking for a network device labeled "VMA-RPA-RGD-8Px-<serial number>".
2. Right click and select **View Device Webpage** to open the device sign in page in your default web browser.

- **Using the IP Address or Hostname**

1. Open a web browser from a network workstation with network access to the device.
2. Enter its IP address or hostname into the web browser to open the device sign in page:

`https://<Device IP address >|<Device hostname>/`

For example: `https://169.254.100.100/` or `https://my_AvigilonDevice/` , where `my_AvigilonDevice/` is the hostname configured in the Device panel.

Note: If you forgot the IP address or hostname that was configured during the installation process, the information is listed in the ACC Client software, in the server Setup tab.

Tip: Bookmark the device sign in page.



To log in to and out of the ACC ES Admin Web UI:

1. To log in, enter the ACC ES Admin Web UI username and password.

The ACC ES Admin Web UI launch page is displayed in your web browser.

2. To log out of the ACC ES Admin Web UI, click the log out icon on the right side of the top banner.

On the ACC ES Admin Web UI launch page, **Dashboard** is selected in the side navigation bar, and the Dashboard status panels are displayed:

- **ACC Server** — Displays **Running** when the ACC Server software is operating; otherwise it displays **Stopped**. The panel provides technical information about the device: site name, server name, server ID, server version, software version, the number of available camera channels, and the maximum number of ACC client instances allowed.
- **System** — Displays **Ready** when the device is fully operational, and **Rebooting** then **Initializing** when the device is restarting. The panel provides technical information about your device: product name, part number, serial number, and firmware version.
- **Network** — Displays information about the two uplink ports on the device. Click  to open the [Network panel](#). See *Connecting the Device to Users and Cameras* on page 24.
- **PoE** — Displays status information about each PoE port. Icons in the panel let you quickly see how many ports are in use, their status, speed and whether the link is up or down. Click  to open the [PoE Panel](#). See *Viewing PoE Port Status* on the next page.

Use the menu options under Services and System in the Dashboard navigation bar to access all the other web interface panels.

- **Services** — Expand **ACC** in the left sidebar to navigate to
 - The **Server** page to control the ACC Server on the device. See *Managing ACC Services and Storage* on page 20
 - The **Logs** page to view ACC Server service logs. See *Providing Service Logs for Support* on page 21.
- **System** — Access the five options to configure the device and view its status:
 - **Device**. See:
 - *Rebooting the Device and Managing Device Settings* on page 21
 - *Upgrading the Firmware* on page 35
 - *Managing Certificates* on page 32
 - **Storage**. See *Monitoring and Disconnecting the Storage SSD* on page 22.
 - **Network**. See *Connecting the Device to Users and Cameras* on page 24.
 - **PoE**. See:
 - *Assigning a PoE Power Budget* on page 24.
 - *Budgeting PoE Power* on page 31
 - **Logs**. See *Providing Device Logs for Support* on page 25

Viewing PoE Port Status

The PoE panel displays a status for each port in the Status column. Statuses include the following:

Green	Powered	A PoE device is connected to the port and is operating normally.
	High powered	PoE+ is turned on.
Gray	Disconnected	There is no device connected to the port.
	Unpowered	The PoE port power is switched off from the PoE page in the ACC ES Admin Web UI
Yellow	Overloaded	A PoE device is connected to the port but is not receiving power. This status typically occurs when one port is overcurrent, or the device is requesting more power than budgeted, etc.
	Low current	The device is getting low current from the port.
Red	Error	The device is in an error state.

Tip: If a camera is disconnected then reconnected to the device, you may need to refresh this page to view the latest status and budget values.

Managing ACC Services and Storage

On the **Server** panel use the:

- General pane:

To...	Do this...
Shut down all the services before you shut down the device.	Click Stop .
Start up all the services after they have been shut down.	Click Start .
Format the storage drive.	Click Reinitialize to delete all configuration and recorded video data.

- Network Storage Management pane:

To allow users to archive video from this device using the ACC Client software:

1. Click **Enabled**.
2. From the Protocol drop down list, select one of the following:
 - **CIFS** — Common Internet file system. The network path is typically in this format: *//<hostname or IP> / <path>*
 - **NFS** — Network file system. The network path is typically in this format: *<hostname or IP> : <path>*
3. In the **Network Path** field, enter the path to the preferred video archiving location.
4. If the network location requires authentication, enter the credentials in the Username and Password fields.
5. Click **Apply**.

- Service and RTP Ports panes

To change the UDP and TCP ports used to communicate with the appliance:

- In the Service Ports pane, enter the **Base** value to use for the HTTP, HTTPS, and UDP ports and click **Apply**. The list of ports is updated.
- In the RTP Ports pane, enter the **Base** value to use for the UDP ports and click **Apply**. The range of ports available for RTP is updated.

Important: These changes can only take effect after the system restarts. When you are prompted, allow the system to restart.

Providing Service Logs for Support

Use the Logs page to view service logs. The logs are typically requested by Avigilon Technical Support to help resolve an issue.

By default, the page displays 100 warning messages from the logs.

Typically, Avigilon Technical Support assists you to access and filter the logs on this panel to isolate the logs that they require. You then copy and paste the logs into a text file, save it and send it to Avigilon Technical Support.

You can filter the logs to display the information that you need:

1. In the drop down list, select the type of application log that you need. The options are:
 - **Exception Logs**
 - **FCP Logs**
 - **Server Logs**
 - **WebEndpoint Logs**
2. In the **Maximum Logs** drop down list, select the number of log messages you want to display each time.
3. Enter text in the **Filter** field to apply a filter to the log listings.
4. Click the **Sync** button to display the updated logs.

Rebooting the Device and Managing Device Settings

On the Device panel use the:

- **General** pane to:
 - **Reboot** the device from the ACC ES Admin Web UI. You can monitor the progress of the device as it reboots from the ACC ES Admin Web UI launch page (see . For more information see, *Launching the ACC ES Admin Web UI* on page 17).
 - Select a **Language** for the ACC ES Admin Web UI from the drop down list.
- **Hostname** pane to enter a new **Hostname**. Click **Apply** to make the change.

The default hostname is the same as the server name. The server name is in the form *<Model>-<Serial Number>*

- **Password** pane to change the administrator password:

Note: You cannot change the default *administrator* username on the ACC ES Admin Web UI, only the password.

1. To change your password, confirm your identity by entering your current password in the **Old Password** field.
2. Enter the new password in the **New Password** field.
3. Re-enter the new password in the **Confirm Password** field.

CAUTION — You will lose recorded video and configuration data if you forget your password. To reset the administrator password, you must reset the device to the factory default settings. For more information on performing a factory restore, see *Restoring Factory Default Settings* on page 39.

- **Time** pane to customize how the device keeps time:
 - Select your **Time Zone** from the drop-down list. The time zone that you set here is used by the recording schedules defined in the ACC Client software.
 - Select whether you want to keep synchronized time through a Network Time Protocol (NTP) server (recommended) in the NTP field.

Select:

- **DHCP** to automatically use the existing NTP servers in the network.
- **Manual** to enter the address of NTP servers in the Servers list. Controls to add and delete addresses in the list, and reorder them are activated.
- **Off** if you do not use an NTP server.

Note: The default set of NTP servers is always present in the Servers list. The default list cannot be rearranged or deleted:

- 0.pool.ntp.org
- 1.pool.ntp.org
- 2.pool.ntp.org
- 3.pool.ntp.org

Click **Apply** to save the time settings.

- **Upgrade Firmware** pane to install the latest version of the firmware on your device, or to reinstall the firmware if it becomes corrupted. For more information, see *Upgrading the Firmware* on page 35.
- **Certificates** pane to manage the certificates used by the ACC ES Admin Web UI and the device. For more information, see *Managing Certificates* on page 32.









Monitoring and Disconnecting the Storage SSD


On the **Storage** panel of the ACC ES Rugged 8-Port Appliance you can:



- View the storage capacity and the status of the replaceable storage SSD.
- Set the status of the storage SSD to Eject, prior to removing it from the appliance for replacement if it ever fails.


Important: The storage SSD must be replaced with an SSD of the same capacity (2TB for the VMA-RPA-8P2 model, or 4TB for the VMA-RPA-8P4 model).

Click **Storage** on the navigation bar to open the Storage panel. You can perform any of the following actions in the pane in the Storage panel:

To...	Do this...
View the capacity and status of the SSD.	<p>Click Storage on the navigation bar. When the device is:</p> <ul style="list-style-type: none"> • Correctly working, Ready and  is displayed. • Not correctly working, Error and  is displayed.
View details about the SSD.	<ol style="list-style-type: none"> 1. Click  in the upper right of the pane to open the storage details pane. 2. Click the  to display details about the drive, including its model and serial numbers.
Eject the SSD.	<ol style="list-style-type: none"> 1. Click . The status changes to  and  changes to , indicating all services have stopped.

Tip: If you decide not to remove the SSD, click  to reconnect the SSD.

2. You can now remove the SSD from the appliance. See *Replacing the Storage SSD* on page 40.
3. After installing the replacement SSD in the caddy and inserting it back into the appliance, the status changes to . When complete the status changes to .

Important: If the status changes to  you have inserted an incompatible SSD. You cannot proceed until you insert a SSD of the same capacity as the original factory-installed drive.

Connecting the Device to Users and Cameras

On the Network panel, you can change network connections of the device. Two network connections are supported: one for a corporate network and one for a camera network.

The corporate network is the network that typically provides users with access to the device. Users who monitor video through the ACC Client software connect to the device through this network.

The camera network is a closed network that typically only contains cameras. This reduces the amount of interference with video recording.

Note: The Corporate Network and the Camera Network must be on different subnets.

For more information about the network connections, see *Supported Network Configurations* on page 10.


You can perform any of the following actions in each of the panes in the Network panel:

To...	Do this...
Set how the device obtains an IP address for each network.	<p>In each of the panes in the Network panel, toggle Automatic IP on to discover connected networks automatically (the default setting), or off to manually specify the connections. Enter the appropriate values in the following fields if you are manually entering the connection settings:</p> <ul style="list-style-type: none">• IP Address• Subnet Mask• Default Gateway <p>Click Apply to save your changes.</p>
Set how the device obtains a named address from a DNS server.	<p>Toggle Automatic DNS on to discover connected DNS servers automatically (the default setting), or off to manually specify the DNS servers. Controls to add and delete addresses in the list, and reorder them are activated when Automatic DNS is toggled off.</p>

Assigning a PoE Power Budget

Use the **PoE** panel to see how much power is available to, and being used by, connected devices. The default setting for all ports is Auto. This setting automatically detects and budgets the amount of power required by the device connected to the port. For each port you can adjust this setting manually, or turn off power output completely. If you want to manually adjust the power output of the ports you must calculate a PoE power budget, see *Budgeting PoE Power* on page 31.

To open the PoE panel, either:

- Click  on the PoE status panel on the ACC ES Admin Web UI launch page.
- Click **PoE** from the Dashboard navigation bar.

To...

Do this...

See how much power is available to, and being used by, connected devices.

Look at the two bars at the top of the panel:

- The **Budget** bar indicates the total amount of power budgeted for all devices connected to the PoE ports.
- The **Consumption** bar indicates the actual amount of power currently used by all the connected devices.

Adjust the power used by each PoE port.

Use the **Power** bar for each port to configure a PoE power budget:

Tip: You can also use the **Power** bar to remotely power cycle the camera. After you set the Power setting to Off, wait for the camera to power off then change the Power setting to **Auto** or **Manual**.

- Click **Off** to disable power output to the port. When power to a port is disabled, the port no longer outputs power but can act as a standard network connection for any device.
- Click **Auto** to automatically output power to the connected device depending on its mode of operation.
- Click **Manual** to enter a power budget value in watts. Make sure the budget includes potential power loss at the cable.

Tip: Devices that support both PoE and PoE+ (802.3at) modes of operation can be forced into non-PoE+ mode (802.3af) by using a manual 15W budget.

Settings are not implemented until you click **Apply**.

After you click **Apply**, allow the system to reboot when the following message is displayed:

Applying changes may power-cycle PoE-powered devices.

The ACC ES Admin Web UI automatically refreshes the screen and displays the updated settings after the new power settings are applied.

Providing Device Logs for Support

Use the System Logs panel to view the device logs. The logs are typically requested by Avigilon Technical Support to help resolve an issue.

By default, the page displays 100 warning messages from the Logs.

Typically, Avigilon Technical Support assists you to access and filter the logs on this panel to isolate the logs that they require. You then copy and paste the logs into a text file, save it and send it to Avigilon Technical Support.

You can filter the logs to display the information that you need:

1. In the drop down list, select the type of application log that you need. The options are:
 - **System Logs**
 - **Boot Logs**
 - **Web Server Logs**
2. In the **Maximum Logs** drop down list, select the number of log messages you want to display each time.
3. Enter text in the **Filter** field to apply a filter to the log listings.
4. Click the **Sync** button to display the updated logs.

Installing and Starting the ACC Client

If you are installing the first Avigilon appliance in your security network, you can install the ACC Client software on a network workstation or on the computer you are using to access the Web Interface. Otherwise, add the appliance as a new site in your security network using the ACC Client software on a network workstation.

You can install the latest version of the ACC Client software on a network workstation with network access to the Internet :

1. Open a web browser from a network workstation with network access to the Internet.
2. Download the ACC Client software from the Avigilon website: avigilon.com/support/software. Click through to the installation software for the latest version of the ACC Client software.


Note: The first time you access the web site from which you download the software you will be prompted to register. Enter all of the required information and click **Complete Registration**. Your registration is automatically accepted and you will proceed to the web site.

3. Install the ACC Client software on a network workstation with network access to the device.

To open the ACC Client software:

- Double-click the desktop shortcut icon .
- In the Start menu, select **All Programs** or **All Apps > Avigilon > Avigilon Control Center Client**.

To close the ACC Client software:

1. In the top-right corner, click .
2. Click **Yes**.

Activating and Configuring ACC Software

- [Initial ACC™ System Setup and Workflow Guide](#)
- [ACC 7 Help Center](#)

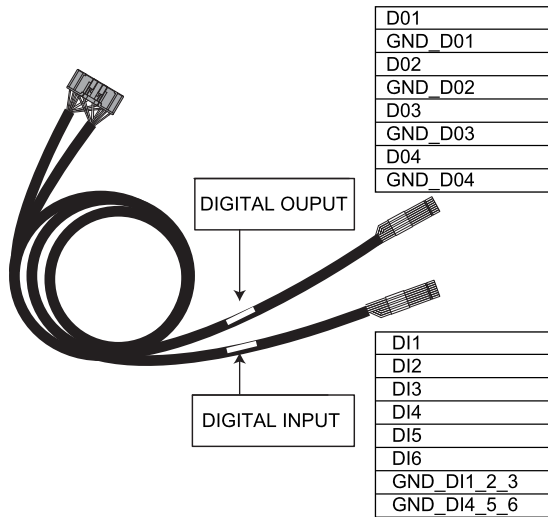
For information about cloud-connecting your ACC server, see [Avigilon Cloud Services Support](#).

Printable versions of these guides are available on the Avigilon website:

<https://www.avigilon.com/support/software/>.

Connecting to External Devices

External devices are connected to the ACC ES Rugged 8-Port Appliance using the digital I/O cable inserted into the digital I/O connector on the rear side of the appliance. Details for the 8 labeled input wires and the 8 labeled output wires is shown below.






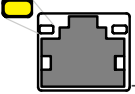
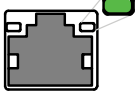

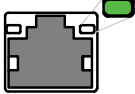
Pin	Function	Description
D11	IN1	Alarm Inputs — Active-Low inputs. To activate, connect the Input to the Ground pin (GND). To deactivate, leave disconnected.
D12	IN2	
D13	IN3	
D14	IN4	
D15	IN5	
D16	IN6	
GND_DI1_2_3	Ground pin for Inputs 1, 2, and 3	
GND_DI4_5_6	Ground pin for Inputs 4, 5, and 6	
D01	OUT1	Outputs — Form-A dry contact outputs. When active, terminals are connected. When inactive, terminals are disconnected.
GND_D01		
D02	OUT2	
GND_D02		
D03	OUT3	
GND_D03		
D04	OUT4	
GND_D04		

Note: Contacts are normally open.

Maximum load is 48V, 0.3A.

LED Indicators

The following list describes what the LEDs on the ACC ES Rugged 8-Port Appliance indicate.

	Icons	LED Status	Description
Front LEDs	Status 	Red	Device is powered and running
			Yellow
Back LEDs	PoE Switch 	Left 	On: Port is delivering PoE power Off: Port is not delivering PoE power Blinking: Port is not delivering PoE power but PoE camera is connected
		Right 	On: Network link is present Off: Network link is not present Blinking: Network activity is present
		Green	
Corporate & Camera Uplink Ports		Right 	On: Network link is present Off: Network link is not present Blinking: Network activity is present
		Green	

Budgeting PoE Power

The PoE switch component in the Avigilon ACC ES Rugged 8-Port Appliance can output a total of 64 W of power to the connected devices. Each PoE port is capable of outputting 16 W to standard PoE devices, and 30 W to PoE+ devices. This typically means that the device can support up to 4 standard PoE devices or up to 2 PoE+ devices.

Advanced users can manually adjust the PoE power budget for each port to consistently accommodate the cameras needed.

If you choose to manually adjust the PoE budget at each port, be aware that you must also account for potential power loss in the cable. Unless the amount of power loss in the cable is known, use the following estimates:

- If the device uses less than or equal to (\leq) 16 W — expect 2.5 W of power loss.
- If the device uses more than ($>$) 16 W — expect 4.5 W of power loss.

To calculate the recommended power budget for each port, use the following equation:

$$\text{Power budget} = \langle \text{Camera power consumption} \rangle + \langle \text{Expected cable power loss} \rangle$$

Example: Connect the following 4 cameras to an ACC ES Rugged 8-Port Appliance:

2 x HD dome cameras	$(9\text{ W} + 2.5\text{ W}) \times 2$	= 23 W
1 x HD PTZ camera	$25.5\text{ W} + 4.5\text{ W}$	= 30 W
1 x HD micro dome	$4\text{ W} + 2.5\text{ W}$	= 6.5 W
Total		= 59.5 W

The total power consumption of the 4 cameras is within the PoE switch component limits.

Note: If you miscalculate the required power for a PoE port, the entire PoE switch may be shut down if total power output exceeds 64 W.

Managing Certificates

Trusted certificates are used by the device to authenticate other servers and clients to which it needs to connect, and to secure those connections. Avigilon provides a self-signed Web Certificate to secure the connection to the ACC ES Admin Web UI and to the WebEndpoint service, and a set of system-level signed certificates from well-known trusted CAs to ensure secure connections to any needed servers. Optionally, you can provide your own certificates and CAs.

The level of security provided by the certificates included with the device should be sufficient for any organization that does not deploy a Public Key Infrastructure (PKI) on its internal servers.

The certificate management feature on the appliance controls only the appliance web certificate used by the WACC ES Admin Web UI and the ACC WebEndpoint product. Within the ACC server the certificate authorities configured by this feature are only used to validate secure email servers used by ACC Email and Central Station Monitoring features. ACC Server to ACC Server and ACC Server to ACC Client connections are not controlled or validated using the appliance certificate management feature.

For example, if your organization uses a public email server such as Google Mail, when email notifications are triggered, ACC accesses the Google Mail server and receives a certificate identifying the Google Mail server. The ACC software verifies the certificate by confirming the CA that signed the Google Mail certificate is from the list of well-known trusted CAs, and the connection is secured.

Note: The signed certificates shipped with the device are the same as those shipped with Mozilla's browser, and are publicly available from [The Debian Project](#). The certificates allow SSL-based applications to check for the authenticity of SSL connections. Avigilon can neither confirm nor deny whether the certificate authorities whose certificates are included with this appliance have in any way been audited for trustworthiness or RFC 3647 compliance. Full responsibility to assess them belongs to the local system administrator.

Organizations that deploy their own PKI can use the Certificates pane of the ACC ES Admin Web UI to manage certificates on the device.

For example, you can:

- Replace the default self-signed Web Certificate with your own organization's certificate.
- Add CAs, such as internal CAs used within your organization, to the device.
- Disable (and enable) any of the system-level CA certificates.

Replacing the Web Certificate

Manage the device's Web Certificate from the Web Certificate tab on the Certificates pane. The ACC ES Admin Web UI and the WebEndpoint service use this certificate to authenticate themselves to devices that connect to them. Only one Web Certificate can be active at any time.

You can replace the default Web Certificate with a new certificate. Obtaining a new Web Certificate is a three-step process:

1. Send the certificate issuer used by your organization a Certificate Signing Request (CSR) and the issuer will return you a new certificate file and private key file (typically by email). You can generate a CSR from the Web Certificate tab, or using the certificate issuer's preferred method if they do not accept the CSR from the ACC ES Admin Web UI:
 - a. Open the Web UI, click Device in the navigation bar, and scroll down to the Certificates pane.
 - b. On the Web Certificate tab, click the Certificate Signing Request button.
 - c. Fill in the standard CSR form with the information defined by the PKI you are using and click Generate.

The CSR file generated.csr is saved in your Downloads folder.

- d. Send the file to your organization's certificate issuer.

Tip: If the certificate issuer does not accept the CSR, use the certificate issuer's preferred method to generate the CSR.

2. After you receive the .crt file containing the new certificate from the certificate issuer, save it to a location accessible to the device.
3. Upload the new certificate to the device:
 - a. Open the Web UI, click Device in the navigation bar, and scroll down to the Certificates pane.
 - b. On the Web Certificate tab, click Upload.
 - c. In the Upload Web Certificate dialog, enter a name for the certificate, and click and navigate to the .crt file or drag and drop into the Drop '.crt' certificate (pem) file here or click to upload area.
 - If the certificate file was created with the most recently generated CSR file from the ACC ES Admin Web UI, Upload is activated.
 - Otherwise, click and navigate to the .key file or drag and drop into the Drop '.key' private key (pem) file here or click to upload area. Upload is activated.

Note: If the certificate file (.crt) was created with a CSR generated by the certificate issuer's preferred method (or was not generated using the most recent CSR file on the device), repeat this step to upload the private key file.

- d. Click Upload.
4. On the Web Certificate tab, click on the name of the uploaded certificate to enable it. This also disables the previous certificate.

Upload a Trusted CA Certificate

Manage signed certificates from internal CAs deployed in your organization's internal servers from the User Certificate Authorities tab of the Certificates.

For example, an internal email server in an organization that deploys its own PKI may provide a certificate signed by a CA that is not in the set of well-known trusted CAs to the ACC software when it tries to access the mail server. The certificate cannot be verified unless a certificate signed by that CA is uploaded to the User Certificate Authorities tab of the Certificates pane.

If you are required to upload a signed certificate from a CA, complete the following steps:

1. Open the Web UI, click Device in the navigation bar, and scroll down to the Certificates pane.
2. Click the User Certificate Authorities tab.
3. Click Upload.
4. In the Upload User Certificate Authority dialog, enter a name for the certificate, and click or drag and drop to upload the file. You can only upload one file at a time.

Upgrading the Firmware

You can upgrade the firmware using the ACC ES Admin Web UI.

Note: You can also upgrade the firmware from an ACC Client connected to the device. Refer to the procedure for upgrading servers in a site in the Help files provided with the ACC Client.

Upgrade the firmware to ensure the appliance is operating with the latest software, to upgrade from obsolete software, or to replace corrupted firmware. When you upgrade the firmware, all your current settings and all recorded video is retained.

Before you can upgrade or reinstall the firmware, download the latest version of the firmware (.fp) file from the Avigilon website: partners.avigilon.com, and:

1. If you have access to the Internet from your web browser while using the ACC ES Admin Web UI, from the Dashboard, navigate to the About panel. and click **Firmware Updates**.
2. Save the file to a location accessible to the ACC ES Admin Web UI.

To upgrade the firmware from the ACC ES Admin Web UI:

1. Navigate to the Device panel.
2. If necessary, scroll to show the Upgrade Firmware pane;
3. Use one of these methods:
 - Drag-and-Drop
 1. Use Windows Explorer to navigate to the location of the downloaded firmware file.
 2. Click on the file in the Explorer window and drag it over the **Drop '.fp' file here or click to upload** area.
 - Click to upload
 1. Click in the **Drop '.fp' file here or click to upload** area. The Windows Open dialog box is displayed.
 2. Use Windows Explorer to navigate to the location of the downloaded firmware file.
 3. Click on the file in the Open dialog box and click **Open**.
4. Click **OK** to confirm you want to continue. An upload progress indicator appears. Wait while the file is uploaded and verified. After the file is verified, the device will reboot. The Web UI Communication Lost message appears while the device is rebooting. The process takes several minutes. When the device has rebooted, the connection to the ACC ES Admin Web UI is restored in your web browser.

You can cancel a firmware upgrade that is in progress only during the upload and verification phase.

Click **Cancel upload** before the file has uploaded.

Note: If an error occurs during the upload phase or the upgrade process or if the firmware becomes corrupted, you are prompted to remove the file.

Using the Software Reset Button

If the ACC ES Rugged 8-Port Appliance encounters a system error, and you cannot disconnect it from the power source or power-cycle the appliance, use the reset button while the appliance is still powered on to restart it.

Note: The reset function also resets the camera connections, so you will lose video from any connected cameras during the reset.

The reset button is located behind the locked panel on the front of the ACC ES Rugged 8-Port Appliance:

To reset the appliance:

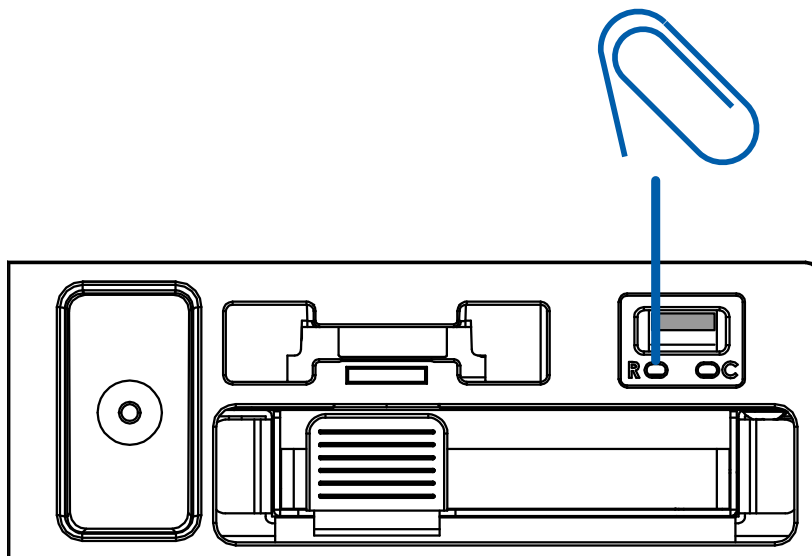
1. Unlock and open the front panel using the provided key.


Tip: Turn the key 180 degrees counter-clockwise to unlock the front panel. The front panel drops down and is attached to the appliance by a strap.

2. After you've located the reset switch on the appliance, use a straightened paperclip or similar tool and gently press and release the reset switch.



Do not apply excessive force. Inserting the tool too far will damage the appliance.



3. Confirm that the appliance has fully restarted and recording has resumed:
 - a. Access the ACC ES Admin Web UI sign in page and log in. For more information, see *Launching the ACC ES Admin Web UI* on page 17.
 - b. On the Storage panel of the web interface launch page, check that the Status is .

Restoring Factory Default Settings

If the ACC Server software no longer functions as expected or if you've forgotten your administrator password, you can restore the ACC ES Rugged 8-Port Appliance to its factory default settings. A USB memory drive is required to complete the restoration process.



CAUTION — Restoring to the factory default settings will delete all configuration settings and recorded video. After the factory default settings are restored, you can restore the most recent system backup from before the functional problems started. You may also have to update the ACC Server software to the most recent release.

1. Prepare the USB memory drive. It must:
 - a. Be FAT32 formatted.
 - b. Contain a file of any size that is named `factory_restore`.
2. Insert the USB memory drive into any of the USB ports.
3. Power cycle the ACC ES Rugged 8-Port Appliance. You can:
 - Unplug the appliance and plug it in again.
 - Reset the appliance (see *Using the Software Reset Button* on page 37)
 - Reboot the appliance from the Device Panel of the Web User Interface (see *Rebooting the Device and Managing Device Settings* on page 21)
4. As soon as the `factory_restore` file is detected as the appliance powers back on again, the current settings and data are deleted, the original factory firmware image is restored, and the ACC ES Rugged 8-Port Appliance is restarted.
5. After the ACC ES Rugged 8-Port Appliance has restarted, launch the Web User Interface and verify that it has been restored to its factory default settings.
6. Remove the USB memory drive.

Important: If you do not remove the USB memory drive after restoring the factory default settings, the restore process will be rerun.

Replacing the Storage SSD

The system settings for the ACC software (including the ACC password, and the settings for the camera connections), as well as the self-learning video analytics rules, any recording licenses, and recorded video, are all stored on the removable storage SSD of the ACC ES Rugged 8-Port Appliance.

If a storage SSD fails none of this data can be retrieved from the failed drive. After a storage SSD fails:

- Deactivate recording licenses added to the ACC ES Rugged 8-Port Appliance before the SSD is replaced. Reactivate the licenses after replacing the SSD.
- Restore the ACC system settings from a site settings backup.

Tip: Start backing up the system settings for the appliance after you configure it so that they can be restored if you ever need to replace the storage SSD.

- Video recordings and video analytics rules start over, as they do on a newly installed appliance.

The storage SSD can be removed and replaced without powering down the appliance. It sits in a tray behind the locked front panel of the appliance. The tray slides in and out of the appliance. You must eject the storage SSD from the appliance before you can safely remove it. You eject it from the Storage panel of the ACC ES Admin Web UI.




All recording and software services on the appliance are stopped if a functioning storage SSD is ejected. Recording will resume after the software services have restarted if the same storage SSD is reinserted into the appliance.



Important: The storage SSD must be replaced with an SSD of the same capacity (2TB for the VMA-RPA-8P2 model, or 4TB for the VMA-RPA-8P4 model).

If the storage SSD is still functioning and needs replacement, replacing a functioning storage SSD requires some downtime. All recording is stopped after the SSD is in the ejected state, and can start only after a backup of the previous settings is restored, or the ACC ES Rugged 8-Port Appliance is reconfigured as though newly installed, and the ACC and recording licenses are reactivated.

Important: Before you can physically disconnect and remove the SSD from the appliance, you must initiate the Eject status on the Storage panel of the web interface launch page.

If you need to replace a failed SSD, use the following procedure:

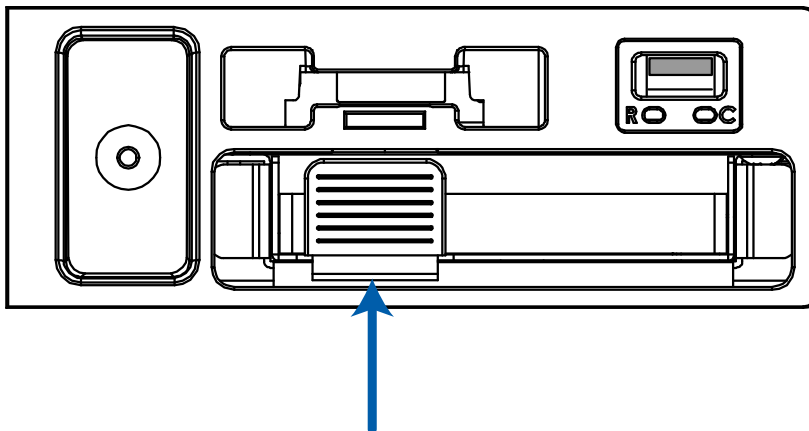
1. Deactivate all the licenses associated with the ACC ES Rugged 8-Port Appliance. For more information on deactivation of site licenses, see the ACC Help or the *Avigilon ACC Client User Guide*.
2. Initiate the Eject status for the SSD:
 - a. Log in to the ACC ES Admin Web UI. For more information, see *Launching the ACC ES Admin Web UI* on page 17.
 - b. Click **Storage** on the navigation bar. For more information, see *Monitoring and Disconnecting the Storage SSD* on page 22.
 - c. On the Storage panel of the web interface launch page, click .

The status changes to  and  changes to , indicating all services have stopped.


3. Unlock and open the front panel using the provided key.

Tip: Turn the key 180 degrees counter-clockwise to unlock the front panel. The front panel drops down and is attached to the appliance by a strap.

4. Locate the blue pull tab of the SSD tray.




5. Removing the SSD:
 - a. With your index finger behind the blue tab, use a small amount of force to pull the tray out of appliance. Opening the tray physically disconnects the SSD from the appliance.

Important: Wait approximately 10 seconds until the Status changes to , which indicates that the appliance has detected the removal of the SSD, before proceeding.



- b. Lift the tray out of the sliding drawer.

- c. Remove the four screws that attach the SSD to the tray. Safely store them to reattach the replacement SSD.
- d. Remove the SSD from the tray.

The status of the SSD in the Storage panel of the web interface launch page remains  while the SSD is removed.

6. Inserting the SSD:

- a. Place the SSD in the tray.
- b. Attach the replacement SSD to the tray.
Use the four screws stored after removing the original SSD.
- c. Put the tray onto the sliding drawer.
- d. Push the blue tab inwards until you hear a faint click as the SSD physically connects to the appliance.

The status of the SSD in the Storage panel of the web interface launch page changes to . When the SSD is physically reconnected the status changes to .

7. Restore the most recent backup of the ACC system settings, or configure the ACC ES Rugged 8-Port Appliance as though newly installed. For more information on backing up the ACC system settings, see the *Avigilon ACC Client User Guide*
8. Reactivate all the licenses used on the ACC ES Rugged 8-Port Appliance. For more information on activation of site licenses, see the ACC Help or the *Avigilon ACC Client User Guide*.

Important: If you cannot reactivate the licenses, contact Avigilon Technical Support.

Troubleshooting

Cannot Discover the Device

If you cannot discover the device using File Explorer (Windows) or Finder (Macintosh) during the hardware installation and it is connected to your network, try the following:

- Access the appliance from your web browser using the URL `https://VMA-RPA-RGD-8Px<serial number>`
- Use the Address Resolution Protocol (ARP) to determine the IP address for the device:
 1. Locate and copy down the MAC Address (MAC) listed on the Serial Number Tag for reference.
 2. Open a Command Prompt window and enter the following command:

```
arp -a
```
 3. Scroll through the response and look for the IP address corresponding to the MAC address.
- Discover the DHCP-assigned IP address from the ACC Client software:
 1. Download and install and open the ACC Client software on to the configuration laptop. For information see *Installing and Starting the ACC Client* on page 27.

Note: The username and password for the Web Interface application is separate from the administrator username and password for the ACC Server.

3. Display the server Setup tab.
4. Open a web browser and enter the IP address in this format: `https://<IP address>`.

Network Configuration

By default, the ACC ES Rugged 8-Port Appliance acquires an IP address on the network through DHCP. If you need to set up the ACC ES Rugged 8-Port Appliance to use a static IP address or any specific network configuration, see *Connecting the Device to Users and Cameras* on page 24 for more information.

Checking System Health

You can check on the health of the system components in the Site Health in the ACC Client software. See the *Windows Help and Support* files for more information.

For More Information

For additional product documentation and software and firmware upgrades, visit [avigilon.com/support](https://www.avigilon.com/support).

Technical Support

Contact Avigilon Technical Support at [avigilon.com/contact](https://www.avigilon.com/contact).

Limited Warranty and Technical Support

Avigilon warranty terms for this product are provided at [avigilon.com/warranty](https://www.avigilon.com/warranty).

Warranty service and technical support can be obtained by contacting Avigilon Technical Support: [avigilon.com/contact-us/](https://www.avigilon.com/contact-us/).