



# User Guide

Avigilon ACC™ ES Rugged 8-Port Appliance

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

© 2021, 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

20210806

# 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
Starting the ACC ES Rugged 8-Port Appliance for the First Time .....	15
Using Server Management .....	16
Starting and Stopping Server Management .....	16
Viewing PoE Port Status .....	17
Manage ACC Services .....	18
Enable ACC Client Users to Archive Video .....	18
Provide Server Logs and System Logs for Support .....	19
Manage Device Settings .....	19
Change the ACC ES Rugged 8-Port Appliance Administrator Password .....	20
Manage Time Settings .....	21
Monitoring and Disconnecting the Storage SSD .....	21
Connect the Device to Cameras and ACC Client Users .....	22
Assigning a PoE Power Budget .....	23
Providing Device Logs for Support .....	24
Installing the ACC Client .....	26
Activate the ACC Software and Connect to Avigilon Cloud Services .....	27
Activate ACC Software and Feature Licenses .....	27
Connect to Avigilon Cloud Services .....	27
Activating a License .....	27
Online Activation .....	28

Offline Activation .....	28
Deactivating a License .....	29
Reactivating a License .....	30
Connecting to External Devices .....	32
LED Indicators .....	33
Budgeting PoE Power .....	34
Manage Certificates .....	35
Replace the Web Certificate .....	35
Upload a Trusted CA Certificate .....	37
Upgrade the Firmware .....	38
Using the Software Reset Button .....	40
Restoring Factory Default Settings .....	42
Replacing the Storage SSD .....	44
Troubleshooting .....	47
Accessing the Server Management page from a Web Browser .....	47
Cannot Discover the Device .....	47
Network Configuration .....	48
Monitoring System Health .....	48
For More Information .....	49

# Introduction

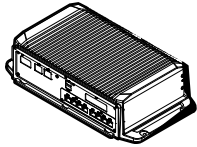

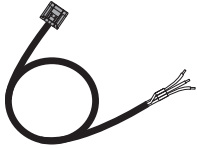
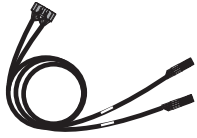

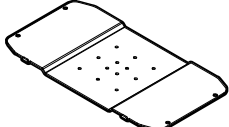


The Avigilon ACC ES Rugged 8-Port Appliance is an all-in-one solution for network video recording incorporating server side video analytics, ruggedly built for installation and use in harsh environments and remote locations. The appliance features:

- 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 ACC ES Rugged 8-Port Appliance to the mounting plate in a plastic bag labeled DIN rail #2	

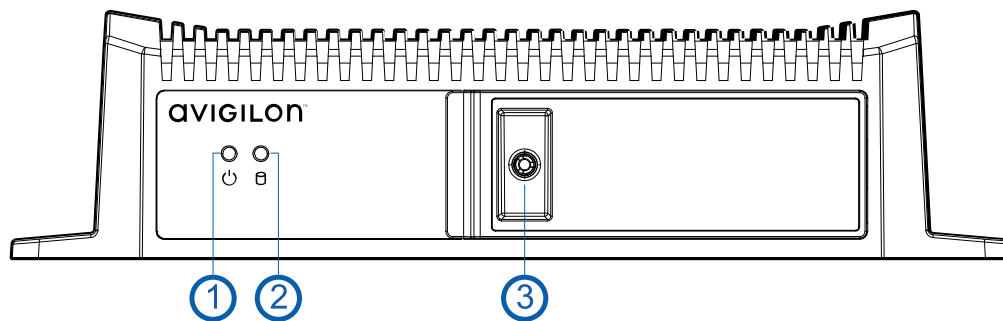
**Important:** For compliance to UL 62368-1, if the ACC ES Rugged 8-Port Appliance is powered by an external power adapter, it must be a UL Listed power adapter suitable for use at Tma is 70C whose output meets ES1 (or SELV) and is rated 9-32Vdc, 100W minimum. Please contact Avigilon for further information.

## 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**

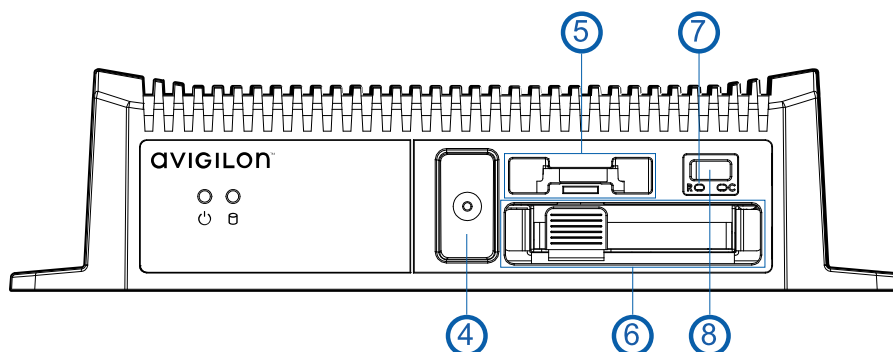
See *LED Indicators* on page 33

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**

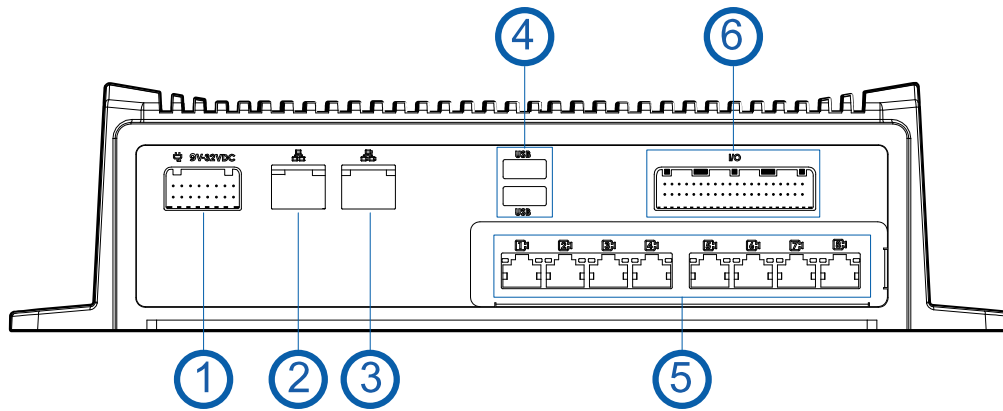
Slide the tray in and out to access the storage SSD. See *Replacing the Storage SSD* on page 44.

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 32.



# 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:

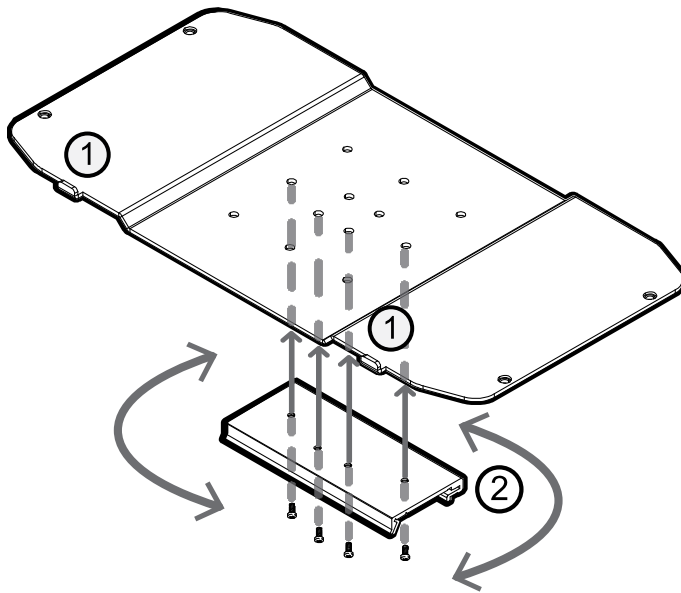
A mounting plate, bracket, and screws to attach the bracket to the plate are provided. The DIN rail bracket clips to a DIN rail with the curved part to the top. The ACC ES Rugged 8-Port Appliance has metal tabs on the rear side that fit into matching slots in the mounting plate.

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.

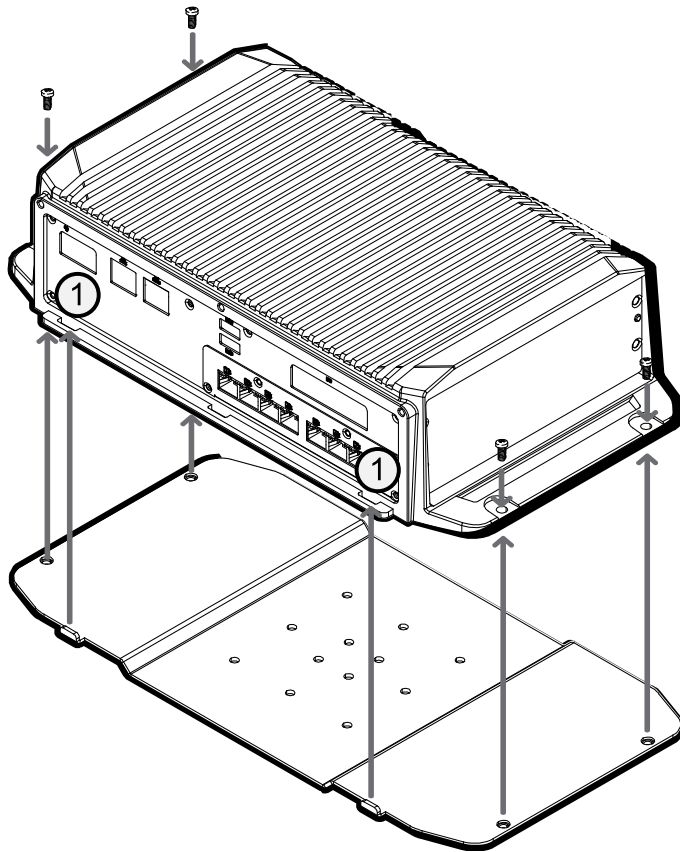


① Indicates the tabs on the mounting plate which fit in to the slots on the rear of the appliance.

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.

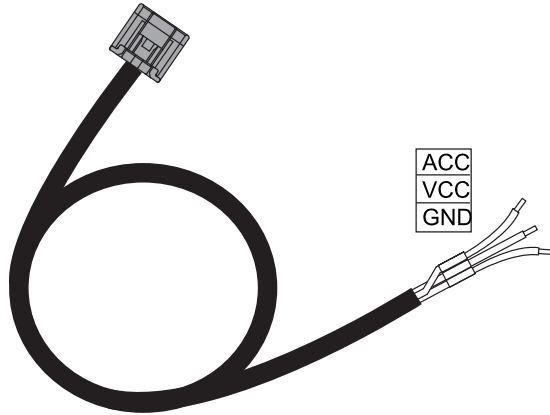


**CAUTION** — The device must be mounted as instructed or any issues that arise will not be covered by the warranty.

# 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.

To connect to a switched power signal (like a vehicle accessory signal in a vehicle), use the ACC wire. The system will turn ON when the ACC wire is connected to the positive side of the power source. The system will go into low-power standby mode when the ACC wire is disconnected from the positive side of the power source.

# Starting the ACC ES Rugged 8-Port Appliance for the First Time

1. Connect a port on the appliance to the local network with an Ethernet cable.
2. On a network workstation, discover the appliance. Use File Explorer on a Windows computer or Finder® on a Macintosh computer.
3. Click past any connection messages displayed by the browser. You will see two warning messages that differ slightly depending on the browser. For example, if the browser is:
  - Chrome—Click **Advanced** on the first screen and **Proceed to <IP address> (unsafe)** on the second screen.
  - Firefox—Click **Advanced** on the first screen and **Add Exception** on the second screen, check **Permanently store this exception**, and click **Confirm Security Exception**.

4. When you are prompted by the Server Management page, 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.

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

The Dashboard panel of the Server Management page is displayed.

6. Set the language for the Server Management page, a user-friendly hostname, and the time zone. In the navigation sidebar, click **Device** to open the Device page. 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 *Manage Device Settings* on page 19.

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

For more information, see *Connect the Device to Cameras and ACC Client Users* on page 22.

For more information about the Server Management page, see *Using Server Management* on page 16

# Using Server Management

The ACC ES Rugged 8-Port Appliance is configured through Server Management, which you can access from the ACC Client application (if you are adding the appliance to an existing multi-server site), or any compatible browser on a workstation on the same network as the appliance. With Server Management you can configure the appliance server settings, set how the server keeps time, and remotely restart or upgrade the server. When the appliance is the first (or only) ACC server deployed at a site, you must access Server Management with a browser, and after you configure the appliance you can download the ACC Client software to the workstation and activate the ACC server software on the appliance. Throughout this section, the term device is used to identify the appliance.



Start backing up the system settings for the appliance 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 Help files provided with the ACC Client software, or the *Avigilon ACC Client User Guide* available from the Avigilon website.

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

## Starting and Stopping Server Management

Start and log in to Server Management from any network workstation with network access to the device, using any of the following methods:

- **Directly from the ACC Client software:**

- a. Start the ACC Client software.
- b. Log in to the site from the System Explorer.
- c. In the New Task menu , click **Site Setup**.
- d. Select the device in the System Explorer and click **Server Management**  to open the device sign-in page.

- **With a bookmark from a web browser:**

Use one of these methods to create a bookmark:

- **Discover the device**

- a. Open the Network tab in File Explorer (Windows) or Finder (Macintosh) to locate the device.
- b. You are looking for a device labeled “VMA-RPA-RGD-8Px-<serial number>” or the hostname you configured in the Server Management page for this device.  
If you cannot locate the device, see *Troubleshooting* on page 47.
- c. Right click and select **View Device Webpage** to open the device sign in page in your default web browser.
- d. Bookmark the device sign in page

- **Use the IP address or hostname**



- a. Open a web browser from a network workstation with network access to the device.
- b. 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/` where 169.254.100.100 is the IP address configured in the Device panel.
- `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.

- c. Bookmark the device sign-in page.

Log out and stop Server Management by clicking the log out icon on the right of the Server Management title bar.

## 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 Server Management
Yellow	Overloaded	A PoE device is connected to the port but is not receiving power. This status typically occurs when one port is over current, 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.

# Manage ACC Services

On the **Server** panel use the:

- General pane:

To...	Do this...
Shut down all the services before you shut down the device.	Click <b>Stop</b> .
Start up all the services after they have been shut down.	Click <b>Start</b> .
Reset the ACC ES Rugged 8-Port Appliance	Click <b>Reset</b>
Format the storage drive.	Click <b>Reinitialize</b> to delete all configuration and recorded video data.

- Network Storage Management pane to enable ACC Client application users to archive video from the ACC ES Rugged 8-Port Appliance. See *Enable ACC Client Users to Archive Video* below
- Service and RTP Ports panes to change the UDP and TCP ports used to communicate with the ACC ES Rugged 8-Port 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.

## Enable ACC Client Users to Archive Video

To allow users of the ACC Client application to archive video from the ACC ES Rugged 8-Port Appliance:

- From the navigation bar, open the **Server** panel.
- In the Network Storage Management pane, click **Enabled**
- 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>*
- In the **Network Path** field, enter the path to the preferred video archiving location.
- If the network location requires authentication, enter the credentials in the **Username** and **Password**

fields.

6. Click **Apply**.

## Provide Server Logs and System Logs for Support

Use the Logs panel to view the Server Logs and System Logs panes and prepare log files requested by Avigilon Technical Support to help resolve an issue.

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.

By default, a log pane displays 100 warning messages from the logs.

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

1. In the drop down list, select the type of logs that you need.
  - For the Server Logs:
    - **Exception Logs**
    - **FCP Logs**
    - **Server Logs**
    - **WebEndpoint Logs**
  - For the System Logs:
    - **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.

## Manage Device Settings

On the navigation bar, click Device.

To...	On the Device panel card...	Setting
Change the language for Server Management	<b>General</b>	Choose your language from the drop down <b>Language</b> list

To...	On the Device panel card...	Setting
Replace the default server name with a user-friendly hostname	<b>Hostname</b>	Change the <b>Hostname</b> . The default hostname is the same as the server name. The server name is in the form <i>&lt;Model&gt;-&lt;Serial Number&gt;</i> .
Set the time zone	<b>Time</b>	Specify the <b>Time Zone</b> and identify the time source in the <b>NTP</b> drop-down and <b>Servers</b> list. See <i>Manage Time Settings</i> on the next page
Change the password for the ACC ES Rugged 8-Port Appliance administrator.	<b>Password</b>	See <i>Change the ACC ES Rugged 8-Port Appliance Administrator Password</i> below.
Install the latest version of the firmware on your device.	<b>Upgrade Firmware</b>	See <i>Upgrade the Firmware</i> on page 38.
Manage the certificates used by Server Management and the ACC ES Rugged 8-Port Appliance.	<b>Certificates</b>	See <i>Manage Certificates</i> on page 35.

## Change the ACC ES Rugged 8-Port Appliance Administrator Password

You can only change the password, not the default *administrator* username for Server Management.

1. On the navigation bar, click **Device**.
2. On the General panel locate the **Password** pane.
3. Enter your current password in the **Old Password** field.
4. Enter your new password in the **New Password** and **Confirm Password** fields.

A complex password is recommended.

Remember to save the password in a secure format and location either physically or digitally so that it can be retrieved if the password is forgotten, and discard the record of the previous password.



**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 42.

## Manage Time Settings

Customize how the ACC ES Rugged 8-Port Appliance keeps time:

1. 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.
2. Select whether you want to keep synchronized time through a Network Time Protocol (NTP) server (recommended) in the NTP field.

**Tip:** To synchronize time with ONVIF devices (that is, non-Avigilon cameras), you can connect to port 123 on the ACC ES Rugged 8-Port Appliance to use it as an NTP server.

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. However, this list is only used if NTP is enabled and not provided by your DHCP server. The default list cannot be rearranged or deleted.

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

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

## 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 solid-state drive (SSD).
- Set the status of the storage SSD to Offline before 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>On the Physical Disks panel, information about each physical disk, including its model and serial number is listed.</p> <p>When the SSD is:</p> <ul style="list-style-type: none"><li>• Correctly working, <b>Ready</b> is displayed.</li><li>• Not correctly working, one of several error states is displayed.</li></ul>
Eject the SSD.	<p>Click . You are prompted to <b>Eject</b> or <b>Cancel</b>. The status changes to <b>Offline</b> and  changes to , indicating all services have stopped. You can now replace the SSD. For more information, .see <i>Replacing the Storage SSD</i> on page 44.</p>

On the **Storage** panel of the AI NVR you can:

## Connect the Device to Cameras and ACC Client Users

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.

**Note:** The corporate network and the camera network must be on different IP subnets.

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.

When connecting an ONVIF device to the camera network, configure it to use the appliance as its time/NTP server.

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 <b>Automatic IP</b> 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"> <li>• <b>IP Address</b></li> <li>• <b>Subnet Mask</b></li> <li>• <b>Default Gateway</b></li> </ul> <p>Click <b>Apply</b> to save your changes.</p>
Set how the device obtains a named address from a DNS server.	<p>Toggle <b>Automatic DNS</b> 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 <b>Automatic DNS</b> 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 34.

**Tip:** If you are using a midspan PoE power injector for cameras that require high power PoE, you should set that PoE port to Off.

To open the PoE panel, either:

- Click  on the PoE status panel on Server Management 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.	<p>Look at the two bars at the top of the panel:</p> <ul style="list-style-type: none"> <li>• The <b>Budget</b> bar indicates the total amount of power budgeted for all devices connected to the PoE ports.</li> <li>• The <b>Consumption</b> bar indicates the actual amount of power currently used by all the connected devices.</li> </ul>

To...	Do this...
Adjust the power used by each PoE port.	Use the <b>Power</b> bar for each port to configure a PoE power budget:
<p><b>Tip:</b> You can also use the <b>Power</b> 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 <b>Auto</b> or <b>Manual</b>.</p>	<ul style="list-style-type: none"> <li>Click <b>Off</b> 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.</li> <li>Click <b>Auto</b> to automatically output power to the connected device depending on its mode of operation.</li> </ul>
<p><b>Tip:</b> 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.</p>	<ul style="list-style-type: none"> <li>Click <b>Manual</b> to enter a power budget value in watts. Make sure the budget includes potential power loss at the cable.</li> </ul>

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.*

Server Management 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:

- In the drop down list, select the type of application log that you need. The options are:
  - System Logs**
  - Boot Logs**
  - Web Server Logs**
- 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 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 Server Management page. Otherwise, add the appliance as a new site in your security network, or merge it into an existing site, using the ACC Client software on a network workstation.

**Important:** Before adding the appliance as a new ACC site, or merging the appliance to an existing ACC Site, first set its IP address. It is highly recommended to be in the same IP subnet as the other servers in the same site.

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](https://www.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.

# Activate the ACC Software and Connect to Avigilon Cloud Services

After you have deployed your ACC ES Rugged 8-Port Appliance , activate your ACC software and feature licenses and connect to Avigilon Cloud Services.

## Activate ACC Software and Feature Licenses

You can activate, deactivate, and reactivate product or feature licenses. Licenses are called Product Keys in the ACC system, and Activation IDs in the licensing portal.

**Important:** When a new server is added to or removed from a multi-server site, the existing site licenses become inactive and must be reactivated to confirm system changes. See *Reactivating a License* on page 30

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

Printable versions of these guides are available on the Avigilon website: [avigilon.com/support/software/](https://www.avigilon.com/support/software/).

Once your license is activated, you can immediately use the new licensed features.

## Connect to Avigilon Cloud Services

After activating your ACC software, you can connect your ACC site to the cloud, which may require a subscription, and take advantage of the capabilities and features that provide centralized access across distributed systems.

To connect your site to Avigilon Cloud Services, see [help.avigilon.com/cloud](https://help.avigilon.com/cloud).

For information about the cloud services, see [Avigilon Cloud Services Support](#).

You can start to back up the system settings for your new site in the ACC Client software after it is configured. 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*.



## Activating a License

Once your license is activated, you can immediately use the new licensed features.

**Tip:** Finish organizing your multi-server site before activating a new license to avoid reactivating the site license each time a new server is added.

## Online Activation

If you have internet access, use online activation. However, if your site is large and contains hundreds of licenses, the server may time out. See *Offline Activation* below instead.

1. In the New Task menu , click **Site Setup**.
2. Select your new site, then click .
3. Click **Add License...**
4. Enter your product keys.

If you copy and paste more than one comma-separated product key, the system will format it automatically.



- To remove the last product key, click **Remove Last Key**.
- To clear all the product keys, click **Clear**.

5. Click **Activate Now**.
6. Click **OK**.

## Offline Activation

Offline licensing involves transferring files between a computer running the ACC Client software and a computer with internet access.

**In the ACC Client:**

1. In the New Task menu , click **Site Setup**.
2. Select your new site, then click .
3. Click **Add License...**
4. Select the **Manual** tab.
5. Enter your product keys.

If you copy and paste more than one comma-separated product key, the system will format it automatically.

- To remove the last product key, click **Remove Last Key**.
- To clear all the product keys, click **Clear**.

6. Click **Save File...** and choose where you want to save the `.key` file. You can rename the file as required.
7. Copy the `.key` file to a computer with internet access.

#### In a browser:

1. Go to [activate.avigilon.com](https://activate.avigilon.com).
2. Click **Choose File** and select the .key file.
3. Click **Upload**. A capabilityResponse.bin file should download automatically.  
If not, allow the download to occur when you are prompted.
4. Complete the product registration page to receive product updates from Avigilon.
5. Copy the .bin file to a computer running the ACC Client software.

#### In the ACC Client:

1. In the License Management dialog box, click **Apply....**
2. Select the .bin file and click **Open**.
3. Click **OK** to confirm your changes.

## Deactivating a License

**Note:** A license can be deactivated a limited number of times. If you encounter an error while activating a previously deactivated license, this may be the issue. Contact Avigilon Technical Support for help.

You can deactivate individual licenses and activate them on a different site. For example if you are upgrading your server hardware, you can deactivate the license on the older server then activate the same license on the new server.

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click .
3. Select the licenses you want to deactivate.
4. Click **Remove License....**
5. To keep a record of the license, click **Copy to Clipboard** and paste into a text file.

#### If you have Internet access:

- Click **Deactivate Now**.

#### If you do not have Internet access:

**Note:** You will need a [licensing.avigilon.com](https://licensing.avigilon.com) account. Contact your organization's Technical Contact for access.

1. Select the **Manual** tab.
2. Click **Save File...** and choose where you want to save the `.key` file.  
The license is deactivated.
3. Copy the `.key` file to a computer with internet access:
  1. Go to [activate.avigilon.com](https://activate.avigilon.com).
  2. Click **Choose File** and select the `.key` file.
  3. Click **Upload**. A `capabilityResponse.bin` file should download automatically.  
If not, allow the download to occur when you are prompted.
  4. Complete the product registration page to receive product updates from Avigilon.
  5. Copy the `.bin` file to a computer running the ACC Client software.



You can now reactivate the license on a new site.

## Reactivating a License

FOR ENTERPRISE EDITION

When servers are added to or removed from a site, the site licenses become inactive and must be reactivated to confirm system changes.

If you do not reactivate the affected licenses, the site will stop normal operations.

1. In the New Task menu , click **Site Setup**.
2. Click the site name, then click .
3. Click **Reactivate Licenses...**

**If you have Internet access:**

1. Click **Reactivate Licenses**.
2. Click **OK** to confirm your changes.

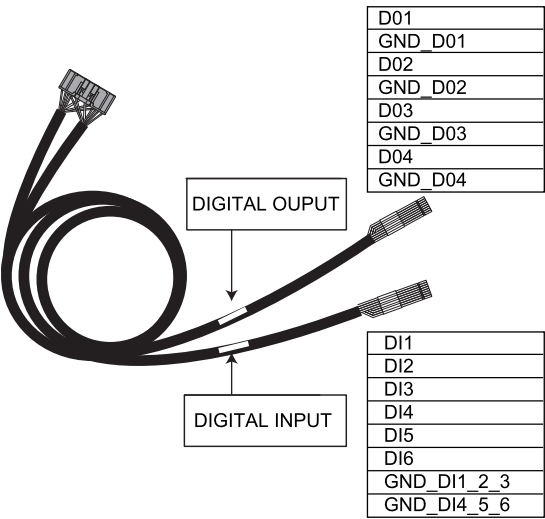
**If you do not have Internet access:**

1. Select the **Manual** tab.
2. Click **Save File...** and choose where you want to save the `.key` files.
3. Copy the `.key` files to a computer with internet access:
  1. Go to [activate.avigilon.com](https://activate.avigilon.com).
  2. Click **Choose File** and select the `.key` file.
  3. Click **Upload**. A `capabilityResponse.bin` file should download automatically.  
If not, allow the download to occur when you are prompted.
  4. Complete the product registration page to receive product updates from Avigilon.
  5. Copy the `.bin` file to a computer running the ACC Client software.

4. In the License Management dialog box, click **Apply....**
5. Select the `.bin` file and click **Open**.
6. Click **OK** to confirm your changes.

# 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.







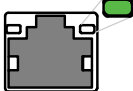


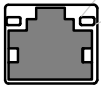


Pin	Function	Description
DI1	IN1	<b>Alarm Inputs</b> — Active-Low inputs. To activate, connect the Input to the Ground pin (GND). To deactivate, leave disconnected.
DI2	IN2	
DI3	IN3	
DI4	IN4	
DI5	IN5	
DI6	IN6	
GND_DI1_2_3	Ground pin for Inputs 1, 2, and 3	
GND_DI4_5_6	Ground pin for Inputs 4, 5, and 6	
D01	OUT1	<b>Outputs</b> — Form-A dry contact outputs. When active, terminals are connected. When inactive, terminals are disconnected.  <b>Note:</b> Contacts are normally open.  Maximum load is 48V, 0.3A.
GND_D01		
D02	OUT2	
GND_D02		
D03	OUT3	
GND_D03		
D04	OUT4	
GND_D04		



# 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	Storage drive activity
Back LEDs	PoE Switch		Left	On: Port is delivering PoE power
			 	Off: Port is not delivering PoE power
			Yellow	Blinking: Port is not delivering PoE power but PoE camera is connected
			Right	On: Network link is present
Corporate & Camera Uplink Ports				Off: Network link is not present
			Green	Blinking: Network activity is present
			Right	On: Network link is present
			 	Off: Network link is not present
			Green	Blinking: Network activity is present

# 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:

$$\text{Power budget} = \text{<Camera power consumption>} + \text{<Expected cable power loss>}$$

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

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

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.

# Manage 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 Server Management and to the WebEndpoint service, and a set of system-level signed certificates from well-known trusted Certificate Authorities (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 Server Management 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 the 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, the ACC software 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 system-level 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 Server Management 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.

## Replace the Web Certificate

Manage the device's Web Certificate from the Web Certificate tab on the Certificates pane. Server Management 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 custom certificate.

**Important:** When you reset the device to its factory settings (also known as a factory reset), you need to reload your custom 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 Server Management:
  - a. Open Server Management, 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 Server Management, 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 Server Management, 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 Server Management, 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.

# Upgrade the Firmware

Upgrade the firmware to ensure the ACC ES Rugged 8-Port Appliance is operating with the latest software. When you upgrade the firmware, all your current settings and all recorded video are retained.

Upgrade the firmware in any of the following ways:

- You can use Cloud Remote Site Upgrade from Avigilon Cloud Services to update:
  - the firmware on the ACC ES Rugged 8-Port Appliance,
  - the firmware on all other Avigilon servers,
  - the firmware on all Avigilon cameras, and
  - the ACC Client software on all network workstations

in the same site all at the same time.

A subscription to the Advanced System Health feature package is required. This is the Avigilon recommended way to quickly and efficiently complete site-level upgrades. Refer to the procedure for upgrading servers in a site in the Help files provided with Avigilon Cloud Services.

- You can use Remote Site Upgrade from an ACC Client connected to all of the ACC ES Rugged 8-Port Appliances in a site at the same time. Refer to the procedure for upgrading servers in a site in the Help files provided with the ACC Client.
- You can use the Server Management page, using the following procedure.

Before you can upgrade or reinstall the firmware with the Server Management page, download the latest version of the firmware (.fp) file from the Avigilon [Support Community](#).

From a workstation connected to the Internet:

1. Navigate to [support.avigilon.com](https://support.avigilon.com) and search for the appropriate ACC ES Rugged 8-Port Appliance firmware.

**Note:** To download firmware you must have, or create an account and be logged into the Community.

2. Save the file to a location accessible to the Server Management page.

To upgrade the firmware from the Server Management page:

1. Navigate to the Device panel.  
If necessary, scroll to show the Upgrade Firmware pane.
2. In the Upgrade Firmware pane, click on **Drop '.fp' file here or click to upload** and navigate to the location where the firmware package (.fp) file was saved.
3. Click **OK** to confirm you want to continue. An upload progress indicator appears. Wait while the file is uploaded and verified.

**Important:** 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.

After the file is verified, the firmware upgrade automatically starts. The device will reboot several times during the upgrade. 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 Server Management page is restored in your web browser.

**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 all recorded videos during the reset. The appliance will not be recording during the reset. However, recorded videos will not be lost.

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

To reset the appliance:

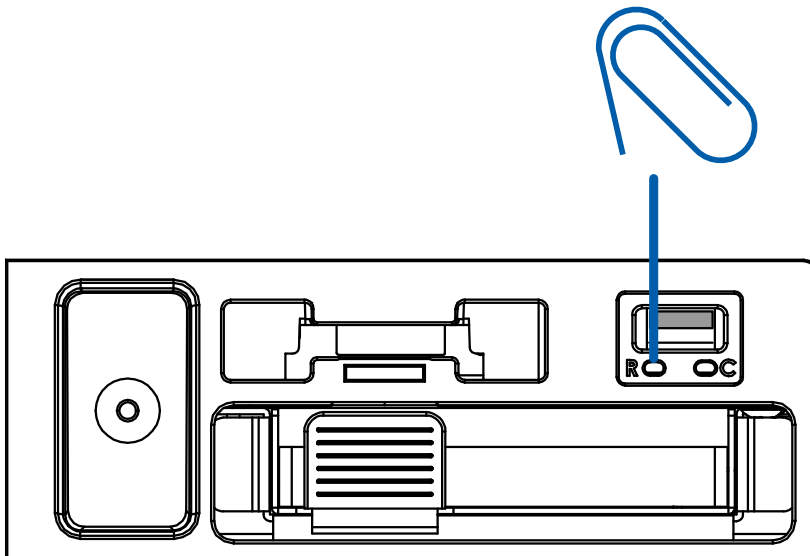
1. Unlock and open the front panel using the provided key.

**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 and void the warranty.





3. Confirm that the appliance has fully restarted and recording has resumed:
  - a. Access the Server Management page sign in page and log in. For more information, see *Starting and Stopping Server Management* on page 16.
  - 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.

**Note:** Restoring to the factory default settings will delete all configuration settings, including any custom certificate you have installed, 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 reload the custom certificate, and update the ACC Server software to the most recent release.

If the appliance is part of a merged Site or parent-child Site family configuration, there are additional steps you must complete in the ACC Client software, which are specified in this procedure.

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. If the appliance is part of a merged Site or parent-child Site family configuration:
  - a. Remove it from the Site before doing the reset.
  - b. If the appliance is not part of a merged Site, deactivate the licenses.
4. 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 40)
  - Reboot the appliance from the Device Panel of the Web User Interface (see *Manage Device Settings* on page 19)
5. 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.
6. 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.
7. 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.

8. If necessary, upgrade the appliance's firmware.

9. If the appliance is part of a Site cluster or parent-child Site family configuration:
  - a. Access the WebUI and reenter the correct IP address via its web UI. It is highly recommended to be in the same IP subnet as the other servers in the ACC Site.
  - b. If the appliance is not part of a merged Site, activate its licenses.
  - c. Merge or connect the appliance back to the Site or Site family.

# Replacing the Storage SSD

You can replace the storage SSD of the ACC ES Rugged 8-Port Appliance that has failed or is still functioning. It 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.

**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).

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.

The Web UI administrator password, the appliance's IP address and the NTP configuration settings are not stored on the SSD, and will not be lost.

**Tip:** Start regularly 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.

Whether replacing a failed SSD or a functioning one, some downtime is required. All recording is stopped as soon as 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.

**Before** a storage SSD is replaced, you must deactivate recording licenses added to the ACC ES Rugged 8-Port Appliance. See *Deactivating a License* on page 29

**After** the SSD is replaced:

- Reactivate the licenses. See *Reactivating a License* on page 30.
- Restore the ACC system settings from a site settings backup.


**Tip:** It is recommended that you restore the system settings before upgrading the firmware on the appliance, if a more recent version of the firmware for the appliance is available.


- Upgrade to the latest version of the firmware, if one is available
- Video recordings and video analytics rules start over, as they do on a newly installed appliance.

To replace a storage 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:

**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.

- a. Log in to the Server Management page. For more information, see *Starting and Stopping Server Management* on page 16.
- b. Click **Storage** on the navigation bar. For more information, see *Monitoring and Disconnecting the Storage SSD* on page 21.
- c. On the Storage panel of the web interface launch page, click .

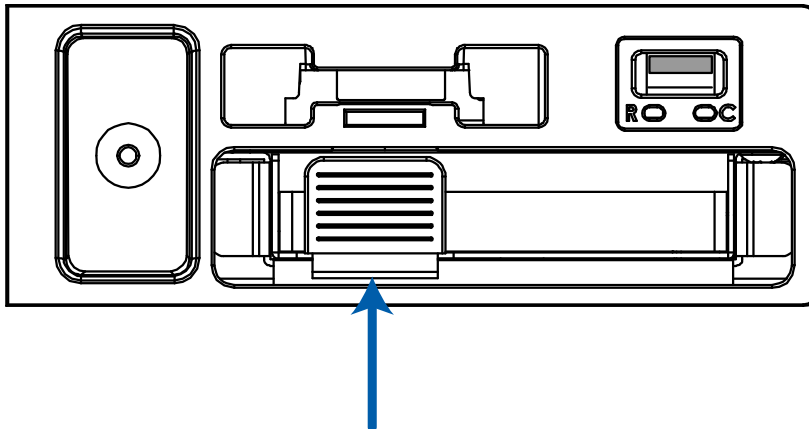
The status changes to  and  changes to , indicating all services have stopped.

**Note:** 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.

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 *AvigilonACC Client User Guide*
8. Install the latest version of the appliance firmware if a newer version is available. For more information, see *Upgrade the Firmware* on page 38.
9. 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 at [avigilon.com/contact](https://www.avigilon.com/contact).

# Troubleshooting

## Accessing the Server Management page from a Web Browser

There may be cases where you want to access the Server Management page without using the ACC Client.

You can access the Server Management page from any Windows®, Apple, or mobile device using most popular web browsers.

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

1. On a network workstation, discover the appliance. Use File Explorer (Windows) or Finder® (Apple). You are looking for a device labeled “VMA-RPA-RGD-8Px-<serial number>” or the hostname you configured in the Server Management page for this device.
2. Click past any connection messages displayed by the browser. You will see two warning messages that differ slightly depending on the browser. If the browser is:
  - Chrome—Click **Advanced** on the first screen and **Proceed to <IP address> (unsafe)** on the second screen.
  - Firefox—Click **Advanced** on the first screen and **Add Exception** on the second screen, check **Permanently store this exception**, and click **Confirm Security Exception**.
3. Log in as administrator.  
The Dashboard panel of the Server Management page is displayed.

## Cannot Discover the Device

There are several ways you can discover a device that is supposed to be connected to your network from a network workstation. The recommended order to discover a device is:

- Check that the appliance is connected to the local network with an Ethernet cable.
- Using File Explorer (Windows) or Finder (Apple)  
You are looking for a device labeled “VMA-RPA-RGD-8Px-<serial number>” or the hostname you configured in the Server Management page for this device.

- Discover the DHCP-assigned IP address from the ACC Client software:
  - Log into the site that uses this naming convention: VMA-RPA-RGD-8Px-<serial number>

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

- 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.

If none of the above suggestions resolve the problem, contact Avigilon Technical Support.

## 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 *Connect the Device to Cameras and ACC Client Users* on page 22 for more information.

## Monitoring System Health

You can monitor the health of the system components in the Site Health in the ACC Client software. See the Help files provided with the ACC Client software, or the *Avigilon ACC Client User Guide* available from the Avigilon website for more information.



## For More Information

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

## Technical Support

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

## Limited Warranty

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