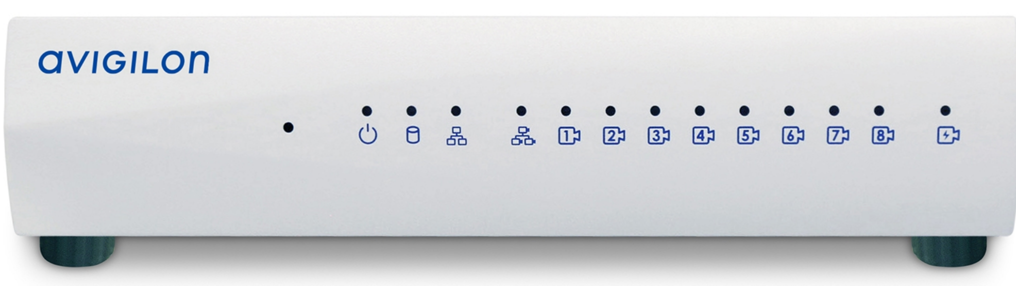
a Motorola Solutions Company

User Guide



Avigilon ACC™ ES 8 Port Appliance

VMA-ENVR1-8P4
VMA-ENVR1-8P8
VMA-ENVR1-8P8B

Important Safety Information

This manual provides installation and operation information and precautions for the use of this device. Incorrect installation could cause an unexpected fault. Before installing this equipment read this manual carefully. Please provide this manual to the owner of the equipment for future use.

The Warning symbol indicates the presence of dangerous voltage within and outside the product enclosure that may constitute a risk of electric shock, serious injury or death to persons if proper precautions are not followed.

The Caution symbol alerts the user to the presence of hazards that may cause minor or moderate injury to persons, damage to property or damage to the product itself if proper precautions are not followed.

WARNING — Failure to observe the following instructions may result in severe injury or death.

- Installation must be performed by qualified personnel only and must conform to all local codes.
- Do not open or disassemble the device. There are no user serviceable parts.
- The coin cell battery is not replaceable.

CAUTION — Failure to observe the following instructions may result in injury or damage to the appliance.

- Do not subject cables to excessive stress, heavy loads or pinching.
- Do not operate in dusty areas.
- This device is for indoor use only.
- Do not expose this product to rain or use near water. If this product accidentally gets wet, unplug it immediately.
- Keep product surfaces clean and dry. To clean the outside case of the device, gently wipe using a lightly dampened cloth (only use water, do not use solvents).
- Do not install near any sources of vibration, such as motors.
- Do not install near any heat sources such as radiators or other sources of heat.
- Do not block ventilation openings located on the device enclosure as they are designed to keep the system cool while running. Install or place this product in an area where there is ample air circulation.
- Do not insert anything into the device ventilation openings.
- Use only accessories recommended by Avigilon.
- Keep these safety instructions.

Regulatory Notices

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This Class B digital apparatus complies with Canadian ICES-003 (B)/NMB-3(B)

This equipment is to be connected only to PoE networks without routing to the outside plant.

The battery isn't user replaceable or service replaceable.

Changes or modifications made to this equipment not expressly approved by Avigilon Corporation or parties authorized by Avigilon Corporation could void the warranty and affect the user’s ability to operate this equipment.

Disposal and Recycling Information

When this product has reached the end of its useful life, please dispose of it according to your local environmental laws and guidelines.

Risk of fire, explosion, and burns. Do not disassemble, crush, heat above 100 °C (212 °F), or incinerate.

European Union:

This symbol means that according to local laws and regulations your product should be disposed of separately from household waste. When this product reaches its end of life, take it to a collection point designated by local authorities. Some collection points accept products for free. The separate collection and recycling of your product at the time of disposal will help conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment.

Avigilon Corporation
avigilon.com

PDF-VMA-ENVR1-8P-B

Revision: 5 - EN

20200814

Table of Contents

Introduction

The Avigilon ACC ES 8 Port Appliance is the all-in-one solution for network video recording. The recorder features:

- A network switch to connect and power IP cameras.
- Built-in server to run the Avigilon Control Center Server Software.
- Local video content storage that can be accessed remotely.

The ACC ES 8 Port Appliance factory default settings allow you to use the recorder immediately after installation, but if you have special requirements, you can use the Avigilon Control Center software or the web interface to customize your settings.

Before You Start

Avigilon recommends the use of an uninterruptible power supply (UPS) system to protect your video surveillance system hardware. A UPS system is used to protect critical equipment from mains supply problems, including spikes, voltage dips, fluctuations and complete power failures using a dedicated battery. It can also be used to power equipment during the time it takes for a standby generator to be started and synchronized.

Any UPS connection must include configuration to shut down the operating system on the appliance when battery power is low or there is 15 minutes of power remaining.

It is recommended that cameras not be connected to the appliance until after the appropriate network configuration has been set up.

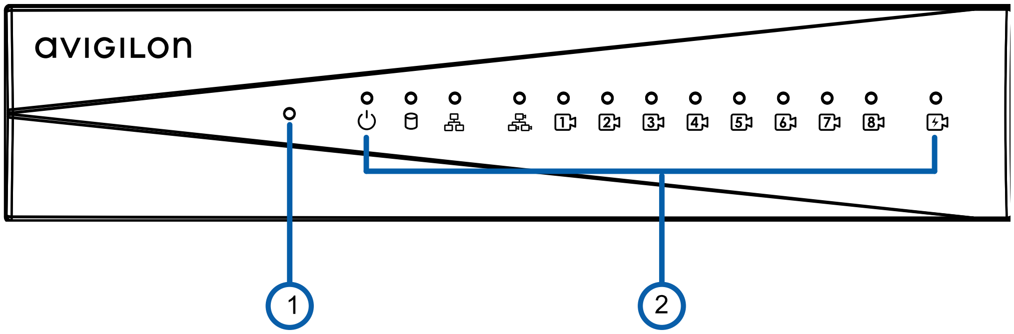
Package Contents

Ensure the package contains the following:

- Avigilon Video Appliance
- Power cord
- Power supply and screwdriver to secure it
- Wall installation hardware
- Digital input/output terminal block connector

Overview

Front View



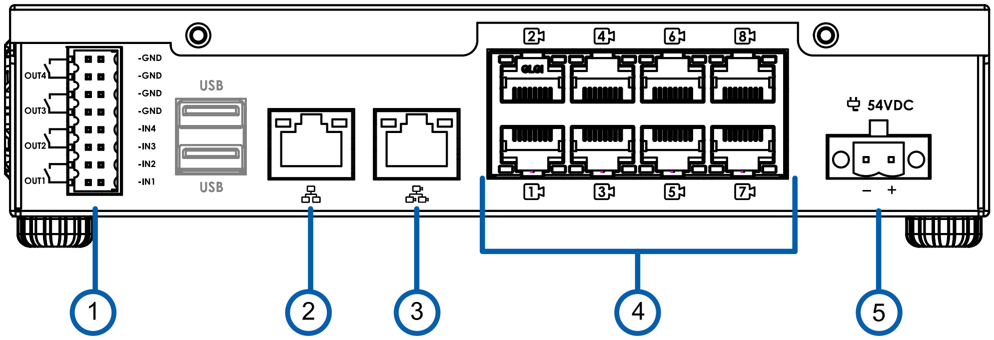
1. **Reset button**

   Use this button to physically restart the appliance or perform a factory reset.

2. **Status LED**

   Provides information about daily operations. For more information, see *LED Indicators* on page 22.

Rear View



1. **I/O connector**

   Provides connections to external input/output devices. For more information, see *Connecting to External Devices* on page 20.

2. **Corporate network uplink port**

   Accepts a 1GbE Ethernet connection to the general network to allow users access to the web interface of the appliance.

3. **Camera network uplink port**

   Accepts a 1GbE Ethernet connection to the cameras that are connected to the PoE switch component. Can be used to link to other PoE switches and cameras, and to access the web interface of any connected camera video.

4. **PoE switch component**

   Connect cameras to the 10/100 speed PoE switch component to power the cameras and record video.

5. **Power connector**

   Accepts power to the appliance.

System Requirements

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.

Installing and Connecting the Hardware

Install the ACC ES 8 Port Appliance in a location free of dust and particles, vibration, and within the specified operating temperature range. Otherwise any issues that arise will not be covered by the warranty.

The ACC ES 8 Port Appliance can be installed as a stand-alone device, mounted on a wall using the supplied mounting brackets, or kept in a server rack using the optional Rack Mount Shelf With Sliding Rails accessory kit.

1. Note down the serial number, located on the label on the underside of the device.
2. If required, mount the ACC ES 8 Port Appliance on a wall using the supplied mounting brackets.

   > **Tip:** You may want to do this step before or after you have made all the required connections depending on where you want to mount the device.

   a. Unscrew the feet on the device and attach the wall mount brackets to the lowest threaded holes on the sides of the ACC ES 8 Port Appliance.
   b. Position the device with the rear panel facing downwards.
   c. Screw the wall mounting brackets to the wall.
3. If required, install the ACC ES 8 Port Appliance in a server rack using the optional Rack Mount Shelf With Sliding Rails accessory kit. Attach the device to the tray and sliding rails, following the instructions provided in the assembly kits.
4. Connect the cameras to the PoE ports.
5. Connect the *corporate network* port on the device to the local network with an Ethernet cable.
6. Connect power and wait for the device to start up. Wait for the power LED to turn green to indicate that the device is turned on and the PoE LED to turn orange to indicate power is provided to all connected PoE devices. It may take several minutes for the power LED to turn green the first time the device is powered on.

   > **Note:** The PoE LED initially shows that PoE is provided to all connected devices, but the status may change if the system detects that the total power consumption exceeds the PoE limits. If the LED is blinking, go to the **PoE** tab in the Network panel of the ACC ES 8 Port Appliance Web Interface after you have activated the device to resolve the power budgeting for each port. For more information, see *Assigning a PoE Power Budget* on page 15.

Starting the ACC ES 8 Port Appliance for the First Time

After powering on the ACC ES 8 Port Appliance, complete the following procedure:

1. Connect a port on the appliance to the local network with an Ethernet cable.
2. Check that the appliance LED indicators display the correct status. See *LED Indicators* on page 22 for more information.
3. On a network workstation, discover the appliance. Use File Explorer on a Windows computer or Finder® on a Macintosh computer.

   You are looking for a device labeled "VMA-ENVR1-8Px-xxxxxxxxxx" or "VMA-ENVR1-8P8B-xxxxxxxxxx", where xxxxxxxxxx is the serial number of your appliance. If you cannot locate the appliance, see *Troubleshooting* on the next page.
4. Click to open the device in a supported web browser. For a list of supported web browsers, see *System Requirements* on page 3.

   > **Important:** The ACC ES 8 Port Appliance is configured with a self-signed certificate, which generates a connection warning in the web browser.

5. 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**.
6. When you are prompted by the Web Interface, 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.
7. Enter `administrator` as the username and your new password.

   The Dashboard panel of the Web Interface is displayed.

8. Set the language for the Web Interface, 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 12.

9. 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 14.

For more information about the Web Interface, see *Configuring the Appliance* on page 9

All ACC ES 8 Port Appliance models are preinstalled with the ACC 7 Server software. An ACC ES 8 Port Appliance can be deployed as a stand-alone ACC site, or if you are adding it to an existing ACC 7 deployment, it can merged into an existing site , or added as a new site.

Tip: If you are using an ACC 6 deployment, you can downgrade the ACC ES 8 Port Appliance models VMA-ENVR1-8P4 and VMA-ENVR1-8P8 only to run the ACC 6 Server software, and add them to the deployment. Downgrade before you start using the preinstalled ACC Server software. The server-side video analytics features are not supported after downgrading to the ACC 6 Server software. When you downgrade, all the configured settings are lost, and all recorded video is deleted. For more details see the *ACC ES 8 Port ApplianceACC Downgrade Guide*.

The ACC ES 8 Port Appliance model VMA-ENVR1-8P8B cannot be downgraded to run the ACC 6 Server software. The error message “Invalid firmware package” appears if you attempt to upload the ACC 6 firmware (.fp) file for the VMA-ENVR1-8Px models to a VMA-ENVR1-8P8B.

You are now ready to install the ACC Client software and connect the ACC ES 8 Port Appliance to an ACC site.

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 https://VMA-ENVR1-8P-<serial number> or https://VMA-ENVR1-8P8B-<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 18.
  2. Log into the site that uses this naming convention: VMA-ENVR1-8Px-<serial number> or VMA-ENVR1-8P8B-<serial number>.

     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>`.
  5. Continue the remaining steps for installing the appliance.

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

Network Configuration

By default, the ACC ES 8 Port Appliance acquires an IP address on the network through DHCP. If you need to set up the ACC ES 8 Port Appliance to use a static IP address or any specific network configuration, see *Connecting the Device to Users and Cameras* on page 14 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 **Site Health** in the *ACC Client User Guide* for more information.

Configuring the Appliance

The ACC ES 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 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-ENVR1-8P-<serial number>" or “VMA-ENVR1-8P8B-<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 username is always `administrator`. Use the password you configured when you logged in to the device for the first time. For more information, see *Installing and Connecting the Hardware* on page 5.

   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.

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 the next page
  - The **Logs** page to view ACC Server service logs. See *Providing Service Logs for Support* on page 12.
- **System** — Access the five options to configure the device and view its status:
  - **Device**. See:
    - *Rebooting the Device and Managing Device Settings* on page 12
    - *Upgrading the Firmware* on page 27
    - *Managing Certificates* on page 24
  - **Storage**. See *Monitoring the Storage Drive State* on page 14.
  - **Network**. See *Connecting the Device to Users and Cameras* on page 14.
  - **Logs**. See *Providing Device Logs for Support* on page 17

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	PoE+ is turned on.

	powered	
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 infomation see, *Launching the ACC ES Admin Web UI* on page 9).
    - 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. This will also format the hard drives and delete the configuration data and recorded video. For more information on performing a factory restore, see *Restoring Factory Default Settings* on page 29.

- **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 27.
- **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 24.

Monitoring the Storage Drive State

On the **Storage** panel you can view the storage capacity of the device and the status of the storage drive on ACC ES 4- and 8-port appliances (or drives on older 4-port ACC ES appliances).

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 storage drive.	When the device is: • Correctly working, Ready and is displayed. • Not correctly working, Error and is displayed.
View details about the drive.	1. Click the 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.

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.

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.

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 ACC Site.

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 if the appliance is running ACC 7.x or later.

For more information about the network connections, see *Supported Network Configurations* on page 4.

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.	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: • **IP Address** • **Subnet Mask** • **Default Gateway** Click **Apply** to save your changes.
Set how the device obtains a named address from a DNS server.	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.

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 23.

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

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, 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 existingACC Site, first set its IP address. It is highly recommended to be in the same IP subnet as the other servers in the ACC 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**. 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**.

Connecting to ACC Software and ACS

Once you have deployed your appliance, you should activate your ACC software and connect to Avigilon Cloud Services (ACS).

Activating and Configuring ACC Software

- **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/**.

Connecting to Avigilon Cloud Services

After activating your ACC software, you can connect your ACC site to the cloud, free of charge, 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**.

For information about the cloud services, see **Avigilon Cloud Services Support**.

Starting Up and Shutting Down the ACC Client Software

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**.

Connecting to External Devices

External devices are connected to the appliance through the I/O terminal. The pinout for the I/O terminal is shown in the following diagram:

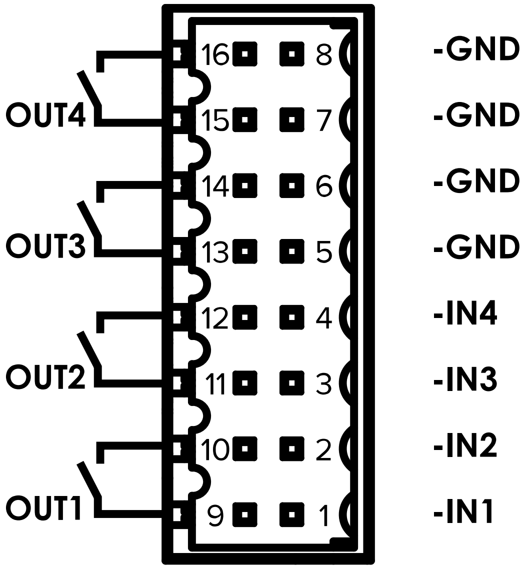


Figure 1: ACC ES 8 Port Appliance I/O pins are numbered as shown in the image above.

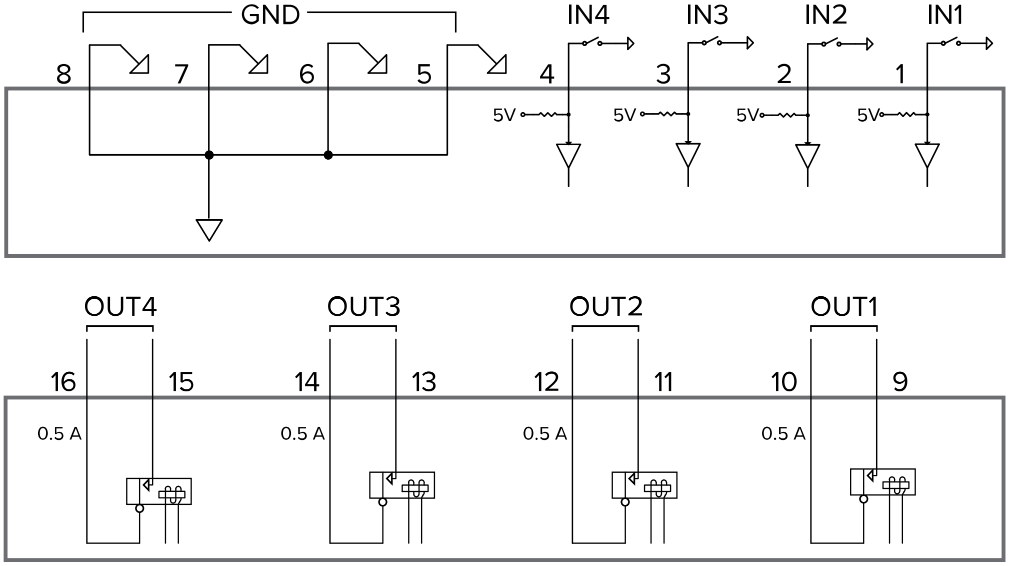


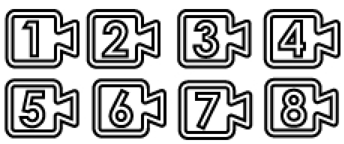
Figure 2: The diagram above shows the pinouts for the I/O terminal.

Pin	Function	Description
1	IN1	Alarm Inputs — Active-Low inputs. To activate, connect the Input to the Ground pin (GND). To deactivate, leave disconnected.
2	IN2	
3	IN3	
4	IN4	
5	GND	
6		
7		
8		
9	OUT1	Relay Outputs — Form-A dry contact outputs. When active, terminals are connected. When inactive, terminals are disconnected. Maximum load is 30 V, 0.5 A.
10		
11	OUT2	
12		
13	OUT3	
14		
15	OUT4	
16		

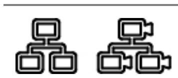
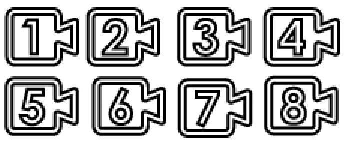
LED Indicators

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

Front Panel LEDs

Icons	LED Status	Description
	Green	Device is powered and running.
	Orange	Device is restarting.
	Orange - blinking	Factory restore button pressed.
	Green	Hard disk drive is connected.
	Red	Hard disk drive connection has an error.
	Green	Link is present.
	Orange	Power is off due to failure.
	Green - blinking	Port activity.
	Orange	10/100 network link is present.
	Orange - blinking	Port activity
	Green	GigE network link is present.
	Green - blinking	Port activity
	Orange	Switch component has reached its PoE output capability.
	Orange - blinking	Over budget.

Back Panel LEDs

Icons	LED Status	Description
	Green	Network activity is present.
	Orange	On for GigE speed. Off for 10/100 Mbps speed.
	Green	Network activity is present.
	Orange	On for 100 Mbps speed. Off for 10 Mbps speed.

Budgeting PoE Power

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 (<=) 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:

Power budget = <*Camera power consumption*> + <*Expected cable power loss*>

Example: Connect the following 8 cameras to an 8-port device:

4 x HD dome cameras	(9 W + 2.5 W) x 4	= 46 W
2 x HD PTZ camera	(25.5 W + 4.5 W) x 2	= 60 W
2 x HD micro dome	(4 W + 2.5 W) x 2	= 14 W
	Total	= 120 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 ACC 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 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 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 uploadarea.
        - 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 uploadarea. 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 theUser 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 theCertificates pane.
2. Click the User Certificate Authorities tab.
3. Click Upload.
4. In theUpload 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.

Choosing to upgrade corrupted firmware helps you avoid reverting to the factory default settings. When you revert to the factory default settings, all of the configured settings are lost and all recorded video is deleted.

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**.

   Otherwise, from a workstation connected to the Internet, navigate to **partners.avigilon.com** and download the appropriate ACC ES firmware.

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 Reset Button

The reset button is located at the front of the appliance and is the small unlabeled circle to the left of the System Status LED. For more information, see *Front View* on page 2

The reset button provides two functions:

- Restart the system — If the appliance encounters a system error, you can force it to restart.
- Restore the factory default settings — If the ACC software no longer functions as expected, you can reset the appliance to its factory default settings. All configuration settings and recorded data will be deleted.

Note: When you use the reset button, the appliance must be powered.

Restarting the System

- Using a straightened paperclip or similar tool, gently press and release the reset button.

  CAUTION — Do not apply excessive force. Inserting the tool too far will damage the recorder and void the warranty.

Important: Do not hold down the reset button for too long or you will revert to the factory default settings.

Restoring Factory Default Settings

If the ACC Server software no longer functions as expected or if you've forgotten your administrator password, you can reset the appliance to its factory default settings.

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.

1. Using a straightened paperclip or similar tool, gently press and hold the reset button.

   ⚠ **CAUTION —** Do not apply excessive force. Inserting the tool too far will damage the recorder and void the warranty.

2. Do not release the button until the ⏻ LED is orange and starts to blink.

For More Information

For additional product documentation and software and firmware upgrades, visit **avigilon.com/support**.

Technical Support

Contact Avigilon Technical Support at **avigilon.com/contact**.

Limited Warranty and Technical Support

Avigilon warranty terms for this product are provided at **avigilon.com/warranty**.

Warranty service and technical support can be obtained by contacting Avigilon Technical Support: **avigilon.com/contact**.