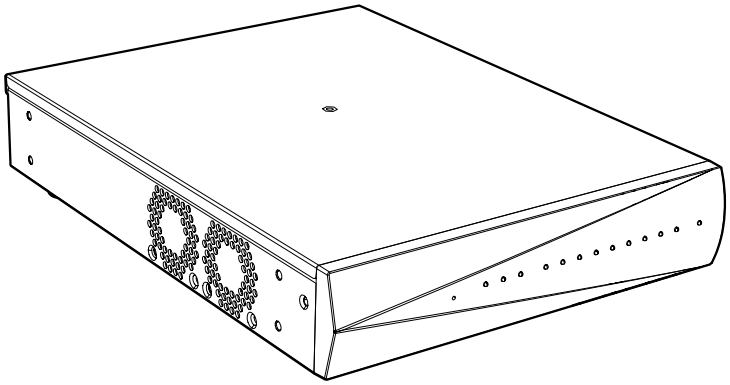
User Guide



Avigilon ENVR2 Plus Appliance

ENVR2-PLUS-8P4
ENVR2-PLUS-8P8

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. Replacement of the battery with an incorrect type is unsafe.
- Connect the power adapter by means of a power cord connected to a socket-outlet with earthing connection.

CAUTION — Risk of explosion if battery is replaced by an incorrect type. Dispose of used batteries according to the instructions.

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.
- Disposal of the battery into fire or a hot oven — or mechanically crushing or cutting the battery — can result in an explosion.

- Leaving the battery in an extremely high temperature surrounding environment can result in an explosion or the leakage of flammable liquid or gas.
- A battery subjected to extremely low air pressure may result in an explosion or the leakage of flammable liquid or gas.
- 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)

The use of EMC compliant support and auxiliary equipment with this device is required in order to fully comply with the EMC regulatory standards.

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.

This equipment satisfies the requirements for use within a residential location.

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

20221004

Table of Contents

Introduction

The Avigilon ENVR2 Plus Appliance is a network security appliance that provides all of the functionality of an Avigilon Network Video Recorder with:

- Avigilon Hardened OS, Avigilon's secure, managed, embedded OS.
- Avigilon Control Center server software.
- Integration of existing multi-megapixel IP cameras in your network that are not already analytic-enabled with most of the features available on Avigilon analytic cameras:
    - Object Detection — Detects and classifies people or vehicles to help operators verify and respond faster. Unusual Activity Detection (UAD) automatically detects atypical behavior of learned objects. Requires an ACC7-VAC license.
    - Avigilon Appearance Search™ — Quickly locates a specific person or vehicle of interest across an entire site using a sophisticated deep-learning AI search engine.
    - Face Recognition — Detects matches from managed watchlists to alert operators of people of interest. Requires Appearance Search and an additional ACC7-FACE license.
    - No-Face-Mask Detection — Detects when a person is not wearing a face mask, with the ability to set-up alarms in ACC's Focus of Attention interface, Radio Alert and ACC Mobile 3 app.
    - License Plate Recognition (LPR) — Accurately captures license plates at a range of distances and speeds. Detects matches from managed license plate watchlists to alert operators of vehicles of interest. Requires an ACC7-LPR license.

System Recommendations

Uninterruptible Power Supply

Use 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.

Camera Frame Rate

The ENVR2 Plus Appliance can provide analytics for non-analytics cameras. For optimal analytics performance, the source camera should stream a minimum of 10 frames per second (fps).

Note: It is acceptable to use frame rates lower than 10 fps for LPR analytics.

Web Browser

Basic administration settings for the ENVR2 Plus Appliance are managed through its Server Management

page, which can be accessed from the ACC Client application or a web browser on a network workstation connected to the ENVR2 Plus Appliance.

Supported web browsers for Windows®, Mac or mobile devices include:

- Mozilla Firefox®
- Google Chrome™
- Microsoft Edge™
- Safari®
- Chrome on Android™
- Safari on Apple® iOS

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

It is recommended to use the latest version of any supported web browser.

Networking

When locating where to install the ENVR2 Plus Appliance in a multi-server deployment, consider the following items:

- Before connecting the ENVR2 Plus Appliance, install the latest ACC Client software package on the ACC Client PC.
- At initial setup time, the ACC Client PC must have network access to the ENVR2 Plus Appliance. After a multi-server site is created, the ACC Client PCs require network access to at least one site member. For more information, see *Installing the ACC Client* on page 14.
- Install the ENVR2 Plus Appliance so that it can communicate over the network with all the ACC Site member servers.
- Do not connect cameras to the ENVR2 Plus Appliance until after the appropriate network configuration has been set up.

Passwords

The first time you start the ENVR2 Plus Appliance you must create new administrator passwords for both:

- The ACC Site running on the ENVR2 Plus Appliance.
- The Server Management page running on the ENVR2 Plus Appliance .

Without these passwords the ENVR2 Plus Appliance can only be brought back into service by resetting it to its default state as it was when first delivered — all recorded data, updates made to the ACC Server software, and all configuration settings are lost and cannot be restored.

Certificate Management

By default, the ENVR2 Plus Appliance is configured with a self-signed certificate, which generates a connection warning in the web browser. Organizations that deploy their own PKI can use the Certificates pane of the Server Management page to manage certificates on the device. For more information, see *Manage Certificates* on page 34.

Package Contents

Ensure the package contains the following:

- Avigilon Video Appliance
- Power cord
- Power supply and screwdriver to secure it
- Wall installation hardware
    - 2 x wall mount brackets
    - 4 x M4x5L bracket mounting screws
    - 4 x wall mounting wood screws
    - 4 x plastic drywall anchors

- Digital input/output terminal block connector

Optional Rack Mount Shelf Contents

If using the Rack Mount Shelf With Sliding Rails accessory kit (RMS1U-ENVR2-8P), ensure it contains the following:

- 2 x rack rails
- 1 x shelf
- 1 x U-bracket for securing the power supply
- 8 x M4x5L ENVR2 Plus Appliance mounting screws
- 10 x M5x10L rack mounting screws
- 2 x M3x5L U-bracket screws

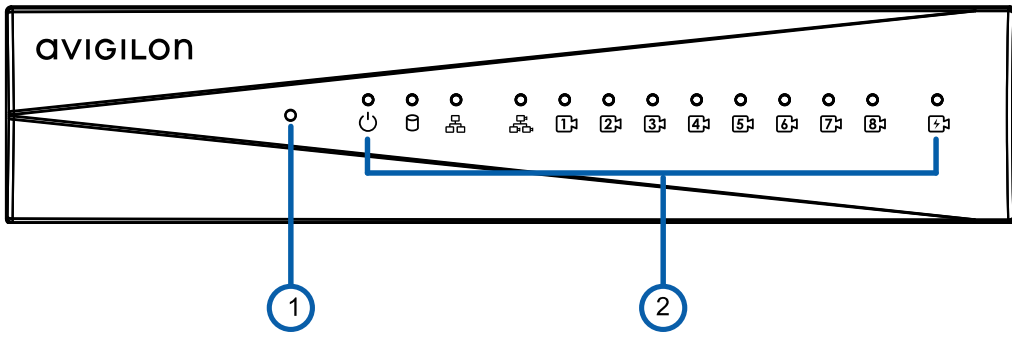
Optional DIN Rail Mount Contents

If using the DIN Rail Mount accessory kit (DIN-ENVR2-8P), ensure it contains the following:

- 1 x DIN rail mount
- 4 x M3x5L DIN rail mounting screws

Overview

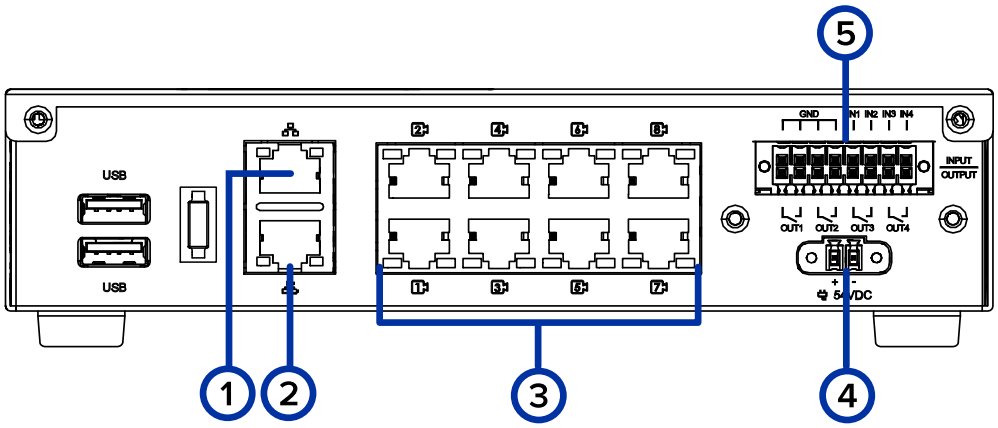
Front View



1. **Reset button**
2. **Status LED**

   Provides information about daily operations. For more information, see *LED Indicators* on page 31.

Rear View



1. **Corporate network uplink port**

   Accepts a 1GbE Ethernet connection to the general network for ACC Client connections and to allow users access to the web interface of the appliance.

2. **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.

3. **PoE switch component**

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

4. **Power connector**

   Accepts power to the appliance.

5. **I/O connector**

   Provides connections to external input/output devices. For more information, see *Connecting to External Devices* on page 30.

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, Zeroconf	
Corporate and Camera LAN Uplink	via Camera LAN Uplink only	Static, DHCP-assigned, Zeroconf	Static, DHCP-assigned, Zeroconf	Corporate and Camera LAN Uplinks must be on different subnets.

Setting Up the ENVR2 Plus Appliance

Installing the Hardware

Install the ENVR2 Plus 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 ENVR2 Plus 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 (RMS1U-ENVR2-8P), or mounted to a DIN rail using the optional DIN Rail Mount accessory kit (DIN-ENVR2-8P). Follow the mounting instructions below for the type of mount you will be using.

> **Tip:** You may want to mount the appliance before or after you have made all the required connections depending on where you want to mount the device. See *Connecting the Hardware* on page 9 for more information on the required connections.

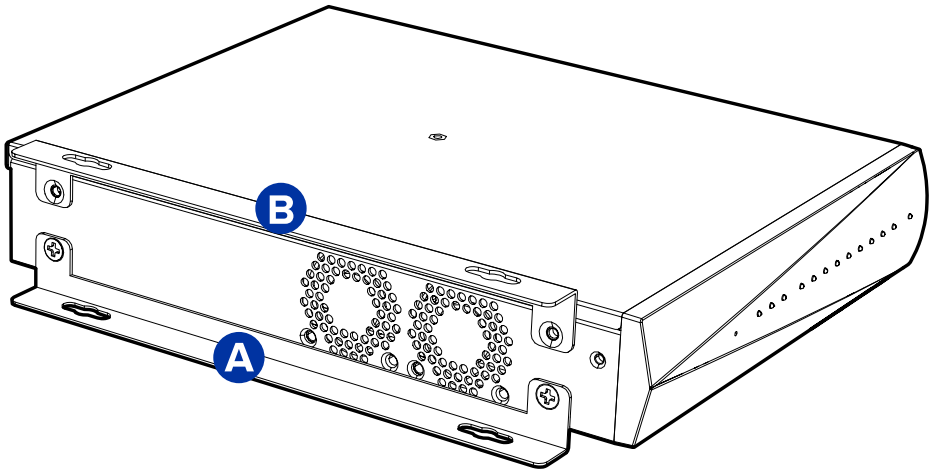
Mounting to the Wall with the Supplied Brackets

If you are not using the supplied mounting brackets, refer to the instructions for the mounting option you are using:

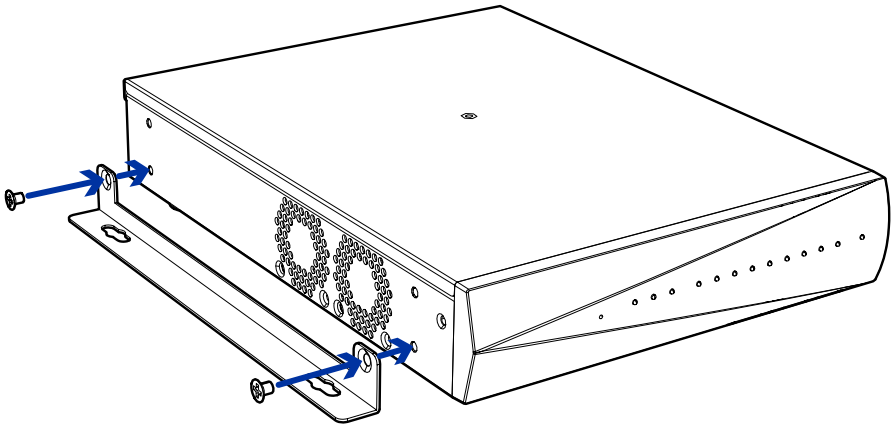
- *Mounting with the Optional DIN Rail Mount Kit* on page 45
- *Mounting with the Optional Rack Mount Kit* on page 41

Follow these instructions to mount the ENVR2 Plus Appliance with the supplied mounting brackets.

1. Note down the serial number, located on the label on the underside of the device.
2. The wall mounting brackets can be mounted to either the lowest threaded holes on the sides of the appliance (A) or the highest threaded holes on the sides of the appliance (B), depending on whether you want to mount the ENVR2 Plus Appliance with the bottom or top towards the wall.

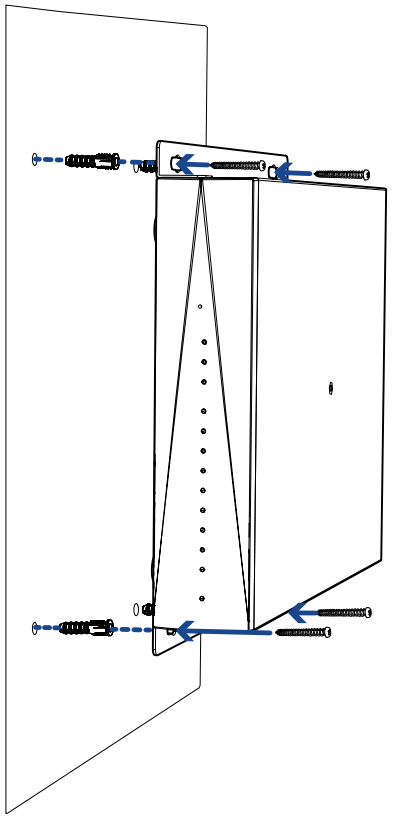


3. Use the four M4x5L screws provided to fasten each wall mounting bracket to the side of the appliance in either the A or B position.



4. Screw the wall mounting brackets to the wall with the four wood screws provided. Using the drywall anchors is recommended.

> **Tip:** The appliance can be mounted in any orientation. Try not to mount in an orientation that puts a lot of strain on the cables or connectors.



Connecting the Hardware

Before connecting to the ENVR2 Plus Appliance, mount the appliance using one of the three mounting options. See *Overview* on page 4 for connector and port locations.

1. Connect the cameras to the PoE ports.
2. Connect the *corporate network* port on the device to the local network with an Ethernet cable.
3. 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. It may take several minutes for the power LED to turn green the first time the device is powered on. The PoE Status LED should be off, indicating the PoE power being used is within the maximum power budget.

   Note: The PoE Status LED status may change if the system detects that the total power consumption exceeds the PoE limits. If the LED is blinking orange, go to the **PoE** tab in the Network panel of the ENVR2 Plus Appliance Web Interface to resolve the power budgeting for each port. For more information, see *Assigning a PoE Power Budget* on page 28.

Connect to the ENVR2 Plus Appliance (using DHCP)

If you use DHCP to assign IP addresses in your network, the new ENVR2 Plus Appliance is immediately detected after it is connected to the security network. The ACC server software then adds it to the list of sites that is displayed in the System Explorer when you start the ACC Client.

1. Power on the appliance and wait for it to startup. Check that the appliance LED indicators display the correct status. See *LED Indicators* on page 31 for more information.
2. On a workstation connected to the same network as the ENVR2 Plus Appliance, start and log in to the ACC Client software.
3. Locate the new site in the Site Login list. You are looking for a site labeled "ENVR2-PLUS-8Px-<serial number>".
4. The `administrator` username is pre-populated along with an empty password. Leave the credentials as they are and click **Log In**.
5. You are prompted to enter new login credentials for the administrator user of the ACC Server running on the ENVR2 Plus Appliance. Enter and confirm the new administrator password and click **OK**.

   Important: Save the password in a secure format and location either physically or electronically so that it can be retrieved if the password is forgotten.
6. In the Explorer right-click on the ENVR2 Plus Appliance and select **Setup**.
7. Click to select the server below the site you right-clicked in the previous step.

8. Click **Server Management**.
9. Click **Trust** on the certificate message that opens.
10. You are prompted to log in to the Server Management interface.

    You are prompted to create a new password for the `administrator` user of the ENVR2 Plus Appliance operating system. Enter and confirm the new administrator password, then click **Apply**. It is recommended to not use the same credentials as the ACC system administrator.

    Important: Save the password in a secure format and location either physically or electronically so that it can be retrieved if the password is forgotten.

    The Dashboard panel of Server Management for the ENVR2 Plus Appliance is displayed.

    Note: On subsequent logins, you will need to enter the `administrator` username and this password when logging in to the ENVR2 Plus Appliance Server Management interface. The administrator is the only user that can log in to the Server Management interface.
11. Configure the basic settings for your new ENVR2 Plus Appliance in Server Management, including the hostname, time zone, and language. For more information see *Configuring the ENVR2 Plus Appliance for the First Time* on page 12.

Connecting to the ENVR2 Plus Appliance (using Static IP)

After powering on the ENVR2 Plus Appliance:

Check that the appliance LED indicators display the correct status. See *LED Indicators* on page 31 for more information.

1. Discover the appliance. Use File Explorer on a Windows computer or Finder® on a Macintosh computer on the same local network as the ENVR2 Plus Appliance.

   You are looking for a device labeled "ENVR2-PLUS-8Px-<serial number>" or the hostname you configured in the Server Management page for this device.

   If you cannot locate the appliance, see *Troubleshooting* on page 12.
2. Click to connect to the device.

   Important: By default, the ENVR2 Plus Appliance is configured with a self-signed certificate, which generates a connection warning in the web browser. Organizations that deploy their own PKI can use the Certificates pane of the Server Management page to manage certificates on the device. For more information, see *Manage Certificates* on page 34.

3. Click past any connection messages displayed by the web 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. You are prompted to log in to Server Management. You are prompted to create a new password for the `administrator` user. Enter and confirm the new administrator password, then click **Apply**. This is the new password for the system administrator of the ENVR2 Plus Appliance operating system.

    Important: Save the password in a secure format and location either physically or electronically so that it can be retrieved if the password is forgotten.

    The Dashboard panel of the Server Management page is displayed.

    Note: On subsequent logins, you will need to enter the `administrator` username and this password when logging in to the Server Management interface. The administrator is the only user that can log in to the Server Management interface.
5. On the navigation sidebar click **Network**.
6. Manually set the IP address for your new ENVR2 Plus Appliance in the Server Management page:
    a. In each of the panes in the Network panel, click on the **IP** tab and toggle **Automatic IP** off to manually specify the connections.
    b. Enter the appropriate values in the following fields if you are manually entering the connection settings:
        - **IP Address**
        - **Subnet Mask**
        - **Default Gateway**
    c. Click **Apply** to save your changes.
7. Configure other basic settings, including the hostname, time zone, and language while you are logged in to Server Management page. For more information see *Configuring the ENVR2 Plus Appliance for the First Time* on the next page.

Configuring the ENVR2 Plus Appliance for the First Time

To...	From the Navigation Sidebar...	On the Card...	Setting
Change the language for Server Management	Click **Device**	**General**	Choose your language from the drop down **Language** list
Replace the default server name with a user-friendly hostname		**Hostname**	Change the **Hostname**
Set the time zone		**Time**	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 24.		

For more information about the other configuration settings in Server Management, see *Using Server Management* on page 21.

If you are installing the first Avigilon appliance in your security network, you can now install the ACC Client software on a network workstation or on the computer you are using to access Server Management. For more information, see *Installing the ACC Client* on page 14.

Troubleshooting

There are several ways you can discover a device that is supposed to 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 "ENVR2-PLUS-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: ENVR2-PLUS-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://ENVR2-PLUS-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 ENVR2 Plus Appliance acquires an IP address on the network through DHCP. If you need to set up the ENVR2 Plus Appliance to use a static IP address or any specific network configuration, see the *Connecting to the ENVR2 Plus Appliance (using Static IP)* on page 10 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.

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**. 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 ENVR2 Plus 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 16.

- **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/**.

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**.

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* on the next page 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**.
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.

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.
      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.

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**.

Enabling Analytics on an ENVR2 Plus Appliance

To enable analytics processing on the video streams from cameras connected to the ACC site to be done by the ENVR2 Plus Appliance:

1. Open the ACC Client software and log in to the ENVR2 Plus Appliance.
2. In the New Task menu , click **Site Setup**.
3. Select a server, then click **Server Analytics** .
4. Select an analytics feature tab and then select the cameras to enable the feature on:
   - Classified Object Detection (requires ACC7-VAC licenses)
   - Appearance Search (requires ACC7-ENT licenses)
   - Face Mask Detection (requires ACC7-ENT licenses)
   - Face Recognition (requires ACC7-FACE licenses)
   - License Plate Recognition (requires ACC7-LPR licenses)

   Only cameras that you have access to that have the prerequisite analytics enabled are displayed in each tab. If you do not see a tab, it could be because your site does not have the required analytics license.
5. Click in the option box next to a camera to select or deselect the camera to enable analytics processing by the ENVR2 Plus Appliance for that camera. An estimate of the resource cost is shown on the left of each camera row.

As you enable (or disable) analytics for cameras, the bars at the bottom update to display the ENVR2 Plus Appliance's capacity. The percent usage of each analytics feature is displayed using the color of the analytics feature tab.

To exit the Server Analytics panel, click **Close**.

Setting Up License Plate Recognition

Configuring LPR lanes and settings must be done on the License Plate Recognition page. If the button doesn't appear on the Server Setup page, ensure your LPR licenses have been activated. For more information, see *Activating a License* on page 15.

1. In the New Task menu , click **Site Setup**.
2. Select the ENVR2 Plus Appliance server, then click .

   The License Plate Lane list is pre-populated with the number of lanes that you have licensed for the site.

3. Select a lane from the License Plate Lane list and complete the following fields:
    - **Name:** — The name for the lane. This should be unique throughout the ACC site.
    - **Camera:** — The camera that will perform LPR. One camera can be used for multiple lanes.
    - **License Plate Configuration:** — The regional plate format the camera will recognize.
    - **Pre-Event Record Time:** — How long video is recorded before the license plate is recognized.
    - **Post-Event Record Time:** — How long video is recorded after the license plate is recognized.
    - **Minimum Confidence:** — The minimum confidence required for a detected license plate to be registered as an LPR event.
    - **Enable this lane** — Enable LPR on this lane.
    - **Max Image Analysis Rate:** — Enter an image rate between 1-60 images per second (ips). This specifies the maximum frame rate analyzed by the LPR service. A high **Max Image Analysis Rate:** setting will use more processing capacity than a lower setting.
4. Move and adjust the green overlay until it spans the width of the traffic lane in the camera's field of view. LPR is only performed in the green area.

    A red overlay means the detection area is too large and cannot be used.
5. Click **OK**.

> **Tip:** Navigate back to the Server Analytics panel () to view the analytics usage and remaining resource capacity of the ENVR2 Plus Appliance after setting up LPR lanes. On the Server Analytics panel, you can enable and disable LPR lanes that you have already configured, and check the remaining analytics capacity of the ENVR2 Plus Appliance.

LPR is now configured and you can add Watch Lists to your site. For more information on configuring the LPR lanes and setting up **Watch Lists**, see the **License Plate Recognition** sections in the ACC Client Help Center.

LPR Performance Mode

You can increase the channel capacity of LPR analytics on your ENVR2 Plus Appliance by enabling LPR Performance Mode. This mode will more than double the number of LPR frames per second that can be processed simultaneously, but will limit other analytics on your ENVR2 Plus Appliance. The following analytics will be disabled when LPR Performance Mode is enabled:

- Classified Object Detection
- Appearance Search
- Face Recognition
- Face Mask Detection
- Up to two regional license plate configurations can be used concurrently

To enable LPR Performance Mode:

1. Select the device in the System Explorer and click **Server Management** .
2. Log in to the ENVR2 Plus Appliance.
3. Click **ACC** on the left-hand menu.
4. Select the **Server** panel.
5. On the General pane, click the **LPR Performance Mode** toggle to enable or disable the feature.

Using Server Management

The ENVR2 Plus 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.

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 "ENVR2-PLUS-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 12.
    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:

Color	Status	Description
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.
		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 **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.
Enable or disable LPR Performance Mode. LPR Performance Mode can more than double the number of LPR frames per second that can be precessed simultaneously for the ENVR2 Plus Appliance, but limits other analytics. When enabled, Face Recognition will be disabled.	Click the **LPR Performance Mode** toggle to enable or disable the feature.

- Network Storage Management pane to enable ACC Client application users to archive video from the ENVR2 Plus 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 ENVR2 Plus 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 ENVR2 Plus Appliance:

1. From the navigation bar, open the **Server** panel.
2. In the Network Storage Management pane, click **Enabled**.
3. 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>*

4. In the **Network Path** field, enter the path to the preferred video archiving location.
5. 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:
        - **Analytics Service Exception Logs**
        - **Analytics Service FCP Logs**
        - **Analytics Service Logs**
        - **Exception Logs**
        - **FCP Logs**
        - **Server Logs**
        - **WebEndpoint Logs**
        - **LPR Service: Exception Logs**
        - **LPR Service: FCP Logs**
        - **LPR Service: 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.	**General**	Choose your language from the drop down **Language** list
Reboot your system.	**Reboot**	Click to reboot the appliance.
Install the latest version of the firmware on your device.	**Upgrade Firmware**	See *Upgrade the Firmware* on page 37.
Find information that may be helpful when troubleshooting.	**Support**	Download **Device Logs** and **System Snapshot** to assist in troubleshooting.
Replace the default server name with a user-friendly hostname.	**Hostname**	Change the **Hostname**. The default hostname is the same as the server name. The server name is in the form *<Model>-<Serial Number>*.
Change the password for the ENVR2 Plus Appliance administrator.	**Password**	See *Change the ENVR2 Plus Appliance Administrator Password* below.
Set the time zone.	**Time**	Specify the **Time Zone** and identify the time source in the **NTP** drop-down and **Servers** list. See *Manage Time Settings* on the next page.
Manage the certificates used by Server Management and the ENVR2 Plus Appliance.	**Certificates**	See *Manage Certificates* on page 34.

Change the ENVR2 Plus 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. 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 39.

Manage Time Settings

Customize how the ENVR2 Plus 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 ONVIF cameras), you can connect to port 123 on the ENVR2 Plus Appliance to use it as an NTP server. Once connected, Avigilon cameras will use the ENVR2 Plus Appliance as their NTP time source by default.

   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.

Manage Storage

On the **Storage** panel you can view the storage capacity of the device and the status of the storage drive on ENVR2 Plus 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.	On the Physical Disks panel, information about each physical disk is listed. When the storage drive is: • Correctly working, **Ready** is displayed. • Not correctly working, one of several error states is displayed.

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 6.

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.

To...	Do this...
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 33.

> **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.	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.

To...	Do this...
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 apply the changes when the following message is displayed:

Applying changes may power-cycle PoE-powered devices.

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.

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:

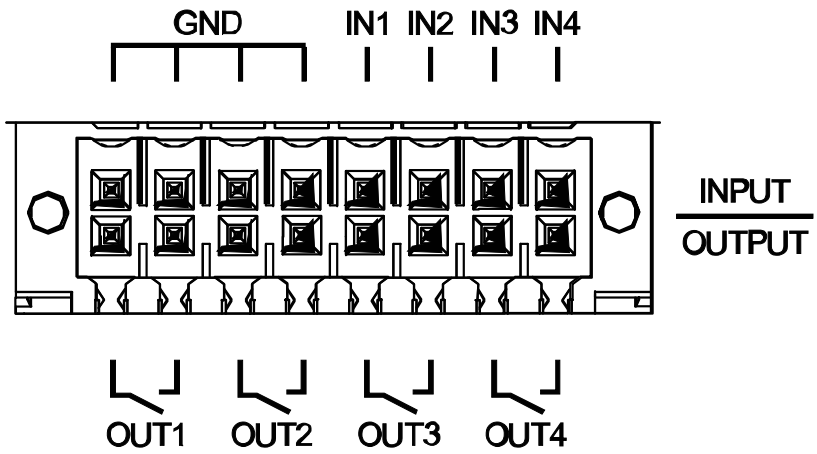


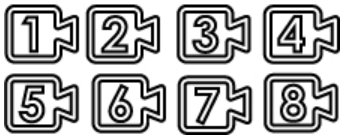
Figure 1: The ENVR2 Plus Appliance I/O pins are shown in the image above.

Function	Description
IN1	Alarm Inputs — Active-Low inputs. To activate, connect the Input to the Ground pin (GND). To deactivate, leave disconnected.
IN2	
IN3	
IN4	
GND	
OUT1	Relay Outputs — Form-A dry contact outputs. When active, terminals are connected. When inactive, terminals are disconnected. Maximum load of each relay output: 1 A at 30 V DC; 0.3 A at 125 V AC.
OUT2	
OUT3	
OUT4	

LED Indicators

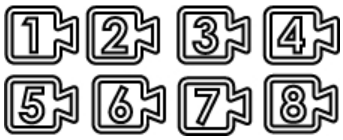
The following list describes what the LEDs on the ENVR2 Plus Appliance indicate.

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	An error is present on a PoE port.
	Orange - blinking	Over budget.
	Off	PoE power is under the maximum PoE power budget.

Back Panel LEDs

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

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

Budgeting PoE Power

The PoE switch component in the Avigilon ENVR2 Plus Appliance device can output a total of 125 W of power to the connected devices. Each PoE port is capable of outputting 15.4 W to standard PoE devices, and 30 W to PoE+ devices. This typically means that the device can support eight standard PoE devices or up to four 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, or you are using cables much shorter than 100 m, use the following estimates:

- If the device uses less than or equal to (<=) 15.4 W and the cable length is 100 m — expect up to 2.5 W of power loss.
- If the device uses more than (>) 15.4 W and the cable length is 100 m — expect up to 4.5 W of power loss.

To calculate the recommended power budget for each port when using 100 m cables, 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

Note: Shorter cables will have a lower expected power loss than the maximum power loss used in this calculation. However, if you miscalculate the required power for a PoE port, the connected cameras may be shut down if total power output exceeds 125 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 ENVR2 Plus Appliance is operating with the latest features and bug fixes. 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 ENVR2 Plus Appliance,
  - the firmware on all other Avigilon servers, 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 ENVR2 Plus 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** and search for the appropriate ENVR2 Plus 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 client machine.

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. 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 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 4.

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

If the appliance encounters a system error and you are unable to access the web interface, you can try to resolve the issue by restarting the system from the physical appliance.

- 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.

Mounting with the Optional Rack Mount Kit

Install the ENVR2 Plus 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.

Tip: You may want to mount the appliance before or after you have made all the required connections depending on where you want to mount the device. See *Connecting the Hardware* on page 9 for more information on the required connections.

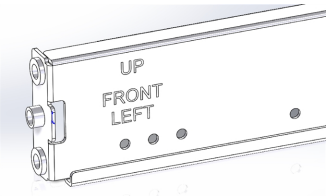
If you are not using the rack mount kit, refer to the instructions for the mounting option you are using:

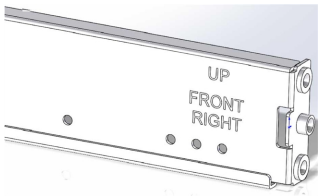
- *Mounting to the Wall with the Supplied Brackets* on page 7
- *Mounting with the Optional DIN Rail Mount Kit* on page 45

Follow these instructions to mount the ENVR2 Plus Appliance with the optional Rack Mount Shelf With Sliding Rails accessory kit (RMS1U-ENVR2-8P).

Important: The rails are designed for rack units with square mounting holes only.

The mounting rails are designed in pairs, with a right and left rail. Each rail is clearly marked to indicate the side of the rack unit it must be attached to, as well as the top and front edges. Before starting, check each mounting rail to verify on which side of the rack the rail is attached. The rail length is adjustable from 641 mm to 910 mm (25.236" - 35.827").

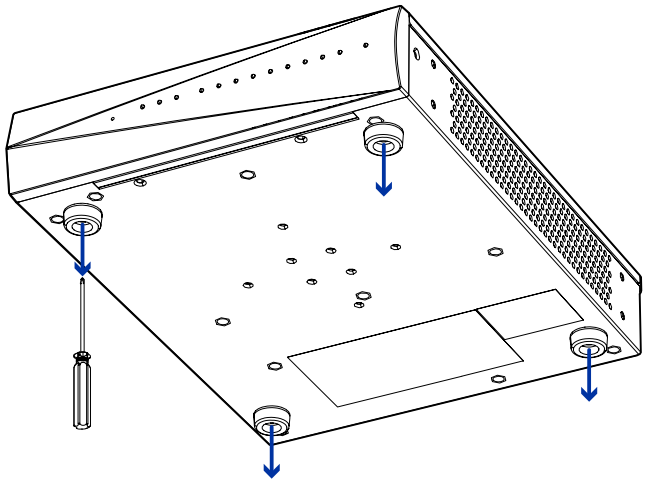




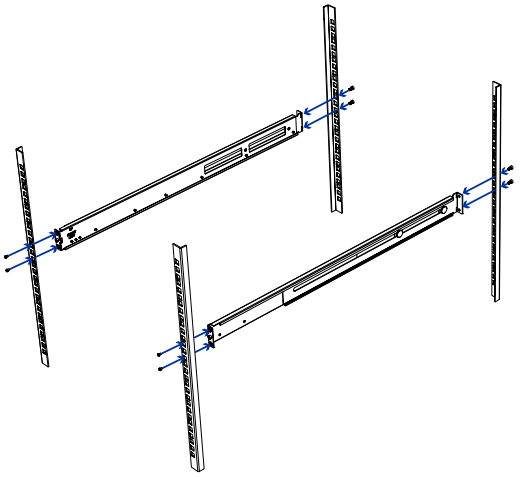
There is a risk of injury and damage to equipment if the appliance falls out of a rack unit. It is extremely important that the ENVR2 Plus Appliance is securely fastened to the mounting rails.

Ensure that the location of the appliance in the rack unit does not impede airflow through the appliance.

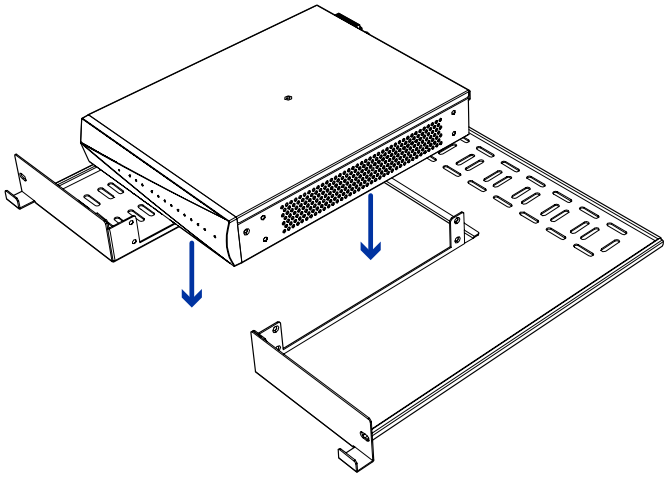
1. Note down the serial number, located on the label on the underside of the device.
2. Use a Phillips #2 screwdriver to remove the four feet from the bottom of the ENVR2 Plus Appliance.



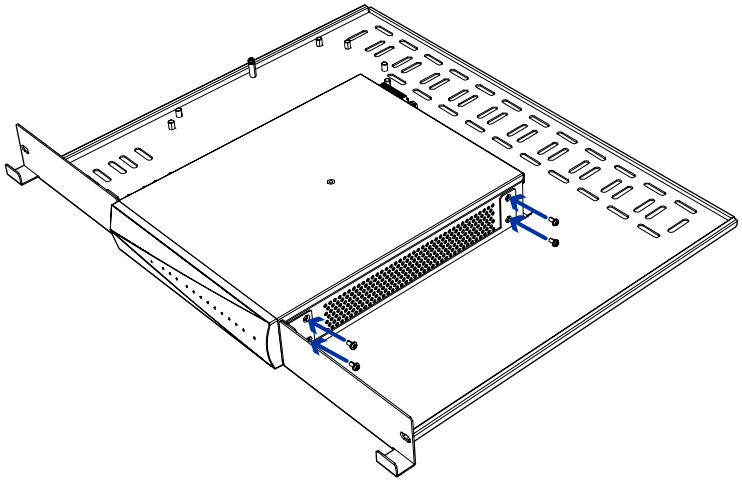
3. Install the left-hand mounting rail to the left side of the rack, and the right-hand mounting rail to the right side of the rack. Each rail is attached to the front and back of the rack using two of the M5x10L screws (provided) at each end. Use the upper and lower screw holes, which align with the mounting holes in the rack unit.



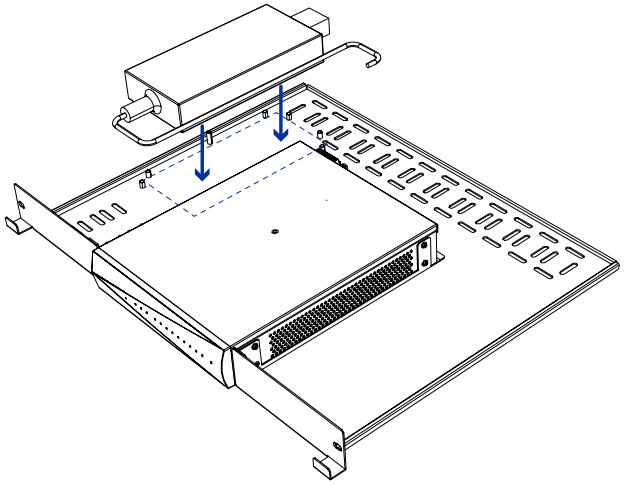
4. Lower the ENVR2 Plus Appliance into place on the rack shelf. Align the screw holes on the sides of the appliance with the rack shelf mounting holes.



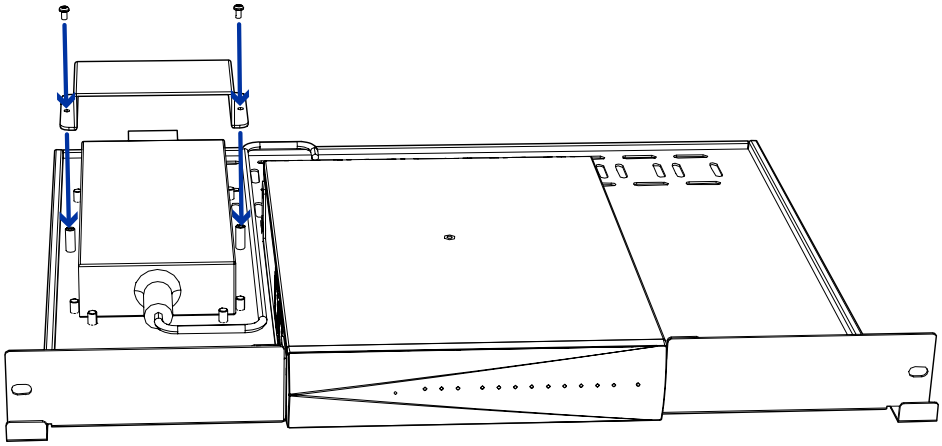
5. Secure the ENVR2 Plus Appliance to the rack shelf with the eight M4x5L screws provided. Secure the appliance with four screws on each side.



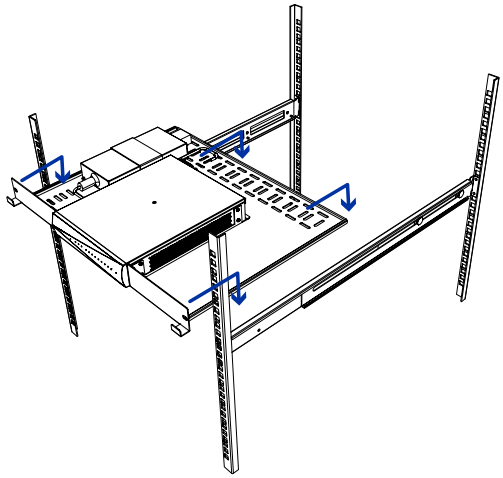
6. Place the power supply in the defined area to the left of the ENVR2 Plus Appliance.



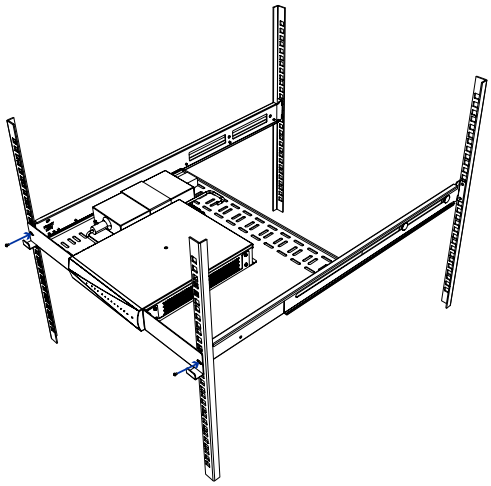
7. Secure the power supply to the rack shelf with the two M3x5L screws and U-bracket provided.



8. Slide the shelf into the rack above the installed rails until the front of the shelf aligns with the front of the rack. Lower the shelf onto the rails so the edges of the shelf are held by the edges of the rails.



9. Secure the shelf to the front of the rack with the two M5x10L screws provided.



Mounting with the Optional DIN Rail Mount Kit

Install the ENVR2 Plus 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.

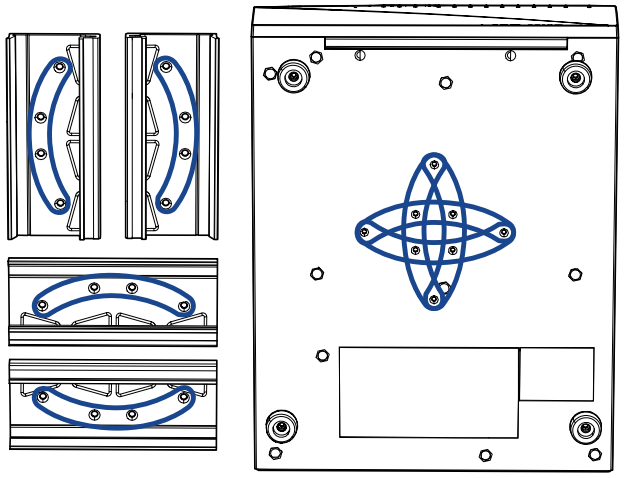
> **Tip:** You may want to mount the appliance before or after you have made all the required connections depending on where you want to mount the device. See *Connecting the Hardware* on page 9 for more information on the required connections.

If you are not using the DIN rail mount kit, refer to the instructions for the mounting option you are using:

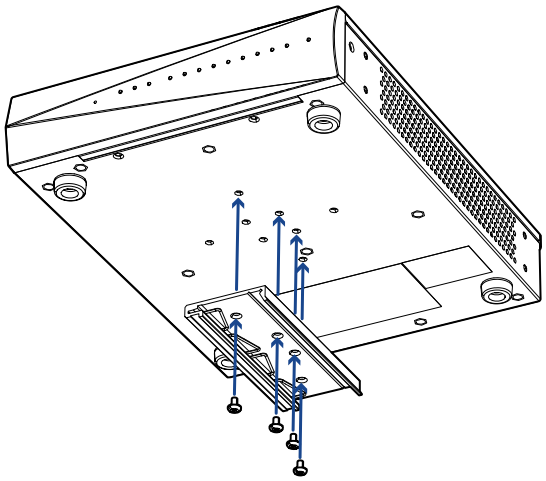
- *Mounting to the Wall with the Supplied Brackets* on page 7
- *Mounting with the Optional Rack Mount Kit* on page 41

Follow these instructions to mount the ENVR2 Plus Appliance with the optional DIN Rail Mount accessory kit (DIN-ENVR2-8P).

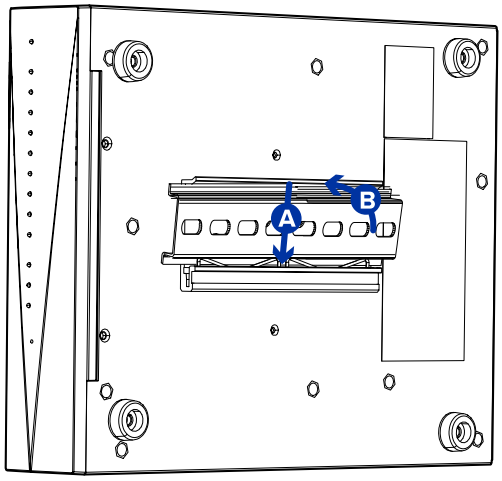
1. Note down the serial number, located on the label on the underside of the device.
2. The bottom of the ENVR2 Plus Appliance has mounting holes for the DIN rail mount. The DIN rail mount can be mounted in any of the four positions.



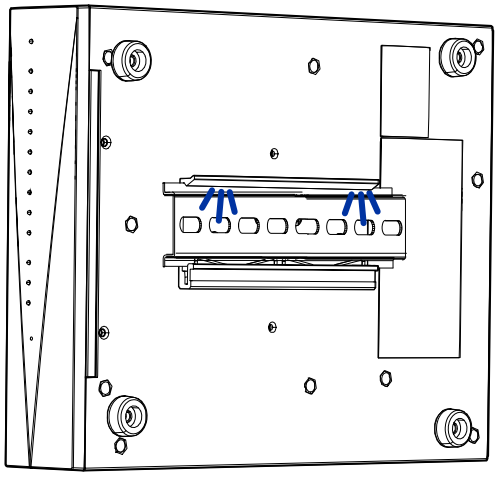
3. Use the four M3x5L screws provided to fasten the DIN rail mount to the bottom of the appliance.



4. Push the spring portion of the DIN rail mount onto the bottom side of the DIN rail (A).



5. Rotate the top side of the DIN rail mount towards the DIN rail (B) until it snaps into place.



For More Information

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

Technical Support

Contact Avigilon Technical Support at **support.avigilon.com/s/contactsupport**.

Limited Warranty

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