avigilon™
a Motorola Solutions Company

User Guide

Avigilon Video Appliance Models:

VMA-AS3-8P
VMA-AS3-16P
VMA-AS3-24P

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.
- Only use the power adapter supplied with your system.

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

The unit shall not be serviced while extended on the slide-rails.

Ensure to connect the power cord to a socket-outlet with earthing connection.

Suitable for installation in Information Technology Rooms in accordance with Article 645 of the National Electrical Code and NFPA 75.

This equipment is not suitable for use in location where children are likely to be present.

For model VMA-AS3-16P, VMA-AS3-24P:

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 A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

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

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

For model VMA-AS3-8P:

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.

Suitable for installation in Information Technology Rooms in accordance with Article 645 of the National Electrical Code and NFPA 75.

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)

Changes or modifications made to this equipment not expressly approved by Avigilon Corporation or parties authorized by Avigilon Corporation could void the user's authority 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-AS3-A

Revision: 2 - EN

20190603

Table of Contents

Introduction

The Avigilon Video Appliance is the all-in-one solution for network video recording. The video appliance includes:

- A network switch to connect and power PoE IP cameras.
- Built-in server and storage to run the Avigilon Control Center Server and retain recorded video content.
- Video ports to display live video and allow users to operate the Avigilon Control Center Client software directly from the appliance.
- Aggregate throughput of 400 Mbps (on the 16- and 24-port models) and 200 Mbps (on the 8-port model, for simultaneous recording, playback, and live streaming.

This guide describes how to configure the system after the appliance has been powered and is connected to a keyboard, mouse and monitor.

Package Contents

Ensure the package contains the following:

- Avigilon Video Appliance
- Power cord
- Power supply and screwdriver to secure it (8-port appliance only)
- Wall installation hardware (8-port appliance only)
- Rack mounting rails and appliance rack mounting hardware (16- and 24-port appliances)
- Digital input/output terminal block connector

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 Windows 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.

Overview

Front View

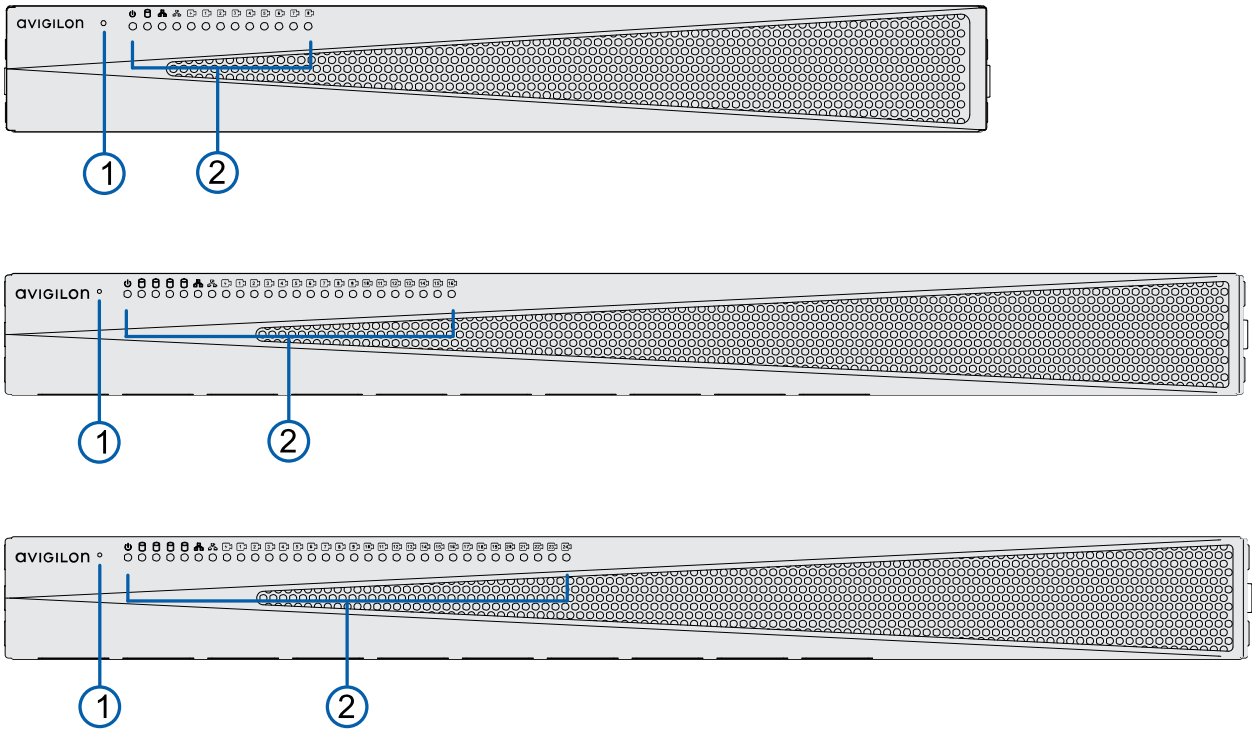


Figure 1: Front view of VMA-AS3-8P, VMA-AS3-16P, and VMA-AS3-24P (top to bottom)

1. **Reset button**

   Use this button to reset the internal PoE switch, or restart the operating system of the appliance. For more information, see *Resetting the Internal PoE Switch to Factory Defaults* on page 43 and *Restarting the Operating System* on page 42.

2. **Status LED**

   Provides information about daily operations. For more information, see *LED Indicators* on page 38.

Rear View

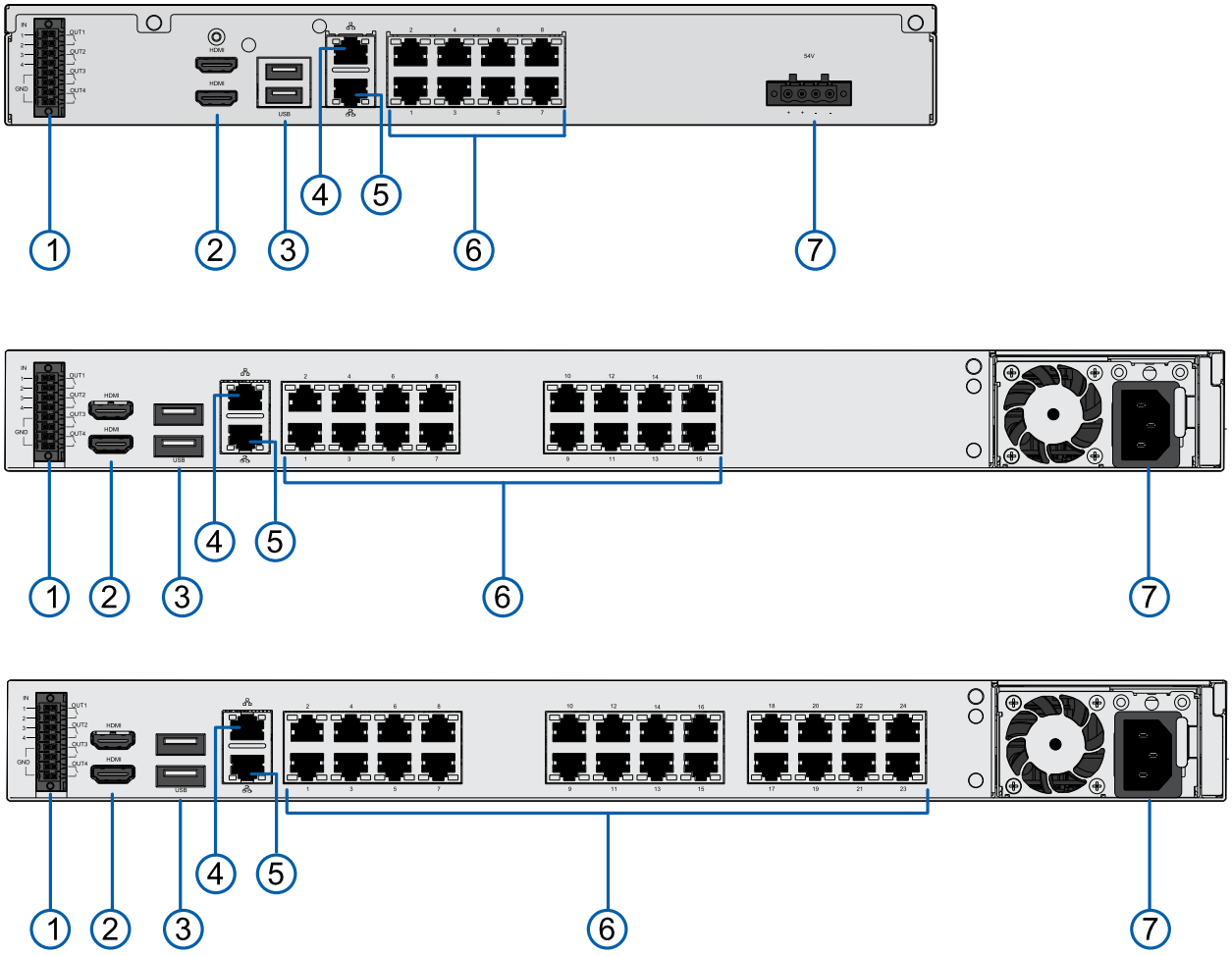


Figure 2: Rear view of VMA-AS3-8P, VMA-AS3-16P, and VMA-AS3-24P (top to bottom)

1. **Digital I/O connector**

   Provides connections to external input/output devices. For more information, see *Connecting to External Devices* on page 40.

2. **HDMI connector**

   Provides HDMI connections to connect monitors to the appliance.

3. **USB connector**

   Provides USB 3.0 connections to USB devices.

4. **Corporate network uplink port connector**

   Accepts a 1GbE Ethernet connection to connect the appliance to the corporate network so that video can be accessed from a client over the network. It also allows access to the Switch Management WebUI of the appliance.

5. **Camera network uplink port connector**

   Accepts a 1GbE Ethernet connection to remote cameras that are connected via a remote 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.

6. **Local camera connector with PoE**

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

7. **Power connector**

   Accepts power to the appliance.

Wall Mounting an 8-Port Video Appliance

You can mount the 8-port Video Appliance to a wall. This can be useful if you want to install the appliance in a location obscured from view, such as a closet or equipment room, or so that it doesn't take up shelf or counter space. A pair of wall mount brackets with drywall screws and anchors are provided with the appliance. If you are mounting the appliance in a wooden cabinet, or a brick or concrete wall, you will need to obtain the appropriate screws.

Tip: Install the wall mount brackets to the appliance and the wall before you permanently power on the appliance, connect cameras to it, and start recording. If you want to set up your appliance before mounting it to the wall, we recommend you turn off the power supply to the appliance and disconnect all cables after set up is complete and before you mount the appliance to the wall.

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

To mount the appliance on a wall:

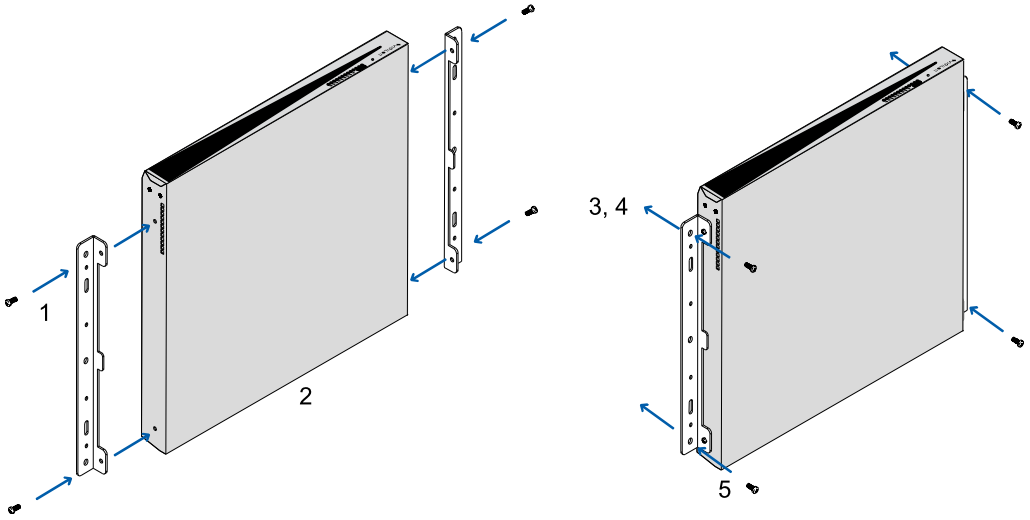


Figure 3: Mounting the 8-port Video Appliance to a wall

1. Attach the wall mount brackets to the lowest threaded holes on the sides of the 8-port Video Appliance.
2. Position the appliance with the rear panel facing downwards. Ensure that the airflow through the appliance is not blocked when it is in position.
3. Mark the locations of the screw holes on the wall.
4. Drill holes for the anchors and insert the anchors into the wall. If you are using wood, concrete or masonry screws, drill holes as appropriate.
5. Attach the appliance to the wall.

Installing a 16- or 24-Port Video Appliance in a Rack Unit

To install a 16- or 24-port Video Appliance in a standard EIA-310 19-inch mounting rack, use the matched pair of mounting rails, matched pair of mounting ears, and pair of unit rails provided with the appliance.

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

Before you can install the appliance in a rack unit, the side brackets attached to protect the front bezel during transport must be removed. They are attached using thumbscrews and can be removed without any special tools. After they are removed, you can attach the two mounting ears that hold the appliance in place when sliding it in and out of the rack.

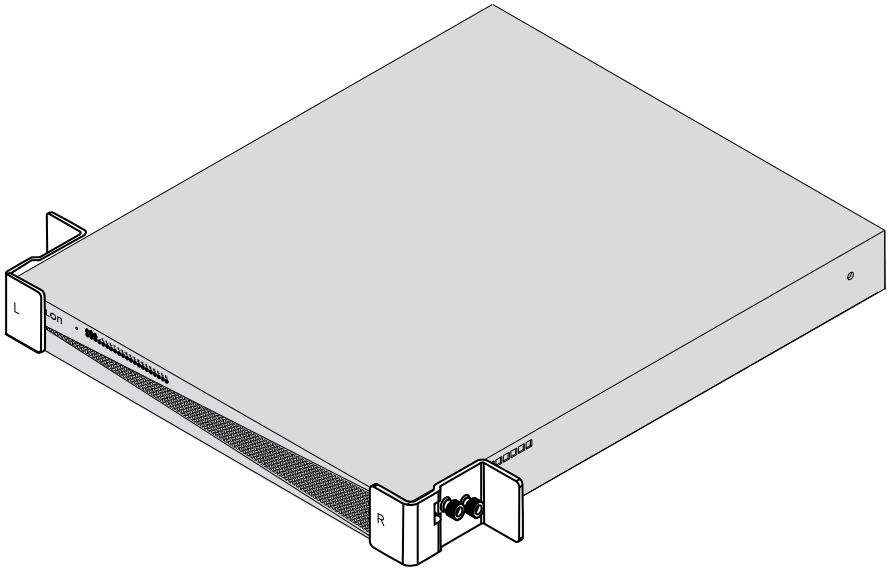


Figure 4: Remove the side brackets that protect the front bezel during transport.

Tip: Save the side brackets to use in case the appliance has to be removed from the rack unit and transported to another location.

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.

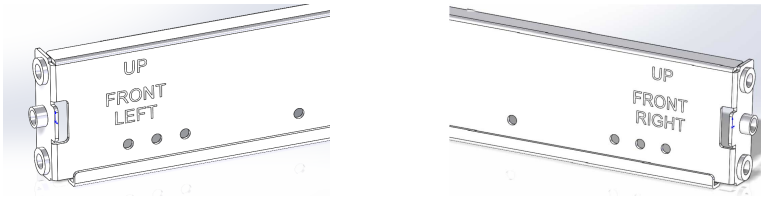


Figure 5: Check each mounting rail to verify on which side of the rack the rail is attached.

Two people are needed to install a 16- or 24-port Video Appliance into a rack unit. These instructions assume that the installers are working from the front of the rack unit.

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

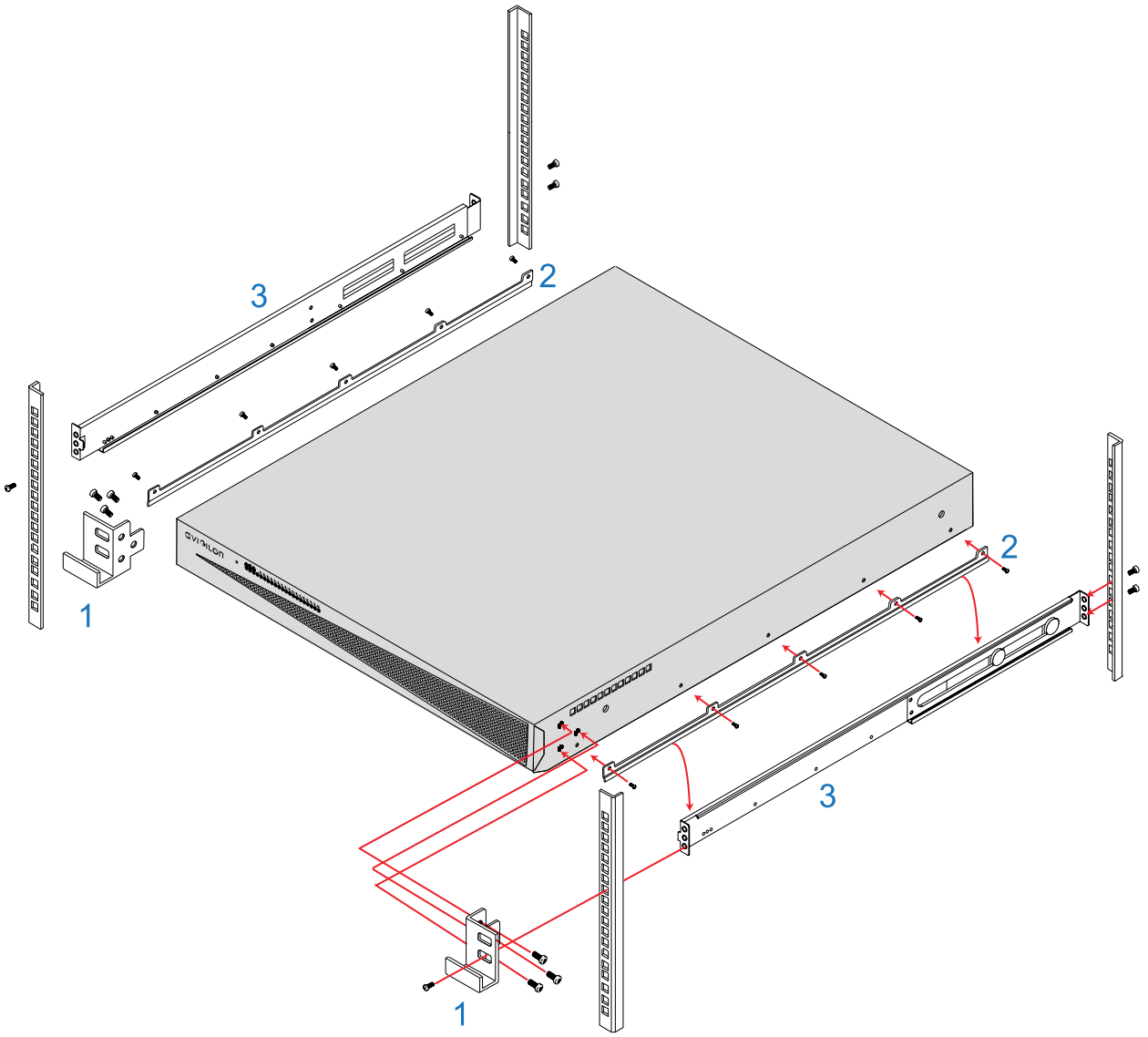


Figure 6: Mounting the Video Appliance into a rack

There is a risk of serious injury and damage to equipment if the Video Appliance falls out of a rack unit. It is extremely important that the Video Appliance is securely fastened to the mounting rails provided with the 16-port or 24-port Video Appliance.

Refer to the figure *Mounting the Video Appliance into a rack* above

1. Attach the mounting ears to the outer side of the appliance at the front using three screws (provided) for each tab.
2. Attach the unit rails to each side of the appliance using five screws (provided) for each guide.
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 screws (provided) at each end. Use the upper and lower screw holes, which align with the mounting holes in the rack unit.
4. Lift the appliance and lower the back of the appliance onto the rails, slide it in against the back bracket of the rails. Slide the unit towards the back of the rack, and ensure the unit rails slide smoothly within the grooves of the mounting rails.
5. Test that the appliance is securely mounted on the rails. Push the appliance fully into the rack, then pull it out at least half-way, and then back in. It should slide in as though it was a shelf.
6. Fasten the appliance to the rack by installing one screw (provided) in the front of each mounting ear.

   NOTE: To remove the appliance, remove the front screw from each mounting ear and slide the unit forward until it is free.

Connecting Cables

Refer to the diagrams in the *Overview* on page 4 for the location of the different connectors. Make the following connections as required:

1. Connect a KVM switch or separate keyboard, mouse and monitor to the appliance.
    - The keyboard and mouse can be connected to any USB port on the appliance.
    - The monitor can be connected to any HDMI connector at the back of the appliance.
2. Connect the appliance to your network using an Ethernet cable.
3. Connect to power cords to the mains supply, or a UPS system if available.
4. To power on the 8-port Video Appliance: Connect the external power supply to the power connector at the back of the appliance and use the supplied screwdriver to fasten it in place. Connect a power cord to the external power supply. Press the switch on the power supply to power on the appliance.
5. To power on the 16-port or 24-port Video Appliance: Connect a power cable to the power supply at the back of the appliance. The appliance immediately powers on.
6. Check that the appliance LED indicators display the correct status.

Configuring Windows 10

When you start the Video Appliance for the first time, you will need to configure the Windows operating system that is installed on the appliance.

1. On the first screen, the MICROSOFT SOFTWARE LICENSE TERMS is displayed. Review the terms and click **Accept**.
2. Select **Join Local Active Directory**.

   Note: This prompt will only appear if an Active Directory is present on the network, see the *Windows Help and Support* files for more information.
3. Enter a user name for accessing the Windows software.
4. Set a password for the user name you entered on the previous screen. When you are ready, click **Next**.

   You are logged into the Windows environment. The ACC client automatically starts in a new window, and the Avigilon End User License Agreement (EULA) is displayed.
5. Review the terms and press the **Enter** key to agree to the EULA.

Video Appliance Network Interface Connections

The Video Appliance is a combination of a built-in computer with storage for recorded video content and a network switch that supports IP camera connections. It supports three network interface connections (NICs), two network ports and either 8, 16, or 24 PoE ports (depending on the model). You can see the NICs in the Network Connections window of the operating system, shown in *The Network Connections Control Panel showing the three NICs. (Used with permission from Microsoft.)* below

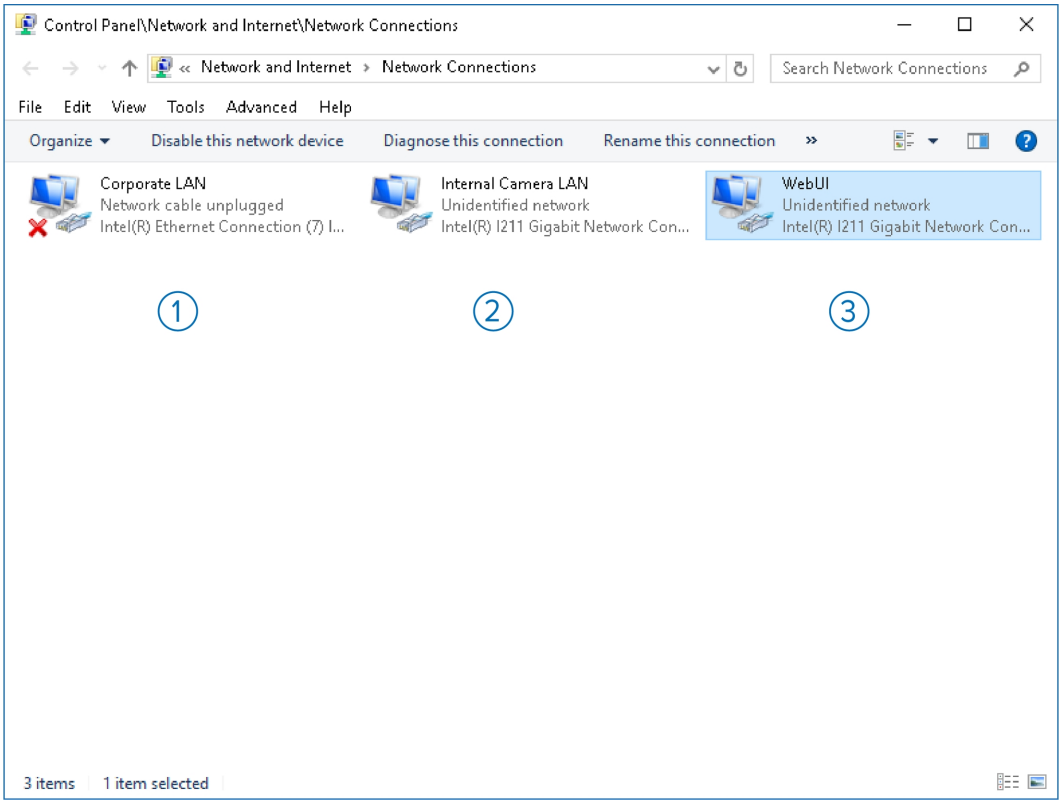


Figure 7: The Network Connections Control Panel showing the three NICs. (Used with permission from Microsoft.)

1. **Corporate LAN**: This NIC is for the connection between the appliance and the corporate network. It routes traffic from the internal computer to the corporate network uplink port.
2. **Internal Camera LAN**: The first of two NICs within the appliance between the internal computer and the internal network switch. This NIC is for the data link between the internal computer and the internal switch and is not associated with any external port.
3. **WebUI**: The second of two NICs within the appliance between the computer and the internal switch. This NIC is dedicated to the camera network uplink port. Its specific purpose is to separate the data traffic for the Switch Management WebUI of the internal switch from the camera data traffic passing through the port.

Video Appliance Port Connectors

In addition to the PoE port connectors for cameras, the Video Appliance has two network port connectors, identified by the following icons:

Corporate network uplink port

Camera network uplink port

Corporate Network Uplink Port

Use the corporate network uplink port to connect the computer in the appliance to the corporate network. Corporate network users can then access video from the appliance from an ACC Client connected over the corporate network.

For example, you can connect the corporate network uplink port to the corporate network to obtain an IP address from the corporate DHCP server. The DHCP server allocates the IP address, subnet mask, a default network gateway, and DNS server details for the computer in the appliance.

Camera Network Uplink Port and PoE Ports

The PoE port connectors and the camera network uplink port connector are all supported by the internal network switch. The switch manages the traffic from these connectors and directs the video data to the built-in computer.

Cameras connected to the PoE port connectors or the camera network uplink port connectors must all be in the same IP subnet. By default the appliance is configured to use ZeroConf and all of the IP addresses are in the local loop.

Important: If your cameras are assigned to their own IP subnet, access the Network Connections control panel to change the IP address of the Camera LAN NIC so that it is in the same range as the camera IP addresses. For more information, see *Connecting to Cameras with Static IP Addresses* on page 21.

In addition, the camera network uplink port is used to access the Switch Management WebUI from a laptop connected to the camera network uplink port. For more information, see *Using the Switch Management WebUI* on the next page.

The Switch Management WebUI can be accessed using a local web browser directly from the appliance, or from a laptop connected to the camera network uplink port connector if you are using the appliance with its default settings.

Using the Switch Management WebUI

The Switch Management WebUI can be accessed using a local web browser directly from the appliance, or from a laptop connected to the camera network uplink port connector if you are using the appliance with its default settings for the WebUI NIC.

Important: When first setting up the appliance, it is recommended that you log in to the Switch Management WebUI and change the default password for the preconfigured login IDs admin and user.

Use the Switch Management WebUI to:

- Manage user accounts and change passwords according to the security policies of your organization. For more information, see *Changing Passwords for Switch Management WebUI Users* on the next page.
- Configure the PoE power budget for the PoE ports you will be using. For more information, see *Configuring the PoE Budget From the Switch Management WebUI* on page 18

Tip: You can connect a stand-alone computer to the camera network uplink port to access the Switch Management WebUI if the operating system on the built-in computer becomes inaccessible, or to reset the passwords again if the switch is restored to its default setting.

To start the Switch Management WebUI, see *Starting the Switch Management WebUI* below

Starting the Switch Management WebUI

The first time the Switch Management WebUI is opened, you must log in with the administrator ID to change the default password for the administrator and user IDs. The default password for the administrator ID **admin** is the serial number of the Video Appliance. The number is located on the label on the underside of the appliance. It is also located on the label on the box in which the appliance was delivered. The default password for the user ID **user** is **user**.

1. Connect to the appliance:
    - Directly: Connect a keyboard, mouse and monitor to the appliance.
    - From a stand-alone computer, such as a laptop:
        - Configure the laptop in the 192.168.2.0/14 subnet
        - Connect the laptop to the camera network uplink port with an Ethernet cable.
2. Start a web browser on the appliance or the laptop connected to the camera network uplink port.
3. Navigate to `https://192.168.2.1`.

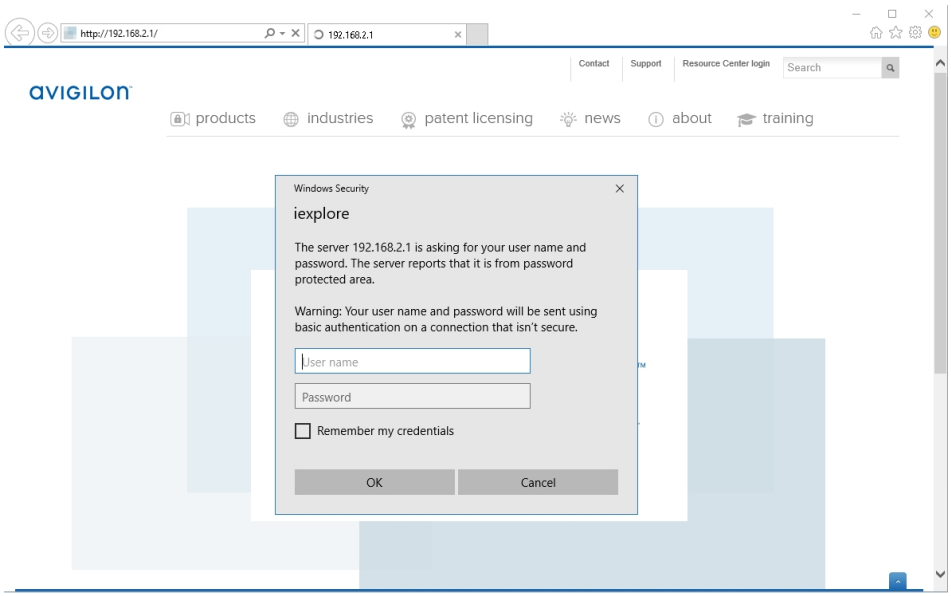


Figure 8: The Switch Management WebUI Log In screen. (Used with permission from Microsoft.)

The browser displays a login screen for the Switch Management WebUI.

4. If this is the first time opening the Switch Management WebUI, refer to *Changing Passwords for Switch Management WebUI Users* below.

   Otherwise enter either the user ID **user** or administrator ID **admin** and password.

   The Switch Management WebUI is displayed.

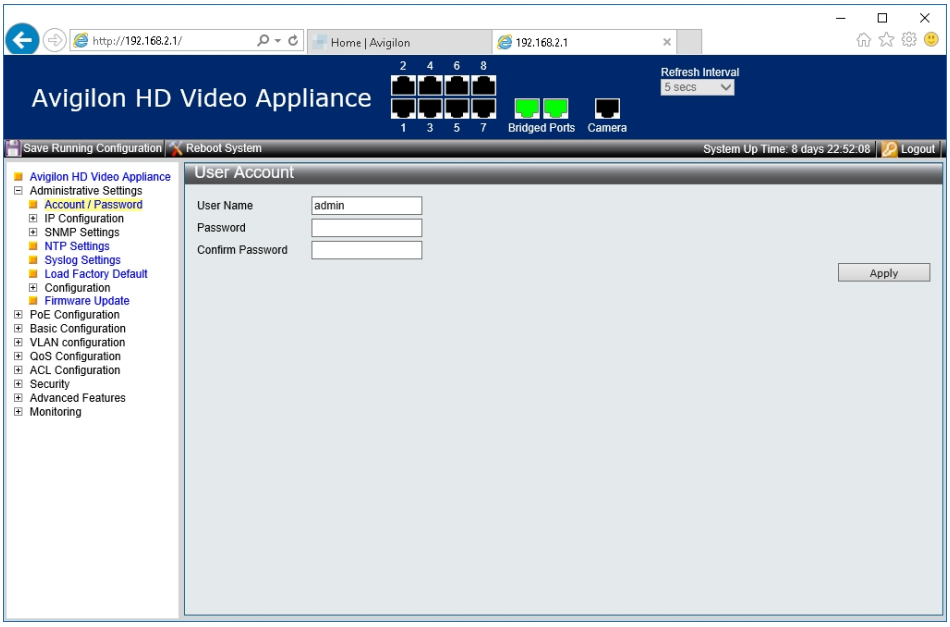
Changing Passwords for Switch Management WebUI Users

Use this procedure to change the preconfigured password for the default user and administrator IDs when you first set up the Video Appliance, and to change passwords according to the security policies of your organization.

The admin user of the Switch Management WebUI can complete this procedure.

1. Open the Switch Management WebUI if it is not already open. For more information, see *Starting the Switch Management WebUI* on the previous page.
2. Enter the administrator ID and password. The:
   - **ID:** admin
   - **Password:** <*Serial number of the unit*>

   The Switch Management WebUI is displayed.



3. Open the Administrative Settings tab and change the password for the administrator ID **admin**.

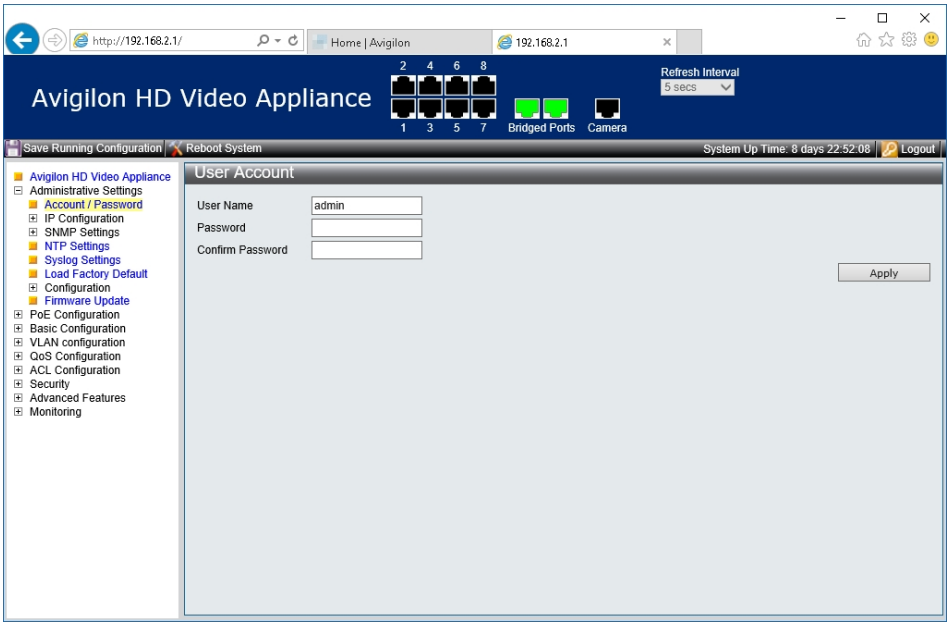


Figure 9: Switch Management WebUI Account | Password tab

4. Click **Apply**.
5. Change the password for the user ID **user**.
6. Click **Apply**.
7. Click **Logout** to exit.
8. When the log in screen reappears, enter the user ID **user** and the new password.

9. If you want to manually configure the PoE power budget for the PoE ports you will be using, see*Configuring the PoE Budget From the Switch Management WebUI* below; otherwise exit the Switch Management WebUI.

Tip: You can connect a stand-alone computer to the camera network uplink port to access the Switch Management WebUI if the operating system on the built-in computer becomes inaccessible, or to reset the passwords again if the switch is restored to its default setting.

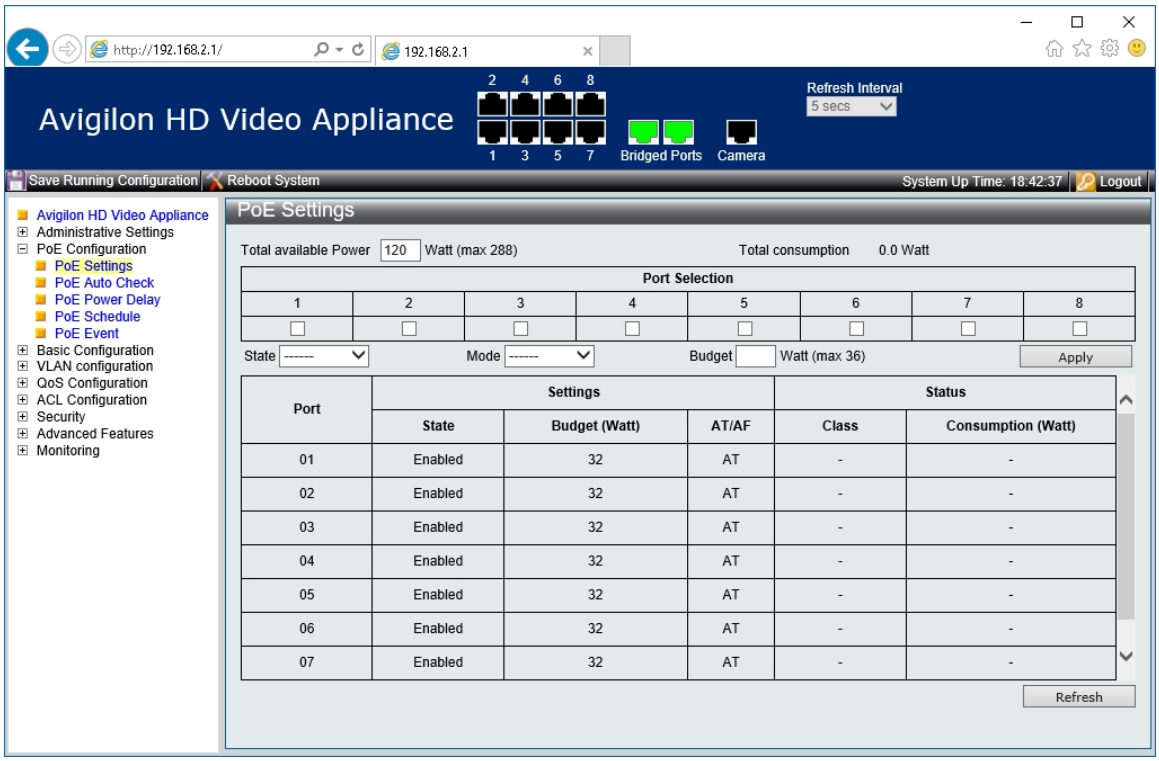
Configuring the PoE Budget From the Switch Management WebUI

The default power budget for all ports on any appliance is 32W. However, the 8-port appliance has a total power budget of 120W (8 x 15W), the 16-port appliance has a total power budget of 240W (16 x 15W), and the 24-port appliance has a total power budget of 360W (24 x 15W). Normally, there is no need to adjust the PoE power budget for individual PoE ports even though the sum total power budget across all ports exceeds the total available power. As long as the total power consumed by all connected devices at any time does not exceed the total available power, there will be no impact.

Individual PoE ports can be configured up to a maximum of 36W. This may be useful if you are connecting a device that may occasionally draw more power than the default budget (such as a camera with an IR illuminator or a heater). In that case, you may want to decrease the power budget of other cameras to ensure that when the high-power device draws full power no cameras are dropped for lack of power.

CAUTION — Changing the power budget on the appliance should be done with care, as there a risk that some devices may lose power. As long as the total power consumed by all connected devices at any time does not exceed the total available power, there will be no impact. However, if the power drawn by all connected devices exceeds the total power available for your appliance, some devices will lose power.

1. Open the Switch Management WebUI if it is not already open.
2. Expand **PoE Configuration** and click **PoE Settings** from the left menu pane.
3. In the PoE Settings area, review the PoE budget for each port and make changes:
    a. Click in the check boxes to select the ports to change.
    b. Enter the new port power budget.
    c. Click **Apply**.
    d. Repeat to change the power budget on other ports if necessary.



    e. Click **Refresh**.
4. Exit the Switch Management WebUI.

Connecting Devices to the Video Appliance

Depending on how you intend to use the Video Appliance, you may choose to configure the network switch component of the appliance differently.

1. A ZeroConf device network— the appliance and the connected cameras will run as a self contained system without a DHCP server.

   This configuration is most likely used by a small business that may not have a network infrastructure, and prefers to use the appliance like a traditional closed circuit surveillance system.

2. A network with an external DHCP server — the appliance and the connected cameras will work with an existing DHCP server on the network.

   This configuration is most likely used by a small office that already has some network infrastructure that will be used with the appliance, like a router that gives the office computers internet access.

3. A network of connected cameras with previously assigned static IP addresses within a different subnet.

   This configuration is most likely used by a business that has existing third-party or Avigilon cameras with static IP address that were previously assigned, or if static IP addresses are desired for cameras.

4. An internal DHCP server — the appliance will act as the local DHCP server for the connected cameras and any other devices that may also be connected to the appliance.

   NOTE: The appliance is intended to be used for connecting and powering IP cameras, not for general computer networking. However, if you prefer, the appliance can be configured to do so.

   This configuration is most likely used by a small business that prefers to use the appliance switch component instead of a router for connecting all network devices together. Other network devices can include voice over IP (VoIP) phones or external network drives.

Complete the procedure that will configure your preferred network:

- *Configuring a ZeroConf Device Network* below.
- *Configuring a Network with an External DHCP Server* on the next page
- *Connecting to Cameras with Static IP Addresses* on the next page
- *Configuring the Internal DHCP Server* on page 23

Configuring a ZeroConf Device Network

If you plan to connect cameras directly to the Video Appliance and run a self contained system, all you need to do is connect cameras directly to the numbered ports.

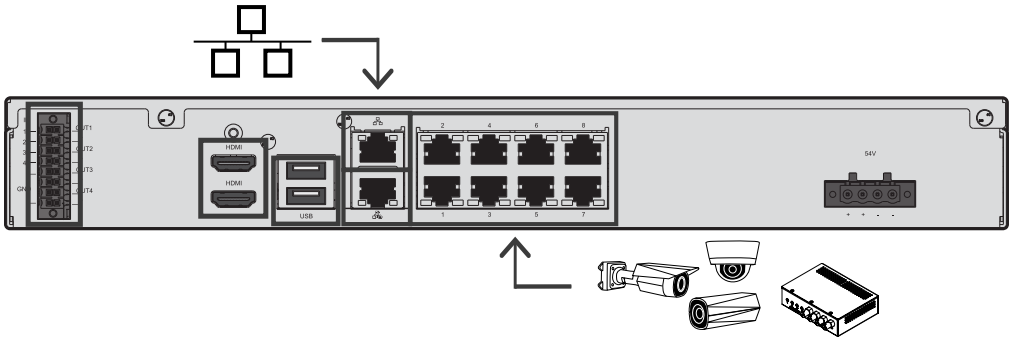


Figure 10: Example of no DHCP network connections on an 8-port Video Appliance.

Avigilon cameras are able to assign IP addresses to themselves through Zero Configuration Networking (ZeroConf) when a DHCP server is not available. The Avigilon Control Center software should automatically detect all connected cameras through the 169.254.0.0/16 subnet.

If you would like to access the Internet through the Video Appliance, you can add an Internet connection to the corporate LAN uplink port, identified by the icon. The corporate LAN uplink port is separate from the numbered camera ports, so it will not interfere with video recording.

After you connect cameras to the numbered ports, you can configure the Avigilon Control Center system. See *Configuring the ACC Software* on page 31.

Configuring a Network with an External DHCP Server

If you already have a router or switch to connect your other network devices you can connect the Video Appliance directly to the router so that cameras can be addressed using the router's built-in DHCP service.

1. Connect a network cable from the router or switch to the camera network port on the back of the appliance, identified by the icon.
2. Connect Avigilon cameras to the numbered PoE ports.
3. If you would like to access the Internet through the Video Appliance, you can add an Internet connection to the corporate LAN uplink port, identified by the icon. The corporate and camera LAN uplink ports are separate from the numbered camera ports, so they will not interfere with video recording. Ensure that the cameras are in a different IP subnet from the corporate network (or Internet connection).

After you've made the required network and camera connections, you can configure the Avigilon Control Center software. See *Configuring the ACC Software* on page 31.

Connecting to Cameras with Static IP Addresses

If you plan to connect cameras with assigned static IP addresses to the Video Appliance, you must change the IP address of the Internal Camera LAN NIC to an IP address in the same subnet as the cameras. For information about identifying this NIC, see *Video Appliance Network Interface Connections* on page 13.

Before you start this procedure, obtain an available IP address from the same subnet as the cameras to assign to the appliance.

1. Connect a monitor, keyboard and mouse to the appliance. Alternatively, you can start a remote session to the appliance if you have network access to the appliance.
2. From the appliance, access the Windows Network Connections window, using one of the following methods:
    - Right-click on the Windows button and select **Network Connections**

      Or

    - Select **Start** > **Settings** > **Network & Internet** > **Change adapter options**

      Or

    - From the taskbar, search for `ncpa.cpl`
3. In the Network Connections window, right-click the Internal Camera LAN connection and select **Properties**.

   NOTE: Do not change or disable any of the other network connections.

4. In the Properties dialog box for the Internal Camera LAN, double-click **Internet Protocol Version 4 (TCP/IPv4)**.

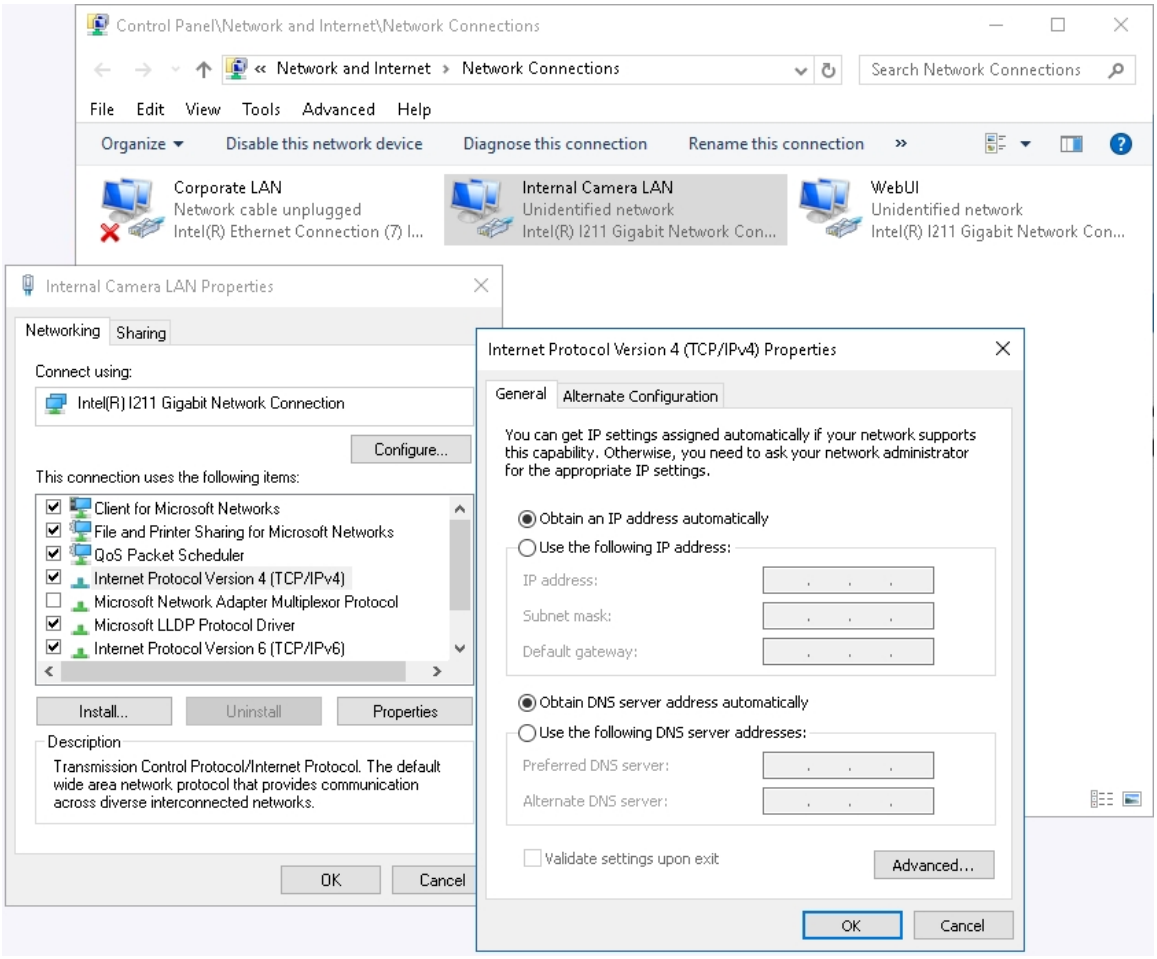


Figure 11: The Network Connections window showing the Properties dialog box for the Internal Camera connection. (Used with permission from Microsoft.)

5. In the dialog box that appears, select the **Use the following IP address:** option and assign the static IP address in the same subnet as the cameras that you obtained.

   The camera network uplink port should have one IP address, subnet mask details, no default network gateway, and no DNS server details.

6. Connect theVideo Appliance to your corporate network using the corporate network uplink port. This port is separate from the numbered camera ports, so it will not interfere with video recording. This allows corporate users to to access the cameras connected to this appliance using the ACC Client.

Configuring the Internal DHCP Server

If you must use IP addresses within a predefined range at your site for your cameras and devices, or you plan to connect network devices that rely on a DHCP server to receive an IP address before they can work with the local camera connector ports, you may need to set up the Video Appliance to be a DHCP server.

The administrative user of the Switch Management WebUI can complete this procedure.

NOTE: After you setup the internal DHCP server, do not connect any external DHCP servers to the appliance or there may be address conflicts and cause connection issues.

Tip: If you are only going to connect Avigilon cameras to the appliance, you do not need to set up a DHCP server. For more information, see *Configuring a ZeroConf Device Network* on page 20.

1. Connect a monitor, keyboard and mouse to the appliance. Alternatively, you can start a remote session to the appliance if you have network access to the appliance.
2. In a web browser, enter `192.168.2.1` into the address bar to open the Switch Management WebUI and log in as the administrator user **admin**.
3. Expand **Advanced Features** and click **DHCP Server** from the left menu pane.

4. In the DHCP Server setting area:
    a. In the Status field, select **Enable**.
    b. In the IP start from field, enter the IP address from which to start numbering.

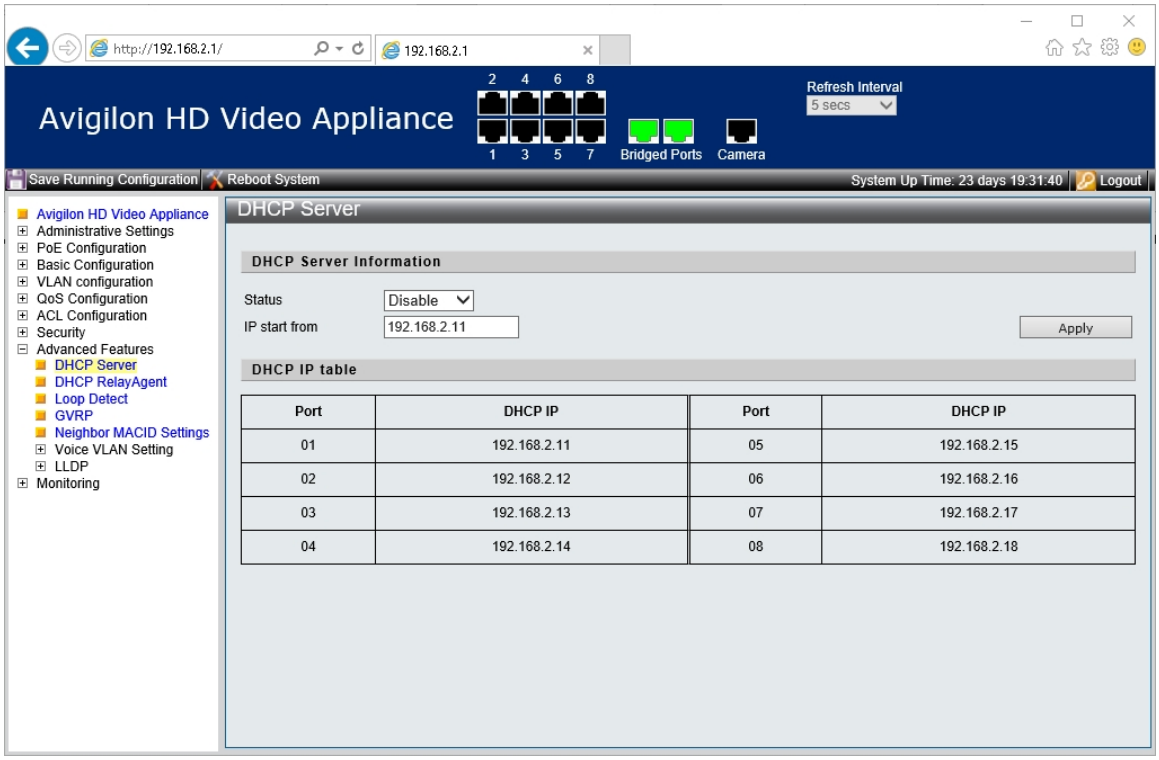


Figure 12: The DHCP Server settings page.

    c. Click **Apply**.
    d. Click **Save Running Configuration**.
    e. The appliance is now set to act as a DHCP server.

    When you connect camera or network devices to a local camera connector port, the IP address beside that connector port's number will be assigned to that camera or device.

    NOTE: The corporate network uplink and camera network uplink ports on the Video Appliance are not part of this DHCP setting. Only the camera network ports broadcast DHCP.

5. Connect Avigilon cameras and other network devices to the numbered ports.

    Each connected device is automatically assigned an IP address by the appliance.

6. If you would like to access the Internet through the Video Appliance, you can add an Internet connection to one of the corporate network ports. The corporate network ports are separate from the numbered camera ports, so they will not interfere with video recording.

After you've made the required network and camera connections, you can configure the Avigilon Control Center system. See *Configuring the ACC Software* on page 31.

Starting the ACC Software for the First Time

The ACC Client software should start automatically when your Windows workstation starts. Refer to *Starting Up and Shutting Down the ACC Client Software* below if it doesn't.

The first time you start the ACC Client software:

1. Log in to an ACC site. For more information, see *Logging In to and Out of a Site* below.
2. Change the site administrator password. For more information, see *Changing the Site Administrator Password* on page 28

Starting Up and Shutting Down the ACC Client Software

Starting Up the ACC Client Software

Perform one of the following:

- In the Start menu, select **All Programs** or **All Apps** > **Avigilon** > **Avigilon Control Center Client**.
- Double-click  or  desktop shortcut icon.
- From the Avigilon Control Center Admin Tool, click **Launch Control Center Client**. For more information, see the *Avigilon Control Center Server User Guide*.

When you are prompted, log in to your site. You can only access cameras and video after you log in.

Shutting Down the ACC Client Software

1. In the top-right corner of the ACC Client software, select  > **Exit**.
2. When the confirmation dialog box appears, click **Yes**.

Logging In to and Out of a Site

After you start the ACC Client software, you are immediately asked to log in.

After you start the ACC Client software, the “Select one or more sites to log in.” message appears. If you are connected only to the new device, one site is listed in the left navigation panel. Otherwise, all the sites that are connected to the same network are listed. The site name of your new device is the hostname that you assigned in the Web Interface. You can use Find Site... to specify the IP address or hostname of the device if the list is long.

The default username is *administrator* with no password. The first time you log in you are asked to change the site administrator password.

Logging In

1. Open the Site Login tab. The Site Login tab is automatically displayed if you are launching the Client software for the first time.

   To manually access the Site Login tab, do one of the following:

   - From the top-right corner of the window, select > **Log In...**.
   - From the top-left corner of the application window, click to open the New Task menu, then click .

2. On the left side of the Site Login tab, select one or more sites.

   If the site you want to log into is not shown, click **Find Site...** to discover the site.

3. Enter your username and password for the selected sites.
4. Click **Log In**.
5. If Two-Factor Authentication is required, a dialog box is displayed.
   a. The first time you log in, a QR code is displayed. On your mobile device, scan the QR code with a TOTP authenticator app like the Google Authenticator™ mobile app or the FreeOTP Authenticator™ mobile app. If you cannot scan the QR code, enter the 20-character key into the authenticator app.

      The authenticator app will display a 6-character verification code.

   b. The next time you log in, use the authenticator app to get your verification code.
   c. Enter the code in the **Verification Code:** box.

      Tip: Select the **Trust this device for 30 days** check box to avoid entering a verification code each time you log in.

   d. Click **OK**.

   You are logged in to the selected sites.

If you want to be notified when new or disconnected sites come online, select the **Notify me when additional sites become available** check box.

If you want to see the login page each time you launch the Client software, select the **Show this tab on startup** check box. If you prefer not to login each time, you can disable this option and configure automatic login from the Client Settings dialog box.

Logging Out

You can log out of one or all sites at any time.

To...	Do this...
Log out of one or select sites	• In the System Explorer, select one or more sites then right-click and select **Log Out**.
Log out of all sites	1. In the top-right corner of the ACC Client, select > **Log Out**.

To...	Do this...
	2. In the confirmation dialog box, click **Yes**.

Changing the Site Administrator Password

After you log in to the site for the first time, it is recommended that you change the default site administrator password. This is only required for a new site.

1. After you login, the Change Password dialog is displayed.
2. Enter a new password and then confirm the new password.

   The password must meet the minimum strength requirements.

   -  — password meets the strength requirements.
   -  — password does not meet the strength requirements, enter a new password.

   The password strength is defined by how easy it is for an unauthorized user to guess. If your password does not meet the strength requirements, try entering a series of words that is easy for you to remember but difficult for others to guess.
3. Click **OK**.

WARNING — If you forget the site administrator password, resetting the password requires restoring the factory default settings on every server in the site. To avoid this issue, it is highly recommended that you create at least one other site administrator level user as a backup.

Connecting Cameras to the Avigilon Control Center Software

After all the cameras in your system have been physically connected to the Video Appliance, you need to connect the cameras to the ACC software so that video can be recorded and indexed for search.

1. In the site Setup tab, click  .

   The Connect/Disconnect Devices... tab is displayed.
2. In the Discovered Devices area, select one or more devices then click **Connect...**.

   Tip: You can also drag the device to a server on the Connected Devices list.
3. In the Connect Device dialog box, select the server you want the device to connect to.

   NOTE: If you are connecting multiple devices, all the cameras must use the same connection settings.

4. If you are connecting a third-party device, you may choose to connect the device by its native driver. In the **Device Type:** drop-down list, select the device's brand name. If there is only one option in the drop-down list, the system only supports one type of driver from the device.
5. In the **Connection Type:** drop-down list, select **Primary**. The device will automatically connect to this server if they are in the same network.

   If you are creating a failover connection, select Secondary or Tertiary.
6. In the **License Priority:** drop-down list, select the appropriate license priority. The highest priority is **1** and the lowest priority is **5**.

   NOTE: This option is only available if you are connecting to a Secondary or Tertiary server.

   The License Priority: setting decides the order that devices are connected to the server. The server will try to connect cameras with a higher priority before cameras with lower priority. If the server does not have enough camera channel licenses, low priority devices may not be connected. A camera channel license is only used when the device actually connects to the server.
7. If the camera supports a secure connection, the **Device Control:** drop-down list is displayed. Select one of the following options:

   NOTE: The setting may not be displayed if the camera only supports one of the options.

   - **Secure** — The system will protect and secure the camera's configuration and login details. This option is selected by default.
   - **Unsecure** — The camera's configuration and login details will not be secured and may be accessible to users with unauthorized access.

     Cameras with a secure connection are identified with the icon in the Status column.
8. In the **Network Type:** drop-down list, select whether the camera is connected to the **LAN** (local area network) or **WAN** (wide area network).

   Select the WAN network type to connect to cameras on your local network if the Internet Control Message Protocol (ICMP) is blocked or disabled.
9. If it is not displayed, click to display the Site View Editor and choose where the device appears in the System Explorer.

   - In the site directory, drag devices up and down the right pane to set where it is displayed.
   - If your site includes folders, select a location for the device in the left pane. The right pane updates to show what is stored in that directory.
   - If you are connecting multiple devices at the same time, the selected devices must be assigned to the same location.

   Tip: If the site you want is not listed, you may need to connect the device to a different server. Make sure the selected server is connected to the site you want.
10. Click **OK**.

11. If the device is password protected, the Device Authentication dialog box appears. Enter the device's username and password, then click **OK**.

Configuring the ACC Software

Complete the following procedures in the ACC Client software to configure the ACC software to work with your newly installed device.

For more information about any of the following procedures, see the Help files provided with the ACC Client software.

Setting the Recording Schedule

Once all the cameras have been connected, you can set when you want each camera to record video.

By default, all connected cameras are set to record when events are detected by the system. You can skip this procedure if you prefer to keep the default settings.

Before you can assign a recording schedule, you must create a template. The template allows you to assign the same schedule to multiple cameras.

Creating a Recording Template

The events that can be selected for the template depend on the licensed features in your system.

1. In the server Setup tab, click  . The Recording Schedule dialog box is displayed.
2. Click **Add Template** below the Templates: list.
3. Enter a name for the **New Template**.
4. Click the **Set Area** button, then click or drag the cursor across the **Recording Mode:** timeline to set the types of events that the cameras will record throughout the day. Individual rectangles on the Recording Mode: timeline are colored when they have been selected.

   The **Recording Mode:** options include:

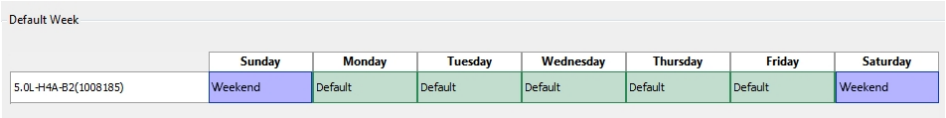
   - **Continuous** — record video constantly.
   - **Motion** — only record video when motion is detected.
   - **Digital Inputs** — only record video when a digital input is activated.
   - **Alarms** — only record video when an alarm is activated.
5. To disable recording in parts of the template, click the **Clear Area** button, then click or drag the cursor across the timeline to remove the set recording areas.
6. If cameras are *not* recording in Continuous mode all day, you can set cameras to record reference images between events in the recording schedule.

   - Select the **Record a reference image every:** check box, then set the time between each reference image.

Setting Up a Weekly Recording Schedule

You can set up a weekly recording schedule by applying templates to cameras for each day of the week.

1. In the server Setup tab, click  . The Recording Schedule dialog box is displayed.
2. Select a template from the Templates: list.
3. In the Default Week area, click the days of the week this template applies to for each camera.



4. Click **OK**.

Setting Data Aging

Data aging defines how long recorded video is stored and the quality of the video as it ages over time. In the ACC software, the recorded image rate is slowly reduced so that the recorded video can be viewed over a longer period of time while still making room for new recordings. You can adjust how long the full image rate video is kept, so that you have the best quality video when you need it.

The amount of data aging that is available depends on the camera you have connected to your system:

- For JPEG2000 or JPEG compression cameras, data aging is available at three rates:
  - **High Bandwidth** keeps recordings at their original quality.
  - **Half Image Rate** discards half of the recorded data to make room for new recordings.
  - **Quarter Image Rate** keeps 1/4 of the original recorded data so that you can still see older video.
- For H.265 and H.264 cameras that support data aging, data aging is available at two rates:
  - **High Bandwidth** keeps the original high quality video and the secondary stream of low resolution video.
  - **Low Bandwidth** only keeps the secondary stream of low resolution video.

  NOTE: The data aging can only occur when the secondary stream is enabled.
- For H.265 and H.264 cameras that *do not* support data aging, only the **High Bandwidth** video is kept.

By default, the system is set to keep recorded video for the maximum amount of time based on the available storage.

At the bottom of the Recording and Bandwidth dialog is the following statement:

> *Total record time estimate is based on constant recording*

The retention time is determined by the **Max. Record Time** setting and the average camera data rate. Since the system can only provide an estimate of the data rate for the full retention period, the actual retention time may exceed the Max. Record Time setting by 5 minutes.

NOTE: The time shown in the Total Record Time column is an estimate only.

1. In the server Setup tab, click .

   The Recording and Bandwidth dialog box is displayed.

   The Data Aging column shows an estimate of the recording time that is available at each image rate, given the amount of space on the recording device.

2. In the Data Aging column, move the sliders to adjust the amount of time video is stored at each image rate.
   - To change the data aging settings for all linked cameras, move the slider for one linked camera and all linked cameras will be updated.
   - To change the data aging setting for one camera, break the camera's link to other cameras by clicking the icon to the left of its name, then make your changes.
3. In the **Max. Record Time** column, manually enter a maximum record time or select one of the options from the drop-down list for each camera.

   NOTE: If the time estimated in the Total Record Time column is significantly shorter than what is set in the Max. Record Time column, the camera's actual recording time will be closer to the Total Record Time estimate.

4. Click **OK**.

Adding Users and Groups

If there will be other people using the system, you may want to add them as separate users rather than giving them access through the default administrator account.

Before you can add individual users, you will need to add permission groups that define what users have access to. By default, the system has the following groups:

- **Administrators** — has access to everything in the system.
- **Power Users** — has access to most features in the system except for the ability to import and export settings.
- **Restricted Users** — has access to live video only and can control audio and digital outputs.
- **Standard Users** — has access to live and recorded video, but cannot make any Setup changes.

It is highly recommended that the Administrators group includes at least two users. In the event one administrator user forgets the default administrator password, the second administrator user can be used to reset the password. If you do not have a second administrator user, you may need to completely reset the system.

Adding Groups

1. In the site Setup tab, click .
2. In the following dialog box, select the Groups tab and click **Add Group**.
3. In the pop-up dialog box, select an existing group to use as a template for your new group, then click **OK**.
4. In the Edit Group dialog box, complete the following:
    a. Give the new group a name.
    b. Select a rank for the group from the **Rank:** drop-down list. To edit or view the entire Corporate Hierarchy, click .
    c. Move the **Min Password Strength:** slider to define how strong the password used by each user in the group must be.

       The password strength is defined by an algorithm that anticipates how easy a password is to guess. There is no defined character minimum, but the stronger the setting, the harder it should be for an unauthorized user to crack the password.

       Tip: If users are expected to change their passwords frequently, you may want to select a weaker setting to ensure users do not have difficulty choosing new passwords.

    d. To enable Two-Factor Authentication, select the **Required** check box.

       The next time users in this group log in, they will need to download an authenticator app on their mobile device and scan a QR code to log in to a site.

       For proper use, ensure your servers sync to a real-time source. Verification codes are only valid within +/- 5 minutes of the server's time. If this does not match the time on the user's mobile device, the user will not be able to log in.

       NOTE: The default administrator will be able to log in to a site without Two-Factor Authentication, even if it is enabled for their group.

       Important: Two-Factor Authentication is not supported on the ACC Mobile 2 or ACC Mobile 3 Preview apps, the ACC Virtual Matrix software, or the ACC Gateway Web Client. Users with Two-Factor Authentication enabled will not have access to these programs.

    e. Select the required **Group Privileges:** and **Access Rights:** for the group. Clear the check box of any feature or device that you do not want the group to have access to.
5. To enable the Dual Authorization feature, click **Enable Dual Authorization**.

   When you enable Dual Authorization, users in this group cannot review recorded video without permission from a user in the authorizing group.

a. In the following dialog box, click the toggle to enable Dual Authorization.
b. Select the groups that can grant authorization to users in this group.
c. To disable the feature, click the toggle at the top of the dialog box.
d. Click **OK**.

6. Select the Members tab to add users to the group.

   If a user is added to the group through the Add/Edit User dialog box, the user is automatically added to the group's Members list.

   a. Click .
   b. Select the users that should be part of this new group. Only users that have been added to the site are displayed.

      Tip: Enter the name of a user in the **Search...** field to locate specific users.

   c. Click **Add**. The users are added to the Members list.
7. Click **OK** to save the new group.

Adding Users

1. In the site Setup tab, click .
2. In the Users tab, click **Add User**.
3. When the Add/Edit User dialog box appears, complete the User Information area.
4. If you don't want this user to be active yet, select the **Disable user** check box. Disabled users are in the system but cannot access the site.
5. In the Login Timeout area, select the **Enable login timeout** check box to set the maximum amount of time the Avigilon Control Center Client software can be idle before the user is automatically logged out of the application.
6. Select the **Member Of** tab to assign the user to a group.
   a. Select the check box beside each access group the user belongs to.

      The other columns display the permissions that are included in the selected groups.

   b. Return to the **General** tab.
7. In the Password area, complete the following fields:
   - **Password:** — enter a password for the user.
   - **Confirm Password:** — re-enter the password.
   - **Strength:** — indicates the strength of the password. The strength is defined by the group the user is assigned to. If the user is a member of more than one group, the user must meet the strongest password requirement.

     The password must meet the minimum strength requirements.

-  — password meets the strength requirements.
-  — password does not meet the strength requirements, enter a new password.

The password strength is defined by how easy it is for an unauthorized user to guess. If your password does not meet the strength requirements, try entering a series of words that is easy for you to remember but difficult for others to guess.

- **Require password change on next login** — select this check box if the user must replace the password after the first login.
- **Password Expiry (Days):** — specify the number of days before the password must be changed.
- **Password never expires** — select this check box if the password never needs to be changed.

8. Click **OK**. The user is added to the site.

Repeat this procedure to add all the users that are required.

Advanced Settings

After you've set up all the required settings in the ACC Client software, the system can start running.

In the following list are some advanced settings on the setup panels you can use to further customize your system. See the application Help files for details about how to configure each setting.

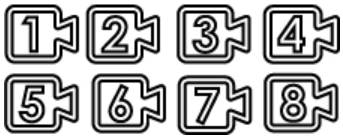
- Adjust camera settings (on the camera setup panel)
    - If the camera video looks slightly blurry or unclear, you can adjust the camera's Image and Display settings.
    - If you want the camera to record at a different image rate, you can adjust the camera's Compression and Image Rate settings.
    - To reduce the amount of ambient motion detection for a specific camera, you can adjust the Motion Detection settings.
    - To maintain the privacy of certain areas, you can set Privacy Zones in the camera's field of view so that private spaces are never recorded.
- Add a joystick (on the camera setup panel)
    - If you prefer to control PTZ cameras with a standard USB joystick, you can install and set up a joystick from the Client Settings dialog box.
    - If you prefer to use the Avigilon Professional Joystick Keyboard with the AvigilonControl Center Client software, you can install and setup the joystick keyboard from the Client Settings dialog box.

- Email notifications (under External Notifications on the site setup panel)
    - You can set up an SMTP email server to send you messages when system events occur.
    - If you have a Standard Edition system, you can set up detailed rules to notify you when specific events occur.
- Setup the Gateway
    - The Avigilon Control Center Gateway software allows you to access video from a remote web browser or mobile device. If the gateway software is not set up, you cannot access video outside of your local network.
    - Install the Avigilon Control Center Mobile app on your mobile device so that you can monitor live and recorded video anywhere.

LED Indicators

The following lists describe what the LEDs on the front and back of each Video Appliance indicate.

Front Panel LEDs

Icons	LED Status	Description
	Green	Device is powered and the ACC server is running normally.
	Orange	Device is powered but ACC has been stopped or has crashed and is not running, or device is restarting and the ACC server is not yet running.
	Green - blinking	Hard disk drive activity.
	Red	Hard disk drive has an error.
 16 for the 16-port Video Appliance. 24 for the 24-port Video Appliance.	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.

RJ45 Ethernet LEDs on the Back Panel

LED Status	Description
Green	Network activity is present.
Orange	For PoE ports: On for 100 Mbps speed. Off for 10 Mbps speed. For corporate and camera uplink ports: On for GigE speed. Off for 10/100 Mbps

LED Status	Description
	speed.

Connecting to External Devices

External devices are connected to the Video Appliance through the digital I/O connector. The pinout for the I/O connector is shown in the following diagram:

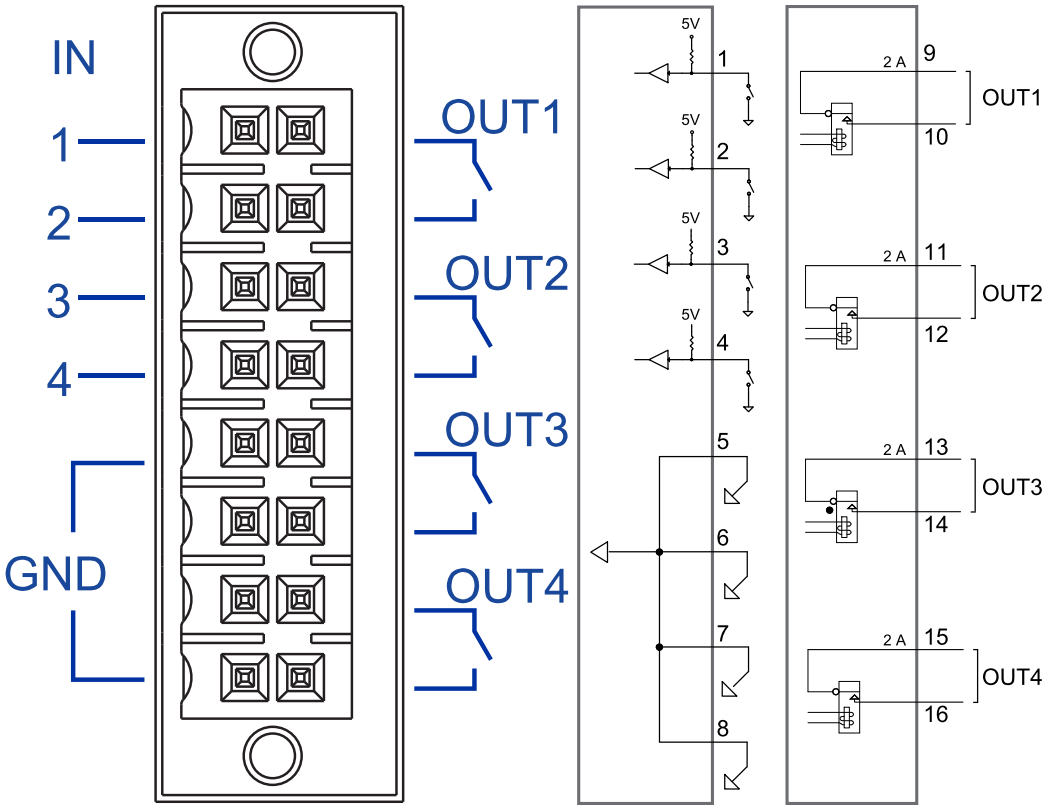


Figure 13: Digital I/O connector pinout schema.

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		

Pin	Function	Description
9	OUT1	Relay Outputs — Form-A dry contact outputs. When active, terminals are connected. When inactive, terminals are disconnected. **NOTE:** Contacts are normally open. The contacts are open when the energizing force (magnet or relay solenoid) is not present. When the energizing force is present, the contact will close. Maximum load is 30 V, 0.5 A.
10		
11	OUT2	
12		
13	OUT3	
14		
15	OUT4	
16		

Restarting the Operating System

Use the reset switch on the front of the appliance to restart the operating system if the operating system ever freezes or displays a fatal system error.

Use the reset switch while the appliance is powered. An operating system reset does not affect the Ethernet switch component or the connected cameras.

The reset switch is located at the front of the appliance and is the small unlabeled hole between the Avigilon logo and the ⏻ status LED.

After you've located the reset switch on the appliance, complete the following steps:

1. Using a straightened paperclip or similar tool, gently press the reset switch and release after one second.

   ⚠ **CAUTION —** Do not apply excessive force. Inserting the tool too far will damage the appliance.

   After you release the reset switch, the operating system should automatically restart.

Resetting the Internal PoE Switch to Factory Defaults

Use the reset switch on the front of the appliance to reset the internal PoE switch to its factory default settings. Resetting the switch to factory default settings also resets the user password back to the appliance's serial number.

The reset switch is located at the front of the appliance and is the small unlabeled hole between the Avigilon logo and the ⏻ status LED.

After you've located the reset switch on the appliance, complete the following steps:

1. Using a straightened paperclip or similar tool, gently press and hold the reset switch.
2. Do not release the reset switch until you hear a confirmation beep, which takes about 12 seconds.

> ⚠ **CAUTION —** Do not apply excessive force. Inserting the tool too far will damage the appliance.

Replacing a Hard Drive

If the ACC software starts to perform excessively slow or becomes prone to freezing, these may be signs of a potential hard drive failure.

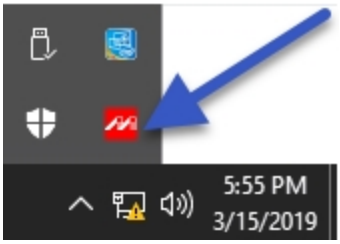
8-port Video Appliance: Immediately shut down your system and contact Avigilon Technical Support for possible recovery instructions.

On the 16-port or 24-port Video Appliance, the **Hard Drive Status** LED turns red if one of the hard drive connections is in error and is potentially failing.

Important: Only use a hard drive for the Video Appliance available from your Avigilon dealer. Always replace a hard drive with the same size, make and model, or the appliance will continue to fail.

Use the Marvell Storage Utility that is provided on the 16-port or 24-port Video Appliance to confirm which hard drive is in error.

1. Open the Windows system tray and click on the MarvellTray icon:



Important: By default, this utility starts when the Video Appliance is powered up and runs in the background. If you don't see the icon in the system tray, you need to start it. From the Windows Start menu, select:

2. The Marvell Storage Utility opens in your web browser.

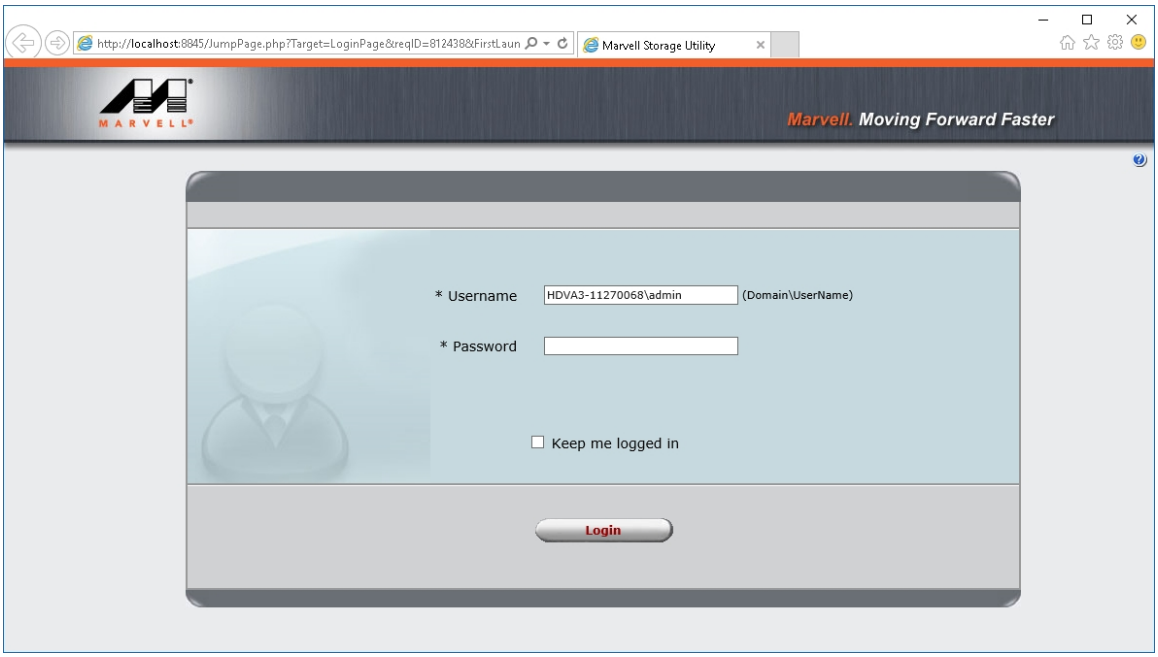


Figure 14: The Marvell Storage Utility Login Page

NOTE: If the MarvellTray icon does not open the Marvell Storage Utility, try opening **http://localhost:8845** in the web browser.

3. In the Marvell Storage Utility page, look in the Marvell Storage Management tree to see if the Array:0 and Virtual Disk:0 icons are in the yellow alarm state. If the icons are yellow, scan the list of physical disks in the array, to identify which disk has failed. In normal operation, the disks are labeled Physical Disk: port 0 to Physical Disk: port 3. If one is missing, this is the disk that has failed.

   You can also review the messages in the Event Log at the bottom of the Marvell Storage Utility page to see additional information.

In the Marvell Manager, the hard drives are listed as Physical Disk: port 0 to Physical Disk: port 3. From the front of the appliance, Physical Disk: port 0 is the hard drive installed on the far left and Physical Disk: port 1 to Physical Disk: port 3 are installed beside each other from left to right.

If more than one drive has failed, immediately shut down your system and contact Avigilon Technical Support for possible recovery instructions.

To replace a failed hard drive, complete the following steps.

1. Exit all running programs and shut down the Windows operating system.
2. Disconnect the appliance from power:
   a. Undo the plastic clip securing the power cable to the power receptacle at the rear of the appliance
   b. Unplug the power cord.

3. Remove the front bezel:
    a. Slide the appliance out from the rack enough to allow you to access the screws that attach the front bezel.
    b. Remove the screw on each side of the bezel.
    c. Pull the bottom edge of the bezel slightly away from the appliance to detach the plastic clip at the top and then remove the bezel. Be careful not to snap off the clip.
4. Remove the hard drive caddy:
    a. Press on the tab on the left side of the hard drive caddy cover to unlatch it and then swing the cover open.

Figure 15: The hard drive caddy in the open position.

    b. Slide the caddy out of the appliance.
    c. Remove the silver-colored screws on the side that attach the hard drive to the caddy.
    d. Use some force to push the right-hand side of the hard drive out of the caddy. It is held in place by several pins on the left-hand side.
5. Properly dispose of the failed hard drive.
6. Install the replacement hard drive:
    a. Insert the new hard drive into the caddy. Make sure that it clips into place.
    b. Screw the hard drive to the caddy.
    c. Place the caddy into the appliance, then slide the caddy into the appliance, close the caddy cover and latch it into the appliance.
    d. Reattach the front bezel.
    e. Connect your mouse, keyboard and monitor back to the appliance.
    f. Before connecting the power cord to the mains, plug in the power cord and reattach the plastic clip securing the power cable to the power receptacle at the rear of the appliance.
7. Connect power to the appliance and allow the system to restart:
    a. The system immediately begins to rebuild the RAID.
    b. When prompted, allow Windows to start normally.

    Important: Shut down the ACC server as soon as it starts, as it will not function while the RAID is rebuilding.

c. While the RAID is being rebuilt, do not reconnect cameras, open other applications or allow any network instances of the ACC Client software to connect to the appliance. If you try to resume normal operations while the RAID rebuilds, you may lose recorded data and cause further issues in the appliance.

8. After Windows has started and the ACC server is shut down:
    a. Start the MarvellTray application and open it from the system tray.
    b. Open the Property tab and confirm that the Background activity state is "Rebuild running".

       The RAID rebuild will take at least 24 hours, or longer depending on the total amount of recorded data stored on the array of disks.

       When the rebuilding process is complete, the RAID status changes to *Normal*.
9. After the system has finished rebuilding, reconnect all your cameras, restart the ACC server and resume normal operations.

Replacing the Power Supply in the 16- or 24-port Video Appliance

The power supply unit (PSU) in the 16- or 24-port Video Appliance is replaceable if the PSU becomes unreliable or fails.

Important: Only use a PSU for the Video Appliance available from your Avigilon dealer.

Important: If you are replacing a PSU before it has fully failed, ensure that you have powered down the appliance by exiting all running programs and shutting down the Windows operating system.

To remove the failed PSU:

1. Undo the plastic clip securing the power cable to the power receptacle at the rear of the appliance, and unplug the power cord.
2. Slide the appliance out from the rack.
3. Undo the screws at the front of the appliance that attach it to the mounting rails.
4. Remove the appliance from the rack unit and place it on a solid work area, with the rear panel facing outward.
5. Hook your index finger into the tab on the inner side of the PSU and use your thumb to press the latch on the outer side inwards until the PSU is released.
6. Pull the PSU out of the appliance and properly dispose of it.

To insert the replacement PSU:

1. With the tab and latch correctly oriented, firmly push the new PSU into the appliance until you hear the PSU click into place and the latch is locked.
2. Place the appliance onto the mounting rails and screw the appliance back to the rails.
3. Reattach all cables, and plug in the power cord last of all.
4. Reattach the plastic clip securing the power cable to the power receptacle at the rear of the appliance.
5. The appliance will power up as soon as the power supply is restored.

Connecting Multiple Video Appliances to the Same Network

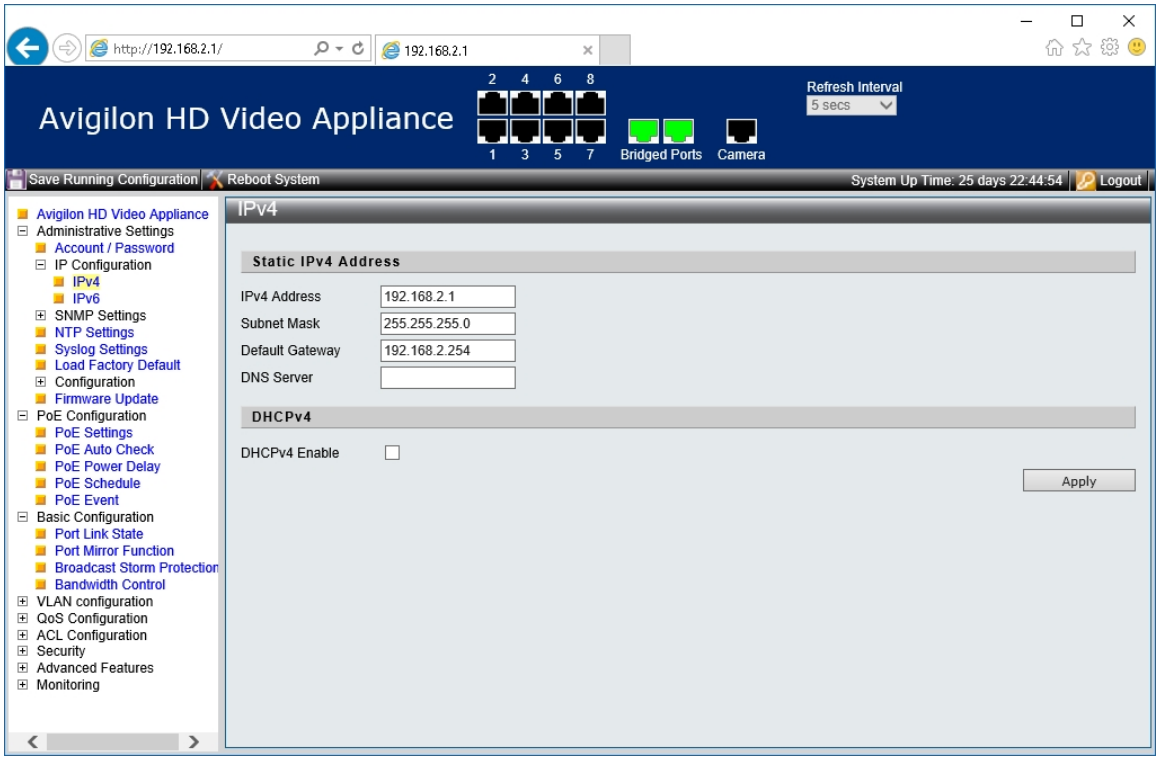
If you add more Video Appliances to the same camera network, and you need to manage the internal network switch with the Switch Management WebUI, assign each added appliance a unique IP address in the local subnet. Changing the local subnet address used to access the Switch Management WebUI of an appliance does not impact usage of the appliance in any other way.

The default IP address for the Switch Management WebUI of the internal network switch in every Video Appliance is 192.168.2.1. If you are adding a Video Appliance to your network, you need to assign it an unused IP address in the local loop. Typically, you only need to increment the default address.

To change the IP address for the Switch Management WebUI on the appliance you are adding to your network, complete the following steps:

1. Open the Switch Management WebUI using the default IP address.
2. Expand **Administrative Settings** > **IP Configuration** > **IPv4** from the left menu pane.
3. In the Static IPv4 Address area, update the value of the last octet of the **IPv4 Address** field to an unassigned IP address in the local subnet. Do not change any of the other fields.

   For example, to add a second appliance, enter 192.168.2.2. For a third appliance, enter 192.168.2.3, and so on.



4. Exit the Switch Management WebUI.

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-us/**.