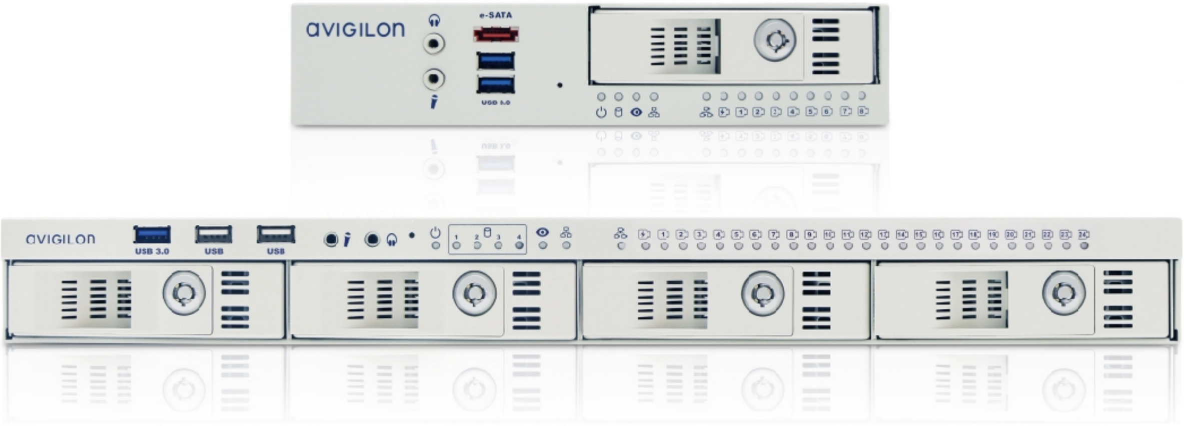


User Guide

Avigilon HD Video Appliance Models:

VMA-AS2-8P, VMA-AS2-16P and VMA-AS2-24P

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.
- Refer all servicing to qualified personnel. Servicing may be required when the device has been damaged, has been exposed to moisture, does not operate normally, or has been dropped.
- 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 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.
- The equipment is not suitable for use in locations where children are likely to be present.
- 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 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).

WARNING — 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.

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

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

For model VMA-AS2-8P: The unit and all interconnected equipment must be installed indoors within the same building, including all POE-powered network connections as described by Environment A of the IEEE 802.3af standard.

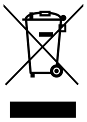
Changes or modifications made to this equipment not expressly approved by Avigilon Corporation or parties authorized by Avigilon Corporation could void the user's authority to operate this equipment.

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.

The contents of this document and the specifications of the products discussed herein are subject to change without notice. Avigilon Corporation reserves the right to make any such changes without notice. Neither Avigilon Corporation nor any of its affiliated companies: (1) guarantees the completeness or accuracy of the information contained in this document; or (2) is responsible for your use of, or reliance on, the information. Avigilon Corporation shall not be responsible for any losses or damages (including consequential damages) caused by reliance on the information presented herein.

Avigilon Corporation
avigilon.com

PDF-VMA-AS2-A

Revision: 1 - EN

20180220

Table of Contents

Introduction

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

- A network switch to connect and power 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.

This guide describes how to configure the system after the appliance has been powered and is connected with keyboard, mouse and monitor. It is recommended that cameras not be connected to the appliance until after the appropriate network configuration has been set up.

Configuring Windows 10

When you start the HD 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**.
5. The Avigilon End User License Agreement is displayed, Review the terms and click **Accept**.

Proceed to activate the license for the Avigilon Control Center software on your HD Video Appliance.

Activate the Avigilon Control Center™ Software

Downgrading to the ACC™ 5 Software:

The HD Video Appliance is pre-installed with Avigilon Control Center (ACC) 6 software. You can use the ACC 6 software or the ACC 5 software. **Do not activate the ACC 6 software if you plan to use the ACC 5 software,** see *Downgrading to the Avigilon Control Center (ACC) 5 Software* on the next page.

Before you can configure cameras and monitor live or recorded video, you will need to activate your ACC software license. The license is provided with the appliance. You will need to purchase a license if you don't already have one.

Other parts of the ACC system may start while you perform this procedure, but you will not be able to use any of the features until after license activation is complete.

Licensing the Avigilon Control Center (ACC) 6 Software

The first time you connect to the new appliance with the ACC Client, you must activate a license for the new ACC software. After the license is activated, you can immediately use the new licensed features.

1. Start and log in to the ACC Client. The "Select one or more sites to log in" prompt is displayed. If you are connected only to the new appliance only one site is listed in the navigation panel to the left. The default name is **HDVA**.
2. Double-click the new appliance name to log in. There is no user name or password set on the appliance.
3. At the top-left corner of the application window, click ☰ to open the New Task menu, then click ⚙.
4. In the site Setup tab, click 🔑.
5. In the License Management dialog box, click **Add License...**.
6. In the following dialog box, select one of the following tabs:
   - If you have internet access, select the **Automatic** tab. Go to *Automatic License Activation* below.
   - If you do not have internet access, or you plan to keep the system in a private intranet, select the **Manual** tab. Go to *Manual License Activation* below.

Automatic License Activation

On the **Automatic** tab:

1. At Enter Product Keys enter the license key.
2. Activate and License Site.

Manual License Activation

On the **Manual** tab:

1. At Enter Product Keys Step 1:, enter the license key.
2. At Generate Activation File click **Save File...** .
3. From the Save As window, choose where you want to save the `.key` file that is generated by the system. You can rename the file as required.
4. Click **Save**.
5. Copy the `.key` file to a computer with internet access.
6. Open a web browser and go to http://activate.avigilon.com.
7. Browse to the location of the `.key` file then click **Upload**. The generated license file (`.lic`) should download automatically. If it does not, allow the download to occur when you are prompted.
8. Copy the downloaded `.lic` file to a location that would be accessible to the ACC Client software.
9. Complete the product registration page to receive product updates from Avigilon, then click **Register**.
10. Return to the ACC Client and at Apply License File click **Apply...**.
11. Locate the downloaded `.lic` file and click **Open**.
12. When the Confirm Licenses dialog box is displayed, click **OK**.

Modifying Licenses

You can also use the the License Management dialog box to add, remove, deactivate, and reactivate licenses for the ACC 6 software. For more information, consult the Help files.

Downgrading to the Avigilon Control Center (ACC) 5 Software

1. Navigate to the **Apps & Features** section of Windows Settings and uninstall the ACC 6 software.
2. Navigate to the D: drive and delete the following directories:

   D:\AvigilonConfig
   D:\AvigilonData

3. Navigate to **C:\Avigilon\Control Center Installation Files\5.10**.
4. Install each application by double-clicking the installers in the following order:

   ACC 5 Server
   ACC 5 Client
   ACC 5 Player
   ACC 5 Gateway

5. To activate your license, refer to the ***Avigilon Control Center Server User Guide*** for the ACC 5 software, available from http://avigilon.com.

HD Video Appliance Networking

The HD 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.

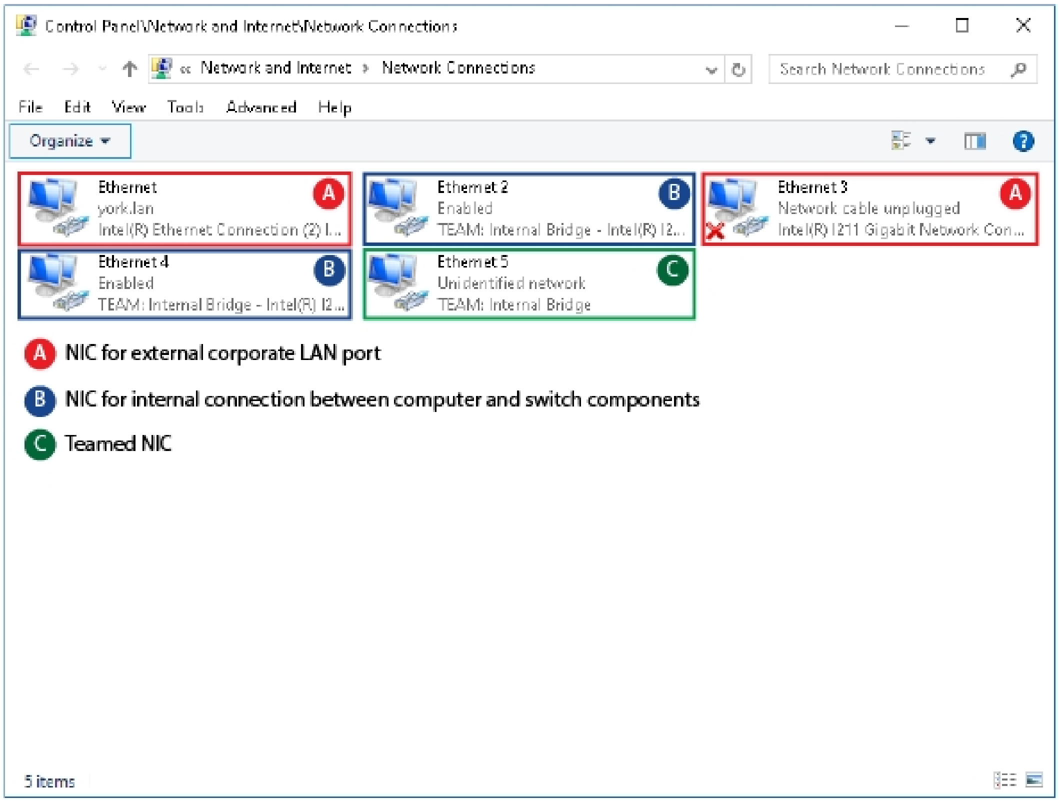
The HD Video Appliance supports five network interface connections (NICs), which appear in the Network Connections window of the operating system, shown in the figure below. These consist of:

- Two NICs for the external corporate LAN ports (see connections labeled "Ethernet" and "Ethernet 3" in Figure 1 below).
- Two internal NICs that connect the built-in computer to the internal switch (see connections labeled "Ethernet 2" and "Ethernet 4" in Figure 1 below).

  CAUTION — DO NOT make any changes to the two internal NICs (labeled "TEAM: Internal Bridge- Intel (R) 1211 Gigabit Network Connection"). Never remove teamed NIC from the Network Connections panel in Windows. If the teamed NIC is removed, the built-in computer cannot connect to the internal switch to receive video traffic. If there is no teamed NIC, or the teamed NIC is not set to Internal Bridge, contact Technical Support.

- A teamed (or virtual) NIC that logically represents the two internal NICs (see connection labeled "Ethernet 5" in Figure 1 below). The teamed NIC, labeled "TEAM: Internal Bridge", is dedicated to handling the traffic between the internal switch and the built-in computer to maintain the highest possible network throughput of recorded video to storage.

NOTE: The NIC label numbering may vary. However, the two internal NICs can be identified by the labels "TEAM: Internal Bridge- Intel(R) 1211 Gigabit Network Connection", and the teamed (or virtual) NIC by the label "TEAM: Internal Bridge". The other two NICs labeled " Intel(R) 1211 Gigabit Network Connection", or "Intel(R) Ethernet Connection I219-LM", are the external corporate network connections.


Control Panel\Network and Internet\Network Connections
« Network and Internet › Network Connections
Search Network Connections
File Edit View Tools Advanced Help
Organize ▾
5 items

Ethernet
york.lan
Intel(R) Ethernet Connection (2) I... A

Ethernet 2
Enabled
TEAM: Internal Bridge - Intel(R) I2... B

Ethernet 3
Network cable unplugged
Intel(R) I211 Gigabit Network Con... A

Ethernet 4
Enabled
TEAM: Internal Bridge - Intel(R) I2... B

Ethernet 5
Unidentified network
TEAM: Internal Bridge C

A NIC for external corporate LAN port

B NIC for internal connection between computer and switch components

C Teamed NIC

Figure 1: The Network Connections Control Panel showing Ethernet 5 as the teamed NIC. (Used with permission from Microsoft.)

The internal network switch supports all of the external PoE ports and two camera network uplink ports, and two internal NICs that connect the switch to the built-in computer. The switch manages the traffic from all of the external connections and directs the video data through the teamed NICs to the built-in computer.

Connecting Devices to the HD Video Appliance

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

The four most typical network configuration scenarios are:

1. A ZeroConf device network— the HD Video 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 HD Video Appliance like a traditional closed circuit surveillance system.

2. A network with an external DHCP server — the HD Video 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 — the HD Video Appliance must be reconfigured so that the Ethernet 5 NIC (labeled "TEAM A") has an IP address in the same subnet as the cameras.

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

4. An internal DHCP server — the HD Video 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 HD Video 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

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

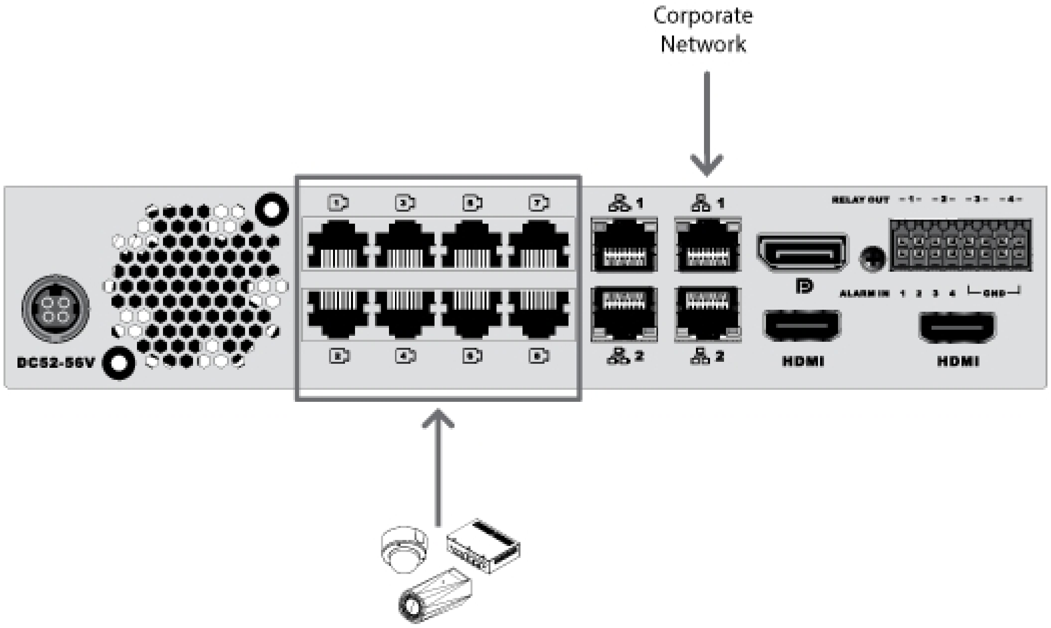


Figure 2: Example of no DHCP network connections on an 8 port HD Video Appliance.

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 HD 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 connect cameras to the numbered ports, you can configure the Avigilon Control Center system. See *Configuring the Avigilon Control Center™ Software* on page 15.

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 HD Video Appliance directly to the router so that cameras can be addressed using the router's built-in DHCP service.

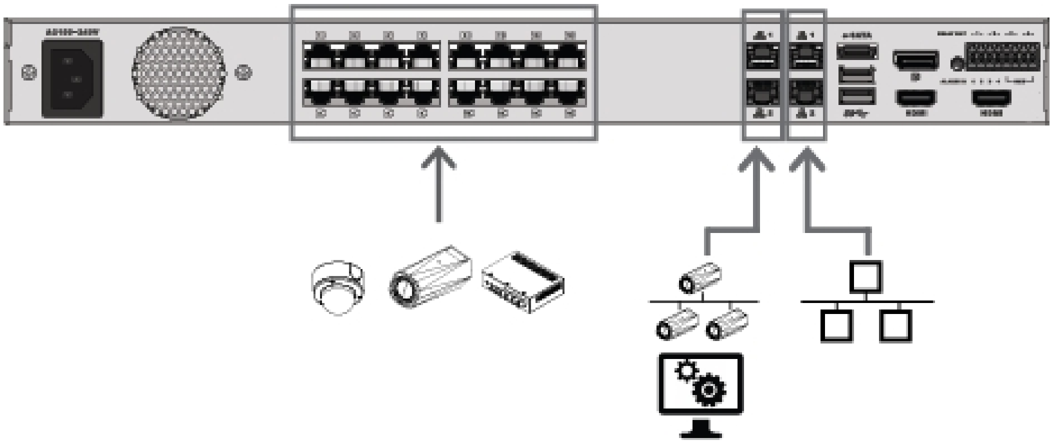


Figure 3: Example of external DHCP network connections on a 16 port HD Video Appliance.

1. Connect a network cable from the router or switch to one of thecamera network uplink ports on the back of the appliance, identified by the 🖧 icon.
2. Connect Avigilon cameras to the numbered ports.
3. If you would like to access the corporate network through the HD 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 software. See *Configuring the Avigilon Control Center™ Software* on page 15.

Connecting to Cameras with Static IP Addresses

If you plan to connect cameras with assigned static IP addresses to the HD Video Appliance, you must change the IP address of the teamed NIC to an IP address in the same subnet as the cameras. For information about identifying the teamed NIC, see *HD Video Appliance Networking* on page 5.

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

     Or

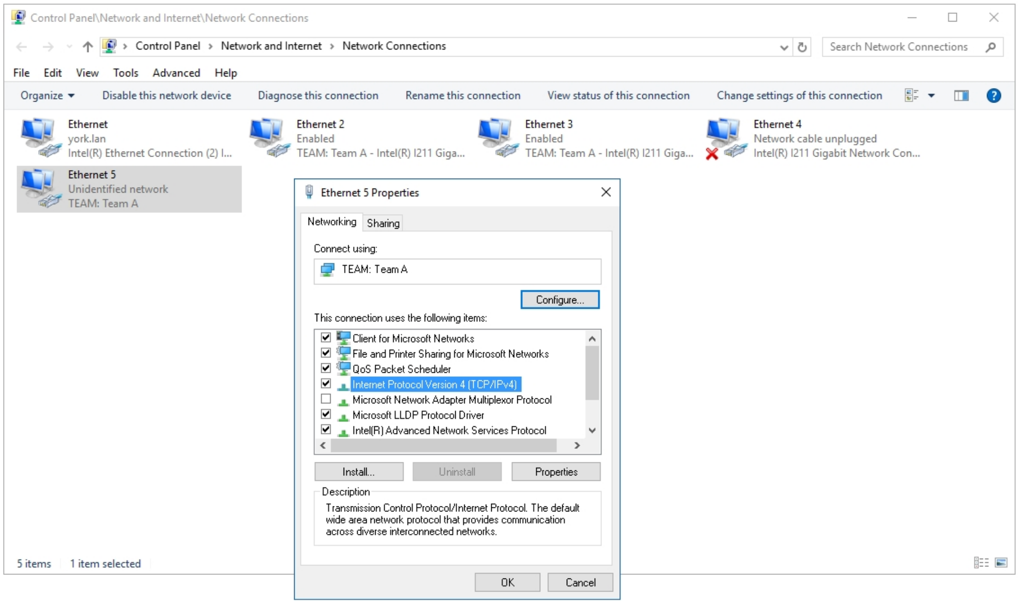
   - From the taskbar, search for `ncpa.cpl`

3. In the Network Connections window, right-click the Ethernet 5 network connection. and select **Properties**.

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

   Important: If Ethernet 5 is not set to TEAM: A or does not appear, contact Technical Support.

4. In the Properties dialog box for the teamed NIC (Ethernet 5), double-click **Internet Protocol Version 4 (TCP/IPv4)**.


Control Panel\Network and Internet\Network Connections
Control Panel › Network and Internet › Network Connections
Search Network Connections
File
Edit
View
Tools
Advanced
Help
Organize
Disable this network device
Diagnose this connection
Rename this connection
View status of this connection
Change settings of this connection
5 items
1 item selected
Ethernet 5 Properties
Networking
Sharing
Configure...
Install...
Uninstall
Properties
OK
Cancel

Ethernet
york.lan
Intel(R) Ethernet Connection (2) I...

Ethernet 2
Enabled
TEAM: Team A - Intel(R) I211 Giga...

Ethernet 3
Enabled
TEAM: Team A - Intel(R) I211 Giga...

Ethernet 4
Network cable unplugged
Intel(R) I211 Gigabit Network Con...

Ethernet 5
Unidentified network
TEAM: Team A

Connect using:
TEAM: Team A

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Intel(R) Advanced Network Services Protocol

Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Figure 4: The Network Connections window showing the Properties dialog box for the teamed NIC. (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.

6. If you would like to access the internet through the HD 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.

Configuring the Internal DHCP Server

If you plan to connect other network devices to the HD Video Appliance, you may need to set up the appliance to be a DHCP server. Some network devices rely on a DHCP server to receive an IP address before theycan work.

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 7.

1. Connect a monitor, keyboard and mouse to the appliance. Alternatively, you can a 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:
   - Select **Start** > **Settings** > **Network & Internet** > **Change adapter options**

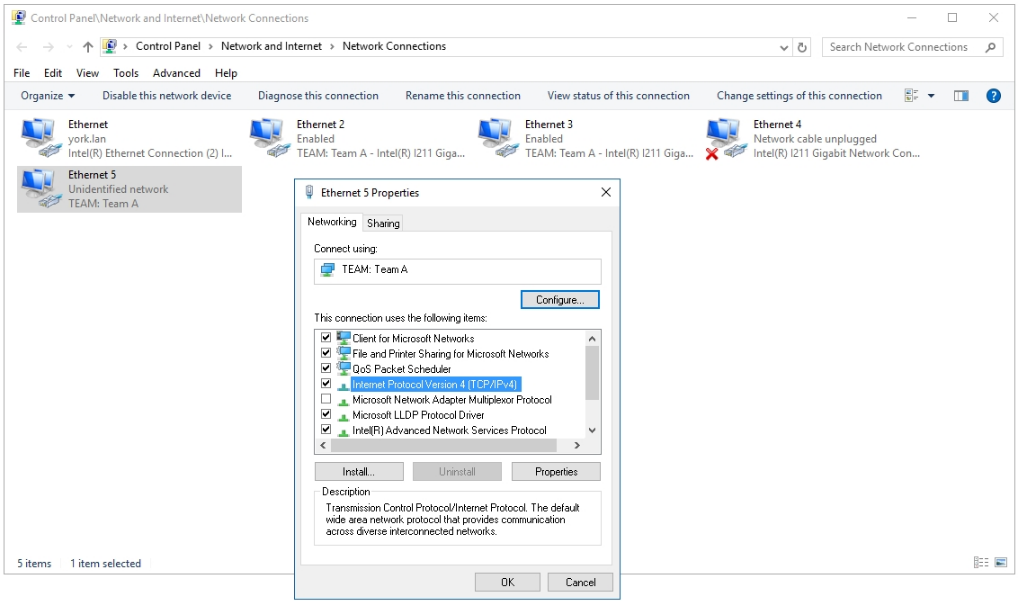
     Or

   - From the taskbar, search for `ncpa.cpl`
3. In the Network Connections window, right-click the Ethernet 5 network connection and select **Properties**.

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

   Important: If Ethernet 5 is not set to TEAM: A or does not appear, contact Technical Support.

4. In the Ethernet 5 Properties dialog box, double-click **Internet Protocol Version 4 (TCP/IPv4)**.



Control Panel\Network and Internet\Network Connections
Control Panel > Network and Internet > Network Connections
Search Network Connections
File Edit View Tools Advanced Help
Organize
Disable this network device
Diagnose this connection
Rename this connection
View status of this connection
Change settings of this connection
Networking
Sharing
Configure...
Install...
Uninstall
Properties
OK
Cancel
5 items
1 item selected

Ethernet
york.lan
Intel(R) Ethernet Connection (2) I...

Ethernet 2
Enabled
TEAM: Team A - Intel(R) I211 Giga...

Ethernet 3
Enabled
TEAM: Team A - Intel(R) I211 Giga...

Ethernet 4
Network cable unplugged
Intel(R) I211 Gigabit Network Con...

Ethernet 5
Unidentified network
TEAM: Team A

Ethernet 5 Properties

Connect using:
TEAM: Team A

This connection uses the following items:

☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol Version 4 (TCP/IPv4)
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver
☑ Intel(R) Advanced Network Services Protocol

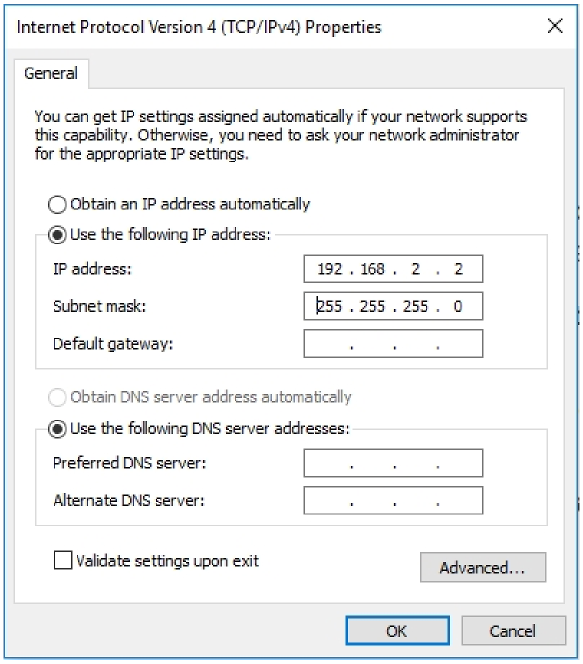
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Figure 5: The Control Panel Network and Internet Network Connections window showing the Ethernet 5 Properties dialog box. (Used with permission from Microsoft.)

5. In the dialog box that appears select the **Use the following IP address:** option and assign a static IP address for the appliance so that it can connect to the switch component.

   By default, the appliance is not connected to the switch component. The appliance must be connected to the switch component before you can configure the system to be a DHCP server.

   The default IP address of the switch component is 192.168.2.1. *Do not* assign this address for the appliance. You can use 192.168.2.**2** or higher. It is recommended that you only change the last digit.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Figure 6: The Internet Protocol Properties dialog box. (Used with permission from Microsoft.)

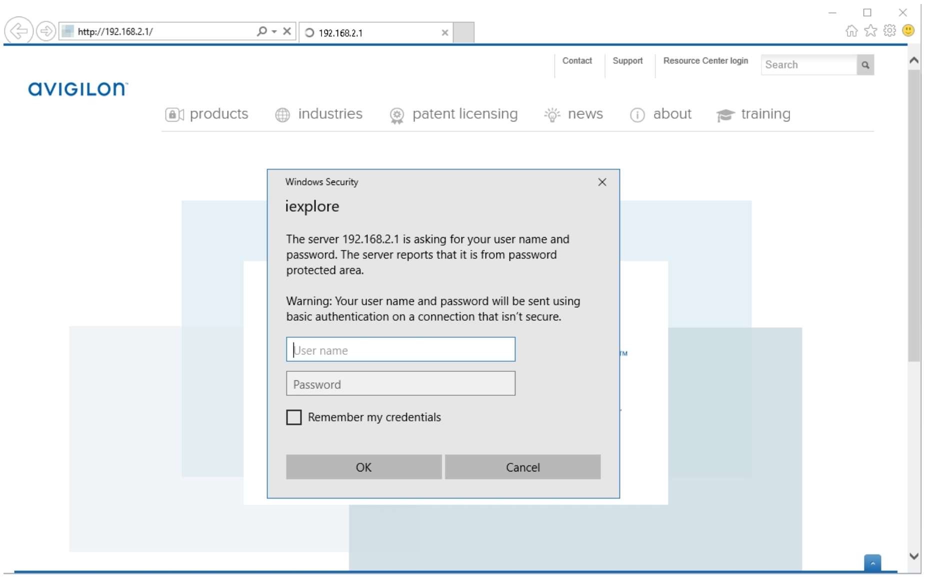
a. In the **Use the following IP address** field, enter `192.168.2.2` or the IP address you prefer.

b. In the **Subnet mask** field, enter `255.255.255.0` if it is not automatically entered.

c. Click **OK** to save your changes.

6. Open the Switch Management Console.

   a. In a web browser, enter `192.168.2.1` into the address bar.



Windows Security

iexplore

The server 192.168.2.1 is asking for your user name and password. The server reports that it is from password protected area.

Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.

User name

Password

□ Remember my credentials

Figure 7: The Switch Management Console Log In screen. (Used with permission from Microsoft.)

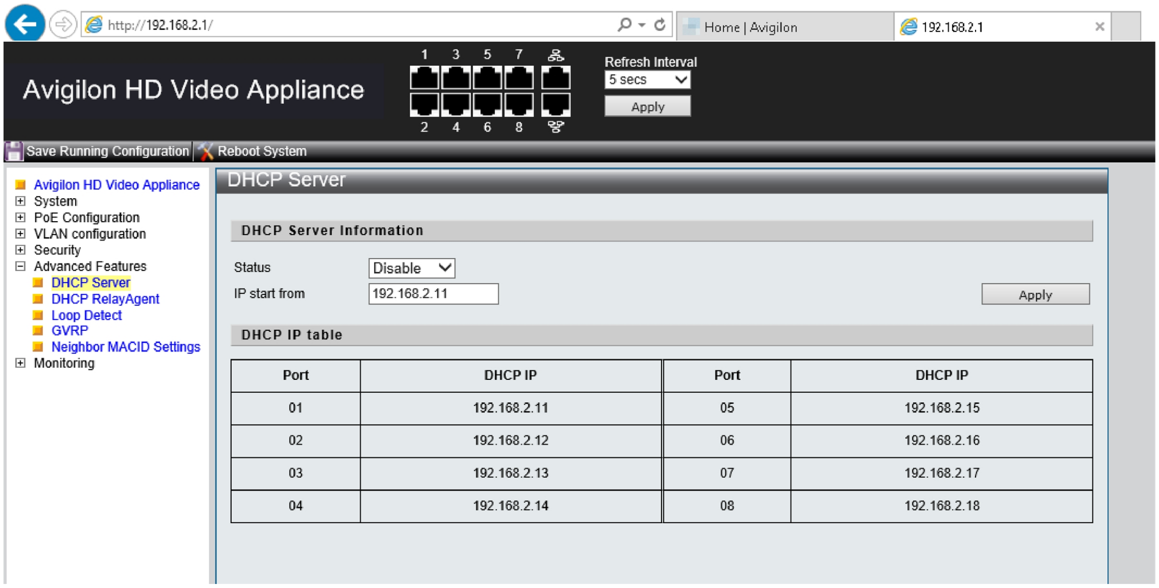
   b. When the log in screen appears, enter the default ID and password:

      - **ID:** user
      - **Password:** Avigilon

   c. Click **OK**.

7. Once you are logged in, expand **Advanced Features** and click **DHCP Server Settings** from the left menu pane.

8. In the Server State setting area, select **Enable,** click **Apply**, then **Save Running Configuration**.



- Avigilon HD Video Appliance
- System
- PoE Configuration
- VLAN configuration
- Security
- Advanced Features
  - DHCP Server
  - DHCP RelayAgent
  - Loop Detect
  - GVRP
  - Neighbor MACID Settings
- Monitoring

DHCP Server

DHCP Server Information

Status: Disable

IP start from: 192.168.2.11

Apply

DHCP IP table

Port	DHCP IP	Port	DHCP IP
01	192.168.2.11	05	192.168.2.15
02	192.168.2.12	06	192.168.2.16
03	192.168.2.13	07	192.168.2.17
04	192.168.2.14	08	192.168.2.18

Figure 8: The DHCP Server Settings page.

The appliance is now set to act as a DHCP server.

As you add cameras and network devices, the IP address for each item will be listed beside the connected port number.

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

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

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

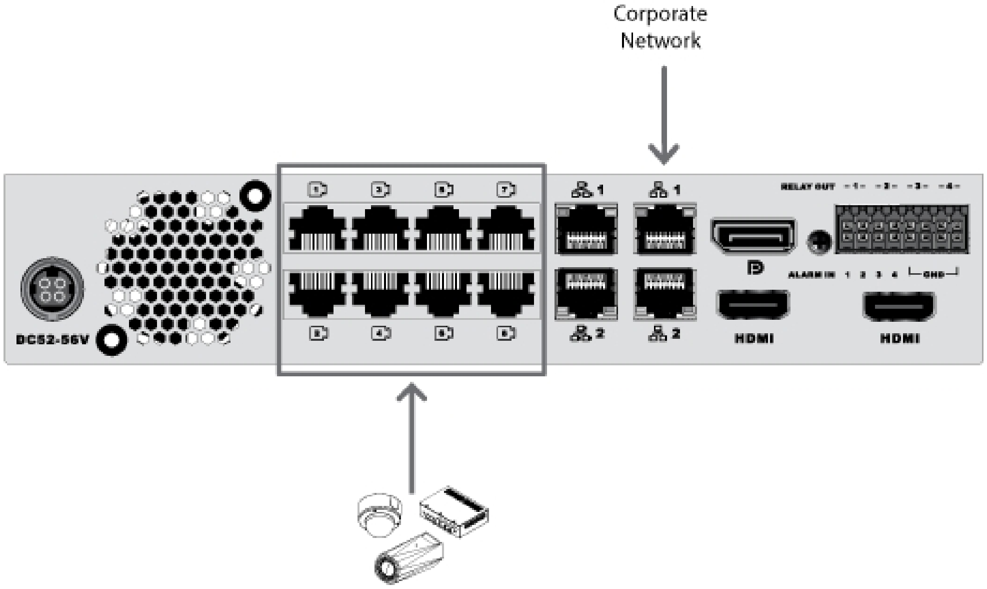


Figure 9: Example cable connections on an 8 port HD Video Appliance.

10. If you would like to access the internet through the HD 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 Avigilon Control Center™ Software* on page 15.

Configuring the Avigilon Control Center™ Software

After you set up and license the HD Video Appliance, it is recommended that you complete the following steps to configure the ACC software.

For more information about any of the following procedures, see the help files provided with the Avigilon Control Center Client software.

Starting Up and Shutting Down the Avigilon Control Center Client Software

After you install the ACC Client software, start the application and access the HD Video Appliance.

Starting Up the 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.

Once the application has started, it will automatically display a list of all the sites that are connected to the same network. You will be prompted to log in to all sites.

Shutting Down the Client Software

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

Logging Into and Out of a Site

After you start the ACC Client software, you are immediately asked to log in to a site. By default, the HD Video Appliance is automatically added to the system as a server within a site of the same name.

The default username is *administrator* with no 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**.

   You are logged into 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 Client, select ⚙ > **Log Out**. 2. In the confirmation dialog box, click **Yes**.

Changing the Administrator Password

After you log in to the ACC software for the first time, it is recommended that you change the default administrator password.

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**.

Tip: If you forget the default 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 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 HD 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. 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.

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

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:

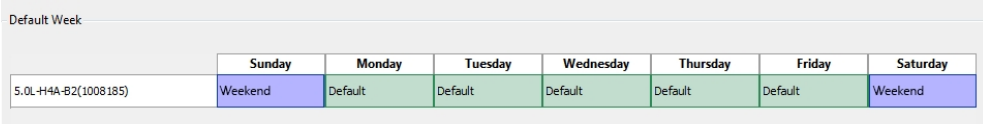
   - **Continuous** — record video constantly.
   - **Motion** — only record video when motion is detected.
   - **Digital Inputs** — only record video when a digital input is activated.
   - **Alarms** — only record video when an alarm is activated.
5. To disable recording in parts of the template, click 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.



Default Week

	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
5.0L-H4A-B2(1008185)	Weekend	Default	Default	Default	Default	Default	Weekend

Figure 10: The Recording Schedule dialog box: Default Week

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 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.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.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 amortized data rate. Since the system can only provide an estimate of the data rate for the full retention period, the actual retention time can vary from the Max. Record Time setting by up to 30 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. 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. Click **Edit Groups** to enable the Dual Authorization feature.

   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, select the groups that can grant authorization to users in this group.
   b. To disable the feature, click the toggle at the top of the dialog box.
   c. 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 Avigilon Control Center 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 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 use the Avigilon Professional Joystick Keyboard with the Avigilon Control 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 HD Video 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.
1 2 3 4	Green	Camera is using the switch for a network connection and Power over Ethernet (PoE) power.
	Orange	Camera is only using the switch for a network connection.
	Orange - slow blinking	Port off due to failure.
	Alternating Green - Orange	Port off due to system over power budget.
🖧 🖧	Orange	GigE network link is present.
	Green	10/100 network link is present.
⚡	Orange	Switch component has reached its PoE output capability.

Back Panel LEDs

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

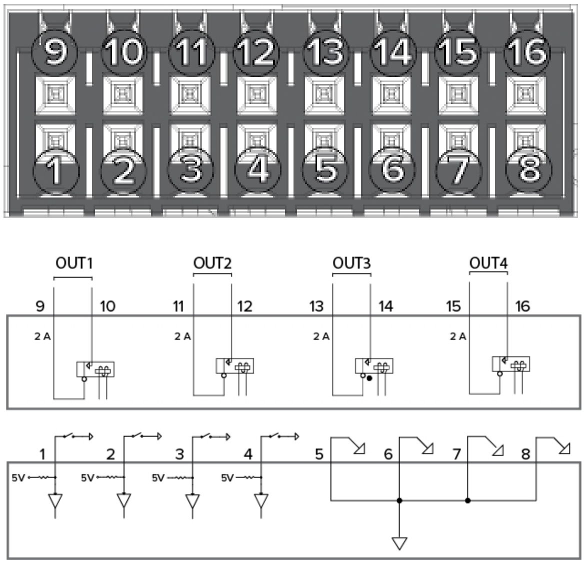
Icons	LED Status	Description

1 2 3 4
1 2 3 4
5 6 7 8
	Green	Network activity is present.

	Orange	On for 100M speed. Off for 10M speed.

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:



Pin	Function	Description
9	OUT1	Relay Outputs — Form-A dry contact outputs. When active, terminals are connected. Terminals are open when inactive. Maximum load is 30 V, 2 A.
10		
11	OUT2	
12		
13	OUT3	
14		
15	OUT4	
16		
1	IN1	Alarm In — 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		

Restarting the Operating System

If the operating system ever freezes or displays a fatal system error, you can restart the operating system by using the reset switch on the front of the appliance.

NOTE: When you use the reset switch, the appliance must be powered.

The operating system reset will not affect the switch component or the connected cameras.

- On the 8 port model, the reset switch is located at the front of the appliance and is the small unlabeled hole between the USB ports and the status LEDs.
- On the 16 and 24 port models, the reset switch is located at the front of the appliance and is the small unlabeled hole between the 🎧 jack and the ⏻ status LED.

After you've found 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.

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

2. Do not release the reset switch until the monitor connected to the appliance turns off, or the 🖴 **Hard Drive Status** LED stops blinking.

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

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/**.