avigilon™
a Motorola Solutions Company

User Guide

Avigilon ACC™ ES Analytics Appliance

VMA-RPA-4P2 and VMA-RPA-4P4

(Firmware releases 3.2 and later)

Avigilon Corporation
avigilon.com

PDF-4PortAnalytics-A

Revision: 5 - EN

20181217

This device is provided with a battery powered real-time clock circuit. There is a danger of explosion if battery is incorrectly replaced. Replace only with same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.

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

Table of Contents

Introduction

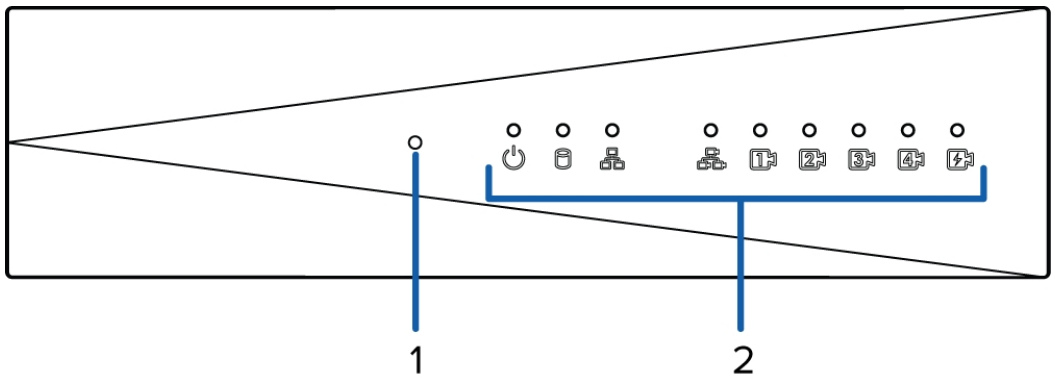
The Avigilon ACC ES Analytics Appliance is an all-in-one solution for network video recording plus server side video analytics. The appliance features:

- A network switch to connect and power IP cameras.
- Built-in server to run the Avigilon Control Center Server Software.
- Video analytics engine to enable connected cameras to detect classified objects.

This guide describes how to configure the system after the appliance has been powered and is connected the local area network.

Overview

Front View



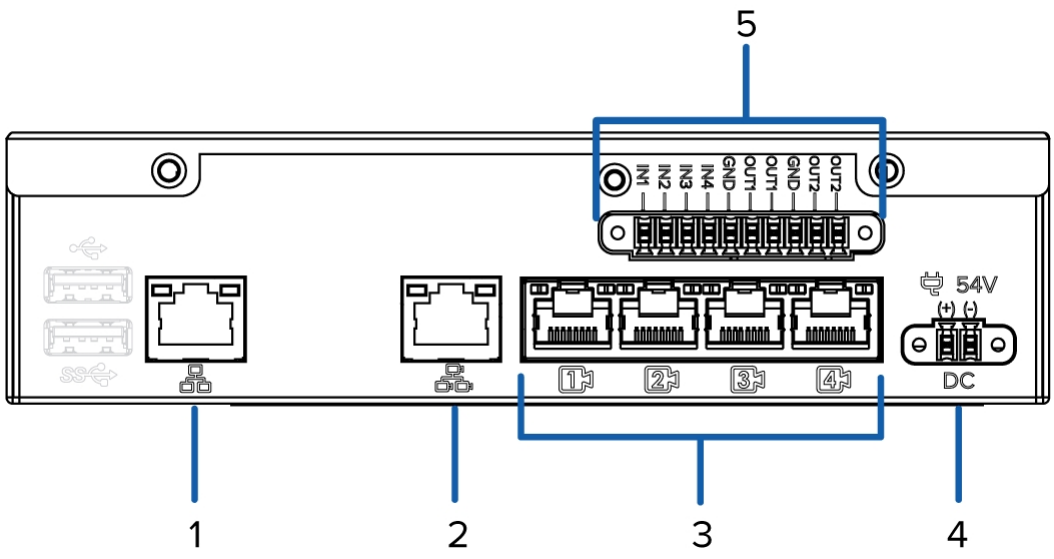
1. **Reset button**

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

2. **Status LED**

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

Rear View



1. **Corporate network uplink port**

   Accepts a 1GbE Ethernet connection to the general network to allow users access to the web interface and connected camera video.

2. **Camera network uplink port**

   Accepts a 1GbE Ethernet connection to the cameras that are connected to the PoE switch component. Can be used to link to other PoE switches and cameras.

3. **PoE switch component**

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

4. **Power connector**

   Accepts power to the appliance.

5. **I/O connector**

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

System Requirements

Camera Frame Rate

The ACC ES Analytics Appliance can provide analytics for non-analytics cameras. For optimal analytics performance, the source camera should stream a minimum of 10 images per second (ips).

Web Browser

Administrative settings for the appliance are managed through a web interface, accessed from any Windows, Mac or mobile device using any of the following web browsers:

- Mozilla Firefox® browser version 3.6 or later
- Google Chrome browser 8.0 or later
- Microsoft Edge browser 25 or later
- Safari 5.0 or later
- Chrome on Android 2.2 or later
- Safari on Apple iOS 5 or later.
- Windows Internet Explorer browser version 7.0 or later

NOTE: Your web browser must be configured to accept cookies or the web interface will not function correctly.

Supported Network Configurations

NOTE: Camera Uplink Port does not support dynamically switching DHCP servers.

Network Connections	Camera Web Interface Access	Supported IP Configurations		Notes
		Corporate LAN Uplink	Camera LAN Uplink	
Corporate LAN Uplink only	No	Static or DHCP assigned	Unconnected (leave as DHCP)	Camera LAN Uplink and connected cameras will use Zeroconf IP addresses.
Camera LAN Uplink only	Yes	Unconnected (leave as DHCP)	Static, DHCP-assigned, DHCP-Zeroconf	
Corporate and Camera LAN Uplink	via Camera LAN Uplink only	Static, DHCP-assigned, DHCP-Zeroconf	Static, DHCP-assigned, DHCP-Zeroconf	Corporate and Camera LAN Uplinks must be on different subnets.

Hardware Installation

Complete the recommended procedure for installing the device:

1. Connect power and wait for the device to start up.

   Do not connect any other cables until instructed in this procedure.

   The  status LED turns green to indicate that the device is turned on.

2. Connect an Ethernet cable directly from a DHCP enabled port on your configuring laptop to the *camera network* port on the device.
3. Open a web browser on the connected laptop and enter this IP address: `https://169.254.100.100`.
4. When you are prompted by the Web Interface, enter a new password for the administrator username.

   The Strength meter measures the complexity of your password: Red is too simple, yellow is reasonably complex, and green is complex. Complexity measures the difficulty to discover your password, not how secure your password is. A complex password is recommended.

   The page refreshes and you are prompted to log in.

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

   The Web Interface launch page is displayed.

6. In the navigation sidebar, expand ACC and click **Server** to open the ACC Server panel.
7. In the General pane, click the Client Installer Download button to download and install a copy of the Avigilon Control Center (ACC) Client software to the connected laptop.
8. Set the language for the Web Interface, and a user-friendly hostname and the time zone. In the navigation sidebar, click **Device** to open the Device panel . In the:
   a. General pane, select the Language from the drop-down.
   b. Hostname pane, optionally replace the serial number of the appliance with a descriptive hostname for the appliance.
   c. Time pane, specify the Time Zone and identify the time source in the NTP drop-down and Servers list.

   For more information see *Device Panel* on page 11.

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

   For more information, see *Network Panel* on page 12.

10. Connect an Ethernet cable from the device to the corporate network.
11. Disconnect the configuring laptop from the device.
12. If required, mount the device on a wall using the supplied mounting brackets.

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

a. Attach the wall mount brackets to the lowest threaded holes on the sides of the device.
b. Position the device with the rear panel facing downwards.
c. Screw the wall mounting brackets to the wall.

13. Connect the cameras to the PoE switch component.

    NOTE: Allow the device 1 to 2 minutes to budget power to all connected devices. The front camera status LEDs initially show that PoE is provided to all connected devices, but the status may change if the system detects that the total power consumption exceeds the PoE limits.

14. If required, connect other switches and cameras to the camera network.

Now, you can configure the device and cameras for daily operation through the Avigilon Control Center Client software. For more information, see *Configuring the ACC Software* on page 19.

Starting the ACC ES Analytics Appliance for the First Time

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

1. Connect a port on the appliance to the local network with an Ethernet cable.
2. Press the power button on the front of the appliance and wait for the appliance to start up.
3. On a network workstation, discover the appliance. Use File Explorer on a Windows computer or Finder® on a Macintosh computer.
4. Click past any connection messages displayed by the browser. You will see two warning messages that differ slightly depending on the browser. If the browser is:
   - Chrome—Click **Advanced** on the first screen and **Proceed to <*IP address*> (unsafe)** on the second screen.
   - Firefox—Click **Advanced** on the first screen and on the second screen click **Add Exception**, check **Permanently store this exception**, and click **Confirm Security Exception**.
5. When you are prompted by the Web Interface, enter a new password for the administrator username.

   The Strength meter measures the complexity of your password: Red is too simple, yellow is reasonably complex, and green is complex. Complexity measures the difficulty to discover your password, not how secure your password is. A complex password is recommended.

   The page refreshes and you are prompted to log in.
6. Enter `administrator` as the username and your new password.

   The Dashboard panel of the Web Interface is displayed.
7. Set the language for the Web Interface, and a user-friendly hostname and the time zone. In the navigation sidebar, click **Device** to open the Device panel . In the:
   a. General pane, select the Language from the drop-down.
   b. Hostname pane, optionally replace the serial number of the appliance with a descriptive hostname for the appliance.
   c. Time pane, specify the Time Zone and identify the time source in the NTP drop-down and Servers list.

   For more information see *Device Panel* on page 11.
8. Select how the appliance obtains IP addresses from the network. On the navigation sidebar, click **Network** to open the Network panel. For each network port used, select Automatic or manually enter the settings.

   For more information, see *Network Panel* on page 12.

For more information about the Web Interface, see *Configuring the Appliance* on page 8

Troubleshooting Installation—Cannot Discover the Device

If you cannot discover the device using File Explorer (Windows) or Finder (Macintosh) during the hardware installation and it is connected to your network, try the following:

- Access the appliance from your web browser using the URL https://VMA-RPA-4Px-<serial number>
- Use the Address Resolution Protocol (ARP) to determine the IP address for the device:
    1. Locate and copy down the MAC Address (MAC) listed on the Serial Number Tag for reference.
    2. Open a Command Prompt window and enter the following command:

       `arp -a`

    3. Scroll through the response and look for the IP address corresponding to the MAC address.
- Discover the DHCP-assigned IP address from the ACC Client software:
    1. Download and install the ACC Client software on to the configuration laptop.

       The ACC Client software can be downloaded from the Avigilon website: **avigilon.com**.

    2. Launch the ACC Client software.
    3. Log into the site that uses this naming convention: VMA-RPA-4Px-<serial number>.

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

       NOTE: The username and password for the Web Interface application is separate from the administrator username and password for the ACC Client. To change the password for the ACC application, see *Changing the Site Administrator Password* on page 20.

    4. Display the server Setup tab.

       At the top of the window, the appliance IP address is displayed.

    5. Open a web browser and enter the IP address in this format: `https://<IP address>`.
    6. Continue the remaining steps for installing the appliance.

Troubleshooting Installation—Networking

By default, the ACC ES Analytics Appliance acquires an IP address on the network through DHCP. If you need to set up the ACC ES Analytics Applianceto use a static IP address or any specific network configuration, see the *Windows Help and Support* files for more information.

Configuring the Appliance

The ACC ES Analytics Appliance can be configured through a Web Interface that is accessible from any browser on the network. The Web Interface allows you to configure the ACC ES Analytics Appliance server settings, set how the server keeps time, and allows you to remotely restart or upgrade the server. It also allows you to download the ACC Client software to the workstation you are using to access the Web Interface. Throughout this section, the term device is used to identify the ACC ES Analytics Appliance.

Accessing the Web Interface

1. Access the Web Interface sign in page, using either of the following methods:
    - **Discovering the Device**
        1. Use File Explorer on a Windows computer or Finder on a Macintosh computer.

           You are looking for a network device labeled “ACC ES Analytics Appliance” with the serial number appended.
        2. Right click and select **View Device Webpage** to open the device sign in page in your default web browser.
    - **Using the IP Address or Hostname**
        1. Open a web browser from a network workstation with network access to the device.
        2. Enter its IP address or hostname into the web browser to open the device sign in page:

           https://*<Device IP address >*|*<Device hostname>*/

           For example: `https://192.168.1.40/` or `https://my_AvigilonDevice/` , where `my_AvigilonDevice/` is the hostname configured in the Device panel.

           Tip: If you forgot the IP address or hostname that was configured during the installation process, the information is listed in the ACC Client software, in the server Setup tab.
2. To log in to and out of the Web Interface:
    a. To log in, enter the Web Interface username and password.

       The username is always `administrator`. Use the password you configured when you logged in to the device for the first time. For more information, see *Hardware Installation* on page 4.

       The Web Interface Dashboard is displayed in your web browser.

    b. To log out of the Web Interface, click the log out icon on the right side of the top banner.

Web Interface Launch Page

The Web Interface launch page consists of a Dashboard navigation bar and a set of panes displaying status information:

- **ACC Server**: Displays Running when the ACC Server software is operating; otherwise it displays Stopped. The panel provides technical information about the device: site name, server name, server ID, server version, software version, the number of available camera channels, and the maximum number of ACC client instances allowed.
- **System**: Displays Ready when the device is fully operational, and Rebooting then Initializing when the device is restarting. The panel provides technical information about your device: product name, part number, serial number, and firmware version.
- **Storage**: Displays the storage capacity of the device and the status of the storage disks.
- **Network**—Displays information about the two uplink ports on the device. Click ⚙ to open the **Network Panel**.
- **PoE**—Displays status information about each PoE port. Icons in the panel let you quickly see how many ports are in use, their status, speed and whether the link is up or down. Click ⚙ to open the **Device Panel**.

Use the menu options under Services and System in the Dashboard navigation bar to access all the other Web Interface panels.

- **Services**: Expand **ACC** in the left sidebar to navigate to the **Server** page to control the ACC Server on the device and the **Logs** page to view ACC Server service logs.
- **System**: Access the five options to configure the device and view its status.

Server Panel

On the **Server** panel use the:

- General pane:

To...	Do this...
Shut down all the services before you shut down the device.	Click **Stop**.
Start up all the services after they have been shut down.	Click **Start**.
Format the disk drives.	Click **Reinitialize** to delete all configuration and recorded video data.
Download and install the ACC Client software on the computer you are using to access the Web Interface.	Click **Download**. After the download is complete, open the installer as you would any application downloaded with a web browser to install the software.

- Network Storage Management pane:

  To allow users to archive video from this device using the ACC Client software:

  1. Click **Enabled**.
  2. From the Protocol drop down list, select one of the following:
     - **CIFS** — Common internet file system. The network path is typically in this format: //*<hostname or IP>* / *<path>*
     - **NFS** — Network file system. The network path is typically in this format: *<hostname or IP>* : *<path>*
  3. In the **Network Path** field, enter the path to the preferred video archiving location.
  4. If the network location requires authentication, select the Authentication check box then enter the credentials in the Username and Password fields.
  5. Click **Apply**.

- Service and RTP Ports panes

  To change the UDP and TCP ports used to communicate with the appliance:

  - In the Service Ports pane, enter the **Base** value to use for the HTTP, HTTPS, and UDP ports and click **Apply**. The list of ports is updated.
  - In the RTP Ports pane, enter the **Base** value to use for the UDP ports and click **Apply**. The range of ports available for RTP is updated.

  Important: These changes can only take effect after the system restarts. When you are prompted, allow the system to restart.

Logs Panel

Use the Logs page to view service logs. The logs are typically requested by Avigilon Technical Support to help resolve an issue.

By default, the page displays 100 warning messages from the logs.

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

1. In the drop down list, select the type of application log that you need. The options are:
    - **Exception Logs**
    - **FCP Logs**
    - **Server Logs**
    - **WebEndpoint Logs**
2. In the **Maximum Logs** drop down list, select the number of log messages you want to display each time.
3. Enter text in the **Filter** field to apply a filter to the log listings.
4. Click the **Sync** button to display the updated logs.

Device Panel

On the Device panel use the:

- **General** pane to:
    - **Reboot** the device from the Web Interface. You can monitor the progress of the device as it reboots from the *Web Interface Launch Page* on page 8.
    - Select a **Language** for the Web Interface from the drop down list.
- **Hostname** pane to enter a new **Hostname**. Click **Apply** to make the change.

  The default hostname is the same as the server name. The server name is in the form *<Model>-<Serial Number>*
- **Password** pane to change the administrator password:

  NOTE: You cannot change the default *administrator* username on the Web Interface, only the password.

  1. To change your password, confirm your identity by entering your current password in the **Old Password** field.
  2. Enter the new password in the **New Password** field.
  3. Re-enter the new password in the **Confirm Password:** field.
  4. Click **Apply** to save the new password.

  CAUTION — You will lose recorded video and configuration data if you forget your password. To reset the administrator password, you must reset the device to the factory default settings. This will also format the hard drives and delete the configuration data and recorded video. For more information on performing a factory restore, see *Restoring Factory Default Settings* on page 33.

- **Time** pane to customize how the device keeps time:
  - Select your **Time Zone** from the drop-down list. The time zone that you set here is used by the recording schedules defined in the ACC Client software.

    For more information, see *Setting the Recording Schedule* on page 23.
  - Select whether you want to keep synchronized time through a Network Time Protocol (NTP) server (recommended) in the NTP field.

    Select:
    - **DHCP** to automatically use the existing NTP servers in the network.
    - **Manual** to enter the address of NTP servers in the Servers list. Controls to add and delete addresses in the list, and reorder them are activated.
    - **Off** if you do not use an NTP server.

    NOTE: The default set of NTP servers is always present in the Servers list. The default list cannot be rearranged or deleted:
    - 0.pool.ntp.org
    - 1.pool.ntp.org
    - 2.pool.ntp.org
    - 3.pool.ntp.org

  Click **Apply** to save the time settings.
- **Upgrade Firmware** pane to install the latest version of the firmware on your device, or to reinstall the firmware if it becomes corrupted. For more information, see *Upgrading the Firmware* on page 32.

Network Panel

On the Network panel, you can change network connections of the device. Two network connections are supported: one for a corporate network and one for a camera network.

The corporate network is the network that typically provides users with access to the device. Users who monitor video through the ACC Client software would connect to the device through this network.

The camera network is a closed network that typically only contains cameras. This reduces the amount of interference with video recording.

NOTE: The Corporate Network and the Camera Network must be on different subnets.

For more information about the network connections, see *Supported Network Configurations* on page 3.

You can perform any of the following panes In each of the panes in the Network panel:

To...	Do this...
Set how the device obtains an IP address for each network.	Toggle Automatic on to discover connected networks automatically (the default setting), or off to manually specify the connections. Enter the appropriate values in the following fields if you are manually entering the connection settings:

To...	Do this...
	In each of the panes in the Network panel, toggle **Automatic** on to discover connected networks automatically (the default setting), or off to manually specify the connections. Enter the appropriate values in the following fields if you are manually entering the connection settings: • **IP Address** • **Subnet Mask** • **Default Gateway** Click **Apply** to save your changes.
Set how the device obtains a named address from a DNS server.	Toggle Automatic on to discover connected DNS servers automatically (the default setting), or off to manually specify the DNS servers. Controls to add and delete addresses in the list, and reorder them are activated.

Budgeting PoE Power

The PoE switch component in a 4-port device can output a total of 64 W of power to the connected devices, and on an 8-port device can output a total of 128 W. Each PoE port is capable of outputting 16 W to standard PoE devices, and 30 W to PoE+ devices. This typically means that a 4-port device can support up to 4 standard PoE devices or up to 2 PoE+ devices, and an 8-port device can support 8 standard PoE devices or up to 4 PoE+ devices.

Advanced users can manually adjust the PoE power budget for each port to consistently accommodate the cameras needed.

If you choose to manually adjust the PoE budget at each port, be aware that you must also account for potential power loss in the cable. Unless the amount of power loss in the cable is known, use the following estimates:

- If the device uses less than or equal to (<=) 16 W — expect 2.5 W of power loss.
- If the device uses more than (>) 16 W — expect 4.5 W of power loss.

To calculate the recommended power budget for each port, use the following equation:

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

Example: Connect the following 4 cameras to a 4-port device:

2 x HD dome cameras	(9 W +2.5 W) x 2	= 23 W
1 x HD PTZ camera	25.5 W + 4.5 W	= 30 W
1 x HD micro dome	4 W + 2.5 W	= 6.5 W
	Total	= 59.5 W

The total power consumption of the 4 cameras is within the PoE switch component limits.

NOTE: If you miscalculate the required power for a PoE port, the connected camera may be shut down if total power output exceeds 64 W.

Assigning a PoE Power Budget

On the PoE page, you can see how much power is available to, and being used by, connected devices. The default setting for all ports is Auto. This setting automatically detects and budgets the amount of power required by the device connected to the port. For each port you can adjust this setting manually, or turn off power output completely. If you want to manually adjust the power output of the ports you must calculate a PoE power budget, see *Budgeting PoE Power* on the previous page.

Click **PoE** from the Dashboard navigation bar to open the PoE page.

The Budget bar indicates the total amount of power budgeted for all devices connected to the PoE ports. The Consumption bar indicates the actual amount of power currently used by all the connected devices.

Use the Powered bar for each port to configure a PoE power budget for each port:

- Click **Off** to disable power output to the port. When power to a port is disabled, the port no longer outputs power but can act as a standard network connection for any device.

  Tip: You can also use this feature to remotely power cycle the camera. After you set the Powered setting to Off, wait for the camera to power off then change the Powered setting to **Auto** or **Manual** .

- Click **Auto** to automatically output power to the connected device depending on its mode of operation.
- Click **Manual** to enter a power budget value in watts. Make sure the budget includes potential power loss at the cable.

  Tip: Devices that support both PoE and PoE+ (802.3at) modes of operation can be forced into non-PoE+ mode (802.3af) by using a manual 16W budget.

Settings are not implemented until you click **Apply**.

After you click **Apply**, allow the system to reboot when the following message is displayed:

Applying changes may power-cycle PoE-powered devices.

The Web Interface automatically refreshes the screen and displays the updated settings after the new power settings are applied.

PoE Status

The PoE panel displays a status for each port in the Status column. Statuses include the following:

Green	Powered	A PoE device is connected to the port and is operating normally.
	High powered	PoE+ is turned on.
Gray	Disconnected	There is no device connected to the port.
	Unpowered	The PoE port power is switched off from the PoE page in the Web Interface
Yellow	Overloaded	A PoE device is connected to the port but is not receiving power. This status typically occurs when one port is overcurrent, or the device is requesting more power than budgeted, etc.

	Low current	The device is getting low current from the port.
Red	Error	The device is in an error state.

Tip: If a camera is disconnected then reconnected to the device, you may need to refresh this page to view the latest status and budget values.

System Logs Panel

Use the System Logs page to view the device logs. The logs are typically requested by Avigilon Technical Support to help resolve an issue.

By default, the page displays 100 warning messages from the Logs.

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

1. In the drop down list, select the type of application log that you need. The options are:
    - System Logs
    - Boot Logs
    - Web Server Logs
2. In the **Maximum Logs** drop down list, select the number of log messages you want to display each time.
3. Enter text in the **Filter** field to apply a filter to the log listings.
4. Use **Filter** to apply filter to the logs.
5. Click the **Sync** button to display the updated logs.

Installing and Starting the Avigilon Control Center ™ Client

To install the ACC Client software:

1. Open a web browser from a network workstation with network access to the Internet.
2. Download the ACC Client software from the Avigilon website: **avigilon.com**.
3. Install the ACC Client software on a network workstation with network access to the device

Complete the following procedures to start, log in to, and log out of the ACC Client software .

Starting Up and Shutting Down the ACC Client Software

After you install the ACC Client software, start the application and log in to the ACC ES Analytics Appliance.

The ACC Client software should start automatically when your Windows workstation starts. Refer to the following steps if it doesn't.

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.

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 first time you log in to a newly installed site, you activate the ACC 6 software license provided with your device. See *Activating the Avigilon Control Center™ License* on page 19.

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 In to 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 ACC ES Analytics Appliance appears as a site with the same name as the hostname.

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.

   Or, select the **Use current Windows credentials** check box to automatically use the same username and password as your computer.

   NOTE: If you are unable to login using your current Windows credentials, your system may be using Kerberos as a network authentication protocol. Contact your network administrator for help.

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 Client, select > **Log Out**. 2. In the confirmation dialog box, click **Yes**.

Configuring the ACC Software

Complete the following procedures in the ACC client to configure the ACC software on the 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.

Activating the Avigilon Control Center™ License

Downgrading to the ACC 5 Software:

The ACC 6 software is pre-installed on the ACC ES Analytics Appliance.

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 ACC 5 Software* on the next page.

Before you can configure cameras and monitor live or recorded video, you will need to activate the ACC 6 software license provided with your device. If you don't have a license, you will need to purchase 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 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 licensed features.

1. In the top-left corner, click  to open the New Task menu, then click  .
2. In the site Setup tab, click  .
3. In the License Management dialog box, click **Add License...**.
4. 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 on a private intranet, select the **Manual** tab. Go to *Manual License Activation* below.

Automatic License Activation

In the **Automatic** tab:

1. In the Enter Product Keys section, enter the license key.
2. In the Activate and License Site section, click **Activate now**.

Manual License Activation

In the **Manual** tab:

1. In the **Enter Product Keys** section, enter the license key.
2. In Generate Activation File section, click **Save File...**.
3. In the Save As window, select 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.

Open a web browser and go to **http://activate.avigilon.com**.

1. Click **Choose File** and select the `.key` file, click **Upload**. The generated license file (`.lic`) will download automatically. If it does not, allow the download to occur when you are prompted.
2. Copy the downloaded `.lic` file to a location that would be accessible to the ACC Client software.
3. Complete the product registration page to receive product updates from Avigilon, then click **Register**.

Return to the ACC Client:

1. In the Apply License File section, click **Apply...**.
2. Locate the downloaded `.lic` file and click **Open**.
3. In the Confirm Licenses dialog box, click **OK**.

Modifying Licenses

You can use the the License Management dialog box to add, remove, deactivate, and reactivate licenses for the ACC 6 software. For more information, see the *Avigilon Control Center Client User Guide*.

Downgrading to the ACC 5 Software

1. Open Windows **Settings** > **Apps** > **Features** and uninstall the ACC 6 software.
2. In Windows explorer, open the **D:** drive and delete the following directories:

   ```
   D:\AvigilonConfig
   D:\AvigilonData
   ```

3. In Windows Explorer, go 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, see the *Avigilon Control Center Server User Guide* for the ACC 5 software, available on **http://avigilon.com**.

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.

Accessing the Setup Tab

The Setup tab is where you configure your system.

In the Setup tab, the System Explorer is displayed on the left and the settings are displayed on the right. The Setup options change depending on the site, server, or device that is selected in the System Explorer.

To open the Setup tab, do one of the following:

- At the top-left corner of the application window, click ☰ to open the New Task menu and then click ⚙ **Site Setup**.
- In the System Explorer, right-click the site or device you want to configure and then click **Setup**.

  NOTE: Server settings are only available after the site or device Setup tab is open. In the System Explorer, select the server you want to configure.

Connecting Cameras to the Avigilon Control Center Software

After all the cameras in your system have been physically connected to the ACC ES Analytics 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** (wireless access network).
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**.

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.

NOTE: Be aware that the system recording schedules use the that is set on the appliance. For more information about setting the timezone on the appliance in the Web Interface, see *Device Panel* on page 11.

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.
   - **POS Transactions** — only record video when a point of sale (POS) transaction is made.
   - **License Plates** — only record video when a license plate is detected.
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.

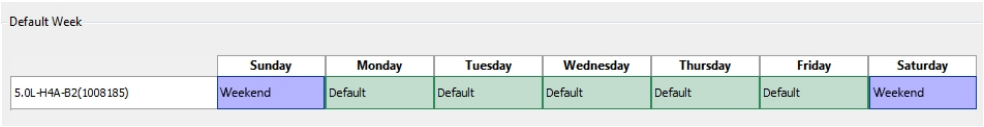


Figure 1: The Recording Schedule dialog box: Default Week

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.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.

        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.

Enabling Server Analytics

You can enable the system to detect classified objects using self-learning video analytics on any non-analytics camera connected to the appliance.

Be aware that there is a limit to the system's analytic capacity. Refer to the Total Analytic Load bar to avoid exceeding the system's analytic capacity.

NOTE: This appliance does not currently support unusual motion detection.

1. In the server Setup tab, click  .
2. In the following dialog box, a list of connected cameras are displayed.

   Only cameras without the Classified Object video analytics mode enabled are displayed.

   If you do not have access rights for a camera, it will not be shown in this list.
3. To enable Classified Object video analytics, select the check box beside the connected camera. If you have an Avigilon Artificial Intelligence (AI) Appliance, enabling video analytics also enables the Avigilon Appearance Search feature.

   The Total Analytic Load bar displays the appliance's video analytics capacity. The percentage is based on the enabled camera's current Compression and Image Rate settings. You cannot exceed a Total Analytic Load of 100%.
4. Click **OK**.

   Your settings are now saved.

Advanced Settings

The following list include some advanced settings that you can use to further customize your system. See the application Help files for details about how to configure these settings.

- Adjust camera settings
  - 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.

    NOTE: For optimal analytics performance, the source camera should stream a minimum of 10 images per second (ips).
  - To reduce the amount of ambient motion detection for a specific camera, you can adjust the

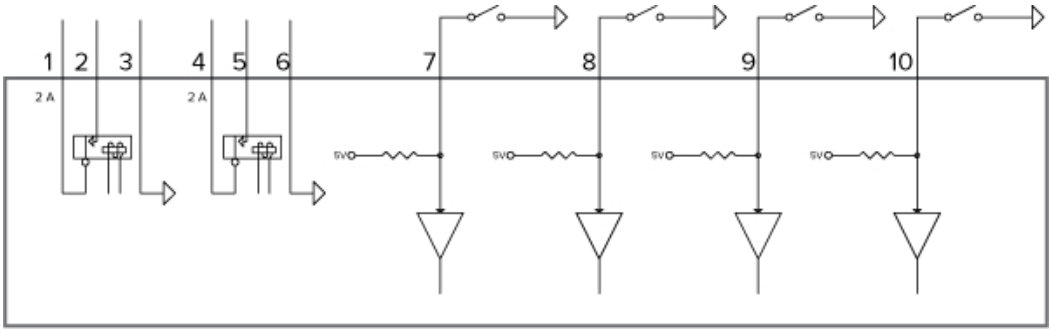
Motion Detection settings.

    - 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.

- Classified object detection
    - Available to cameras that have server-side analytics enabled, and available to other Avigilon video analytics cameras.
    - Use the Analytic Events dialog box to configure classified object motion detection. Once configured, you can receive events, trigger alarms, define rules, and record video when specific object motion requires your attention.
- Alarms
    - Use the Alarms dialog box to create and manage alarms. Once an alarm has been created, you can monitor alarm events in the Alarms tab and in the Avigilon Control Center Mobile App.
- Configure digital inputs and outputs
    - The digital I/O connector on the appliance can be configured as an independent digital I/O device.
    - Use the Digital Inputs and Outputs dialog box to configure the appliance's I/O settings. Once configured, you can use the digital inputs and outputs in alarms and other system actions.
- Email notifications
    - You can set up an SMTP email server to send you messages when system events occur.
- Setup the Gateway
    - The ACC 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 ACC Mobile app on your mobile device so that you can remotely monitor live and recorded video.

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:



1. OUT 2 (Relay Output) — Form-A dry contact outputs. When active, terminals are connected. Terminals are open when inactive.

   Maximum load is 30 V, 2 A or 200 V, 250 mA.

2. OUT 2
3. Ground (GND)
4. OUT 1 (Relay Output) — Form-A dry contact outputs. When active, terminals are connected. Terminals are open when inactive.

   Maximum load is 30 V, 2 A or 200 V, 250 mA.

5. OUT1
6. GND
7. IN 4 (Alarm In) — Active-Low inputs. To activate, connect the Input to the Ground pin (GND). To deactivate, leave disconnected or apply between 3 – 15 V.
8. IN 3
9. IN 2
10. IN 1

LED Indicators

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

Front Panel LEDs

Icons	LED Status	Description
	Green	Device is powered and running.
	Orange	Device is restarting.
	Orange - blinking	Factory restore button pressed.
	Green	Hard disk drive is connected.
	Red	Hard disk drive connection has an error.
	Green	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.
	Green	Network activity is present.
	Orange	On for 100M speed. Off for 10M speed.

Upgrading the Firmware

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

Before you can upgrade or reinstall the firmware, download the latest version of the firmware (`.fp`) file from the Avigilon website (**avigilon.com**) and

1. If you have access to the Internet from your web browser while using the Web Interface, from the Dashboard, navigate to the About panel. and click Firmware Updates.

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

2. Save the file to a location accessible to the Web Interface.

You can upgrade the firmware from:

- The Web Interface
- An ACC Client connected to the device. Refer to the procedure for upgrading servers in a site in the Help files provided with the ACCClient.

To upgrade the firmware from the Web Interface:

1. Use one of these methods:
   - Drag-and-Drop
     1. Use Windows Explorer to navigate to the location of the downloaded firmware file.
     2. Click on the file in the Explorer window and drag it over the **Drop '.fp' file here or click to upload** area.
   - Click to upload
     1. Click in the **Drop '.fp' file here or click to upload** area. The Windows Open dialog box is displayed.
     2. Use Windows Explorer to navigate to the location of the downloaded firmware file.
     3. Click on the file in the Open dialog box and click **Open**.
2. Click **OK** to confirm you want to continue. An upload progress indicator appears. Wait while the file is uploaded and verified. After the file is verified, the device will reboot. The Web UI Communication Lost message appears while the device is rebooting. The process takes several minutes. When the device has rebooted, the connection to the Web Interface is restored in your web browser.

   You can cancel a firmware upgrade that is in progress only during the upgrade and verification phase. Click **Cancel upload** before the file has downloaded.

   NOTE: If an error occurs during the upload phase or the upgrade process or if the firmware becomes corrupted, you are prompted to remove the file. The system may revert to the factory default settings as the system reboots.

Using the Reset Button

The reset button is located at the front of the appliance and is the small unlabeled circle to the left of the System Status LED. For more information, see *Front View* on page 1

The reset button provides two functions:

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

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

Restarting the System

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

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

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

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

Restoring Factory Default Settings

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

NOTE: Restoring to the factory default settings will delete all configuration settings and recorded video.

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

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

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

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/**.