avigilon™
a Motorola Solutions Company

User Guide

Avigilon Artificial Intelligence Appliance

VMA-AIA1-CG1 and VMA-AIA1-CG2

(ACC 6.10 and later with firmware releases 3.2 and later)

Avigilon Corporation
avigilon.com

PDF-VMA-A1A1-B

Revision: 2 - EN

20200611

Table of Contents

Introduction

The Avigilon AI Appliance (Avigilon AI Appliance) provides Avigilon's patented self-learning video analytics and Avigilon Appearance Search™ on existing multi-megapixel IP cameras that are not already analytic-enabled when paired with the Avigilon Control Center software (ACC). The Avigilon AI Appliance features:

- Avigilon's self-learning video analytics with no manual calibration, as available on Avigilon analytic cameras.
- Pre-integrated with Avigilon Control Center High Definition Network Video Management System for simple setup.
- High capacity video analytic processing that accepts video sources from 320 × 240 to 3264 × 2448 pixels.

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

Before You Start

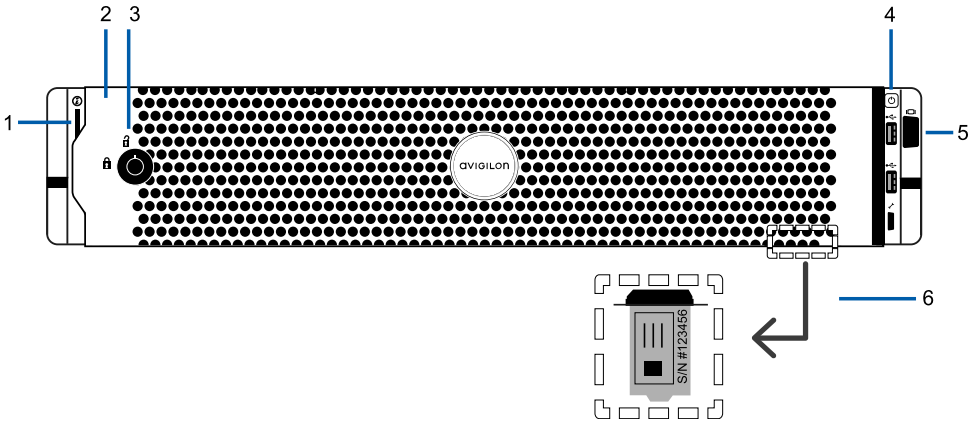
Avigilon recommends the use of an uninterruptible power supply (UPS) system to protect your video surveillance system hardware. A UPS system is used to protect critical equipment from mains supply problems, including spikes, voltage dips, fluctuations and complete power failures using a dedicated battery.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

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

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

Overview

Front View



1. **Diagnostic indicators**

   Provides information about system operations.

   For more information, see *LED Indicators* on page 18.

2. **Bezel**

   Must be installed on site.

3. **Bezel Lock**

   Protects against unauthorized physical access.

4. **Power button**

   Controls the power supply to the appliance.

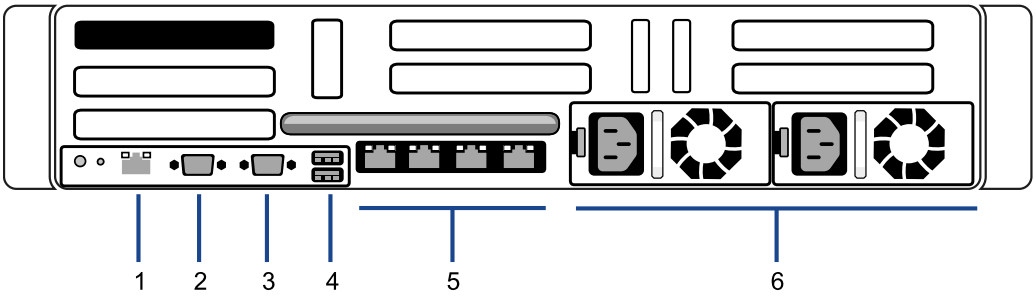
5. **Video connector**

   Accepts a VGA monitor connection.

6. **Information tag**

   Pull-out tag that provides the product service details and support information.

Back View



1. **Out-of-Band Management (OOBM) connector**

   Accepts an OOBM RJ-45 connection.

2. **Serial connector**

   Accepts connections to serial devices.

3. **Video connector**

   Accepts a VGA monitor connection.

4. **USB connectors**

   Accepts USB connections to external devices.

5. **Four (4) RJ-45 1 Gbps Ethernet ports**

   Accepts Ethernet connections to multiple networks. Any port can be used.

6. **Power supply**

   Two hot swappable redundant power supply.

System Requirements

Camera Frame Rate

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

Web Browser

Basic administration settings for the Avigilon AI Appliance are managed through its Web Interface. However, most configuration is done with the ACC Client.

The Web Interface can be 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.

Networking

When locating where to install the Avigilon AI Appliance, consider the following items:

- The Avigilon AI Appliance only requires a single network connection for full video analytics processing throughput, but up to four network connections are available to accommodate advanced site networking deployments.
- The Avigilon AI Appliance must be installed with network connectivity to all ACC Site member servers.
- At initial setup time, the ACC Client PC must be on a network with connectivity to the Avigilon AI Appliance.

  After the Avigilon AI Appliance has joined the ACCsite, this is no longer a requirement (ACC Client PC will still require network access to at least one site member).
- To limit cross-network traffic, it is best if the Avigilon AI Appliance is co-located with the ACC Server connected to the cameras on which the Avigilon AI Appliance will be performing video analytics.

Installation

Before starting the installation, copy down the serial number and MAC address from the label on the underside of the appliance. You will need this information during the installation procedure.

Package Contents

Ensure the package contains the following:

- Avigilon AI Appliance
- Rack sliding rail assembly kit
- Cable management arm assembly kit
- Bezel and key
- Power cables (may be provided in a separate box)

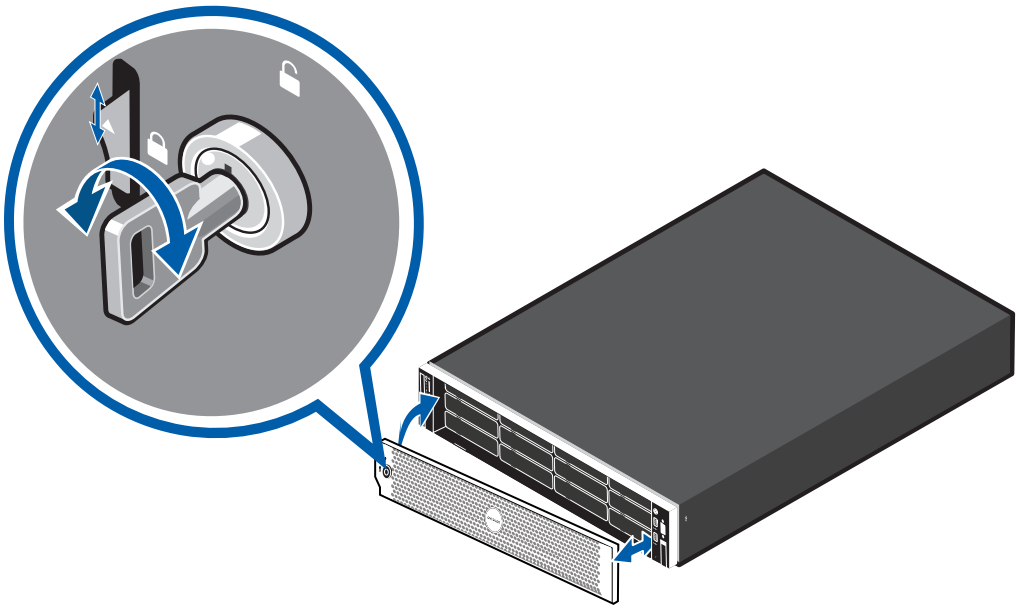
Installing the Sliding Rack Rails and Cable Management Arm

If the Avigilon AI Appliance will be kept in a server rack, install the Sliding Rack Rails and the Cable Management Arm (CMA) provided in the appliance package. Follow the procedures outlined in the *Rack Installation Instructions* and the *CMA Installation Instructions* provided in the assembly kits.

Note: The supplied Sliding Rack Rails are compatible with square and round hole racks.

Installing the Bezel

The bezel can be installed on the front of the Avigilon AI Appliance to help protect against unauthorized access.



1. Align and insert the right end of the bezel until it clicks into place.
2. Push the left end of the bezel into the front of the unit until it clicks into place.
3. Use the provided key to lock the bezel.

Connecting Cables

Refer to the diagrams in *Overview* on page 2 for the location of the different connectors. Make the following connections, as required:

1. Connect the Avigilon AI Appliance to your network using an Ethernet cable.

   Note: It is recommended that the Avigilon AI Appliance follow a similar network configuration to the site NVRs. You can connect up to 4 Ethernet cables.

2. Connect a power cable to each power supply at the back of the Avigilon AI Appliance.

Starting the Avigilon AI Appliance for the First Time

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

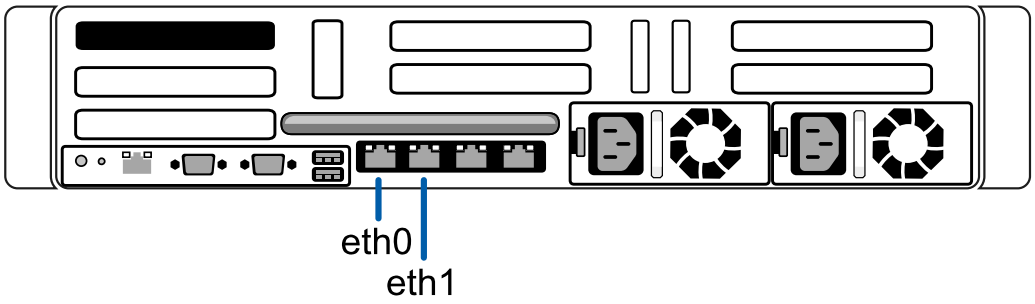
You must configure the device for the first time before connecting it to your security network.

Important: If static IPs are required, a laptop computer is required to manually configure the IP address for the device. Ensure the laptop is not assigned any of these IP addresses: 169.254.100.99 or 169.254.100.100, and has an IP subnet mask of 255.255.0.0.

1. Connect power to the device and wait for it to start up. It may take several minutes to start up the first time it is powered on.

   Check that the appliance LED indicators display the correct status. See *LED Indicators* on page 18 for more information.

2. If you are configuring the device with a static IP address, connect a DHCP enabled port on your configuring laptop with an Ethernet cable directly to the *camera network* (eth0) port on the device. Otherwise, connect the device to the corporate network using the *corporate network* (eth1) port.



3. On the connected laptop or network workstation, discover the appliance. Use File Explorer on a Windows computer or Finder® on a Macintosh computer.

   You are looking for a device labeled "VMA-AIA1-CGx-xxxxxxxxxx", where xxxxxxxxxx is the serial number of your appliance. If you cannot locate the appliance, see *Troubleshooting* on page 26.

4. Click to open the device in a supported web browser. For a list of supported web browsers, see *System Requirements* on page 3.

   Important: The Avigilon AI Appliance is configured with a self-signed certificate, which generates a connection warning in the web browser.

5. Click past any connection messages displayed by the browser. You will see two warning messages that differ slightly depending on the browser. If the browser is:
    - Chrome—Click **Advanced** on the first screen and **Proceed to <*IP address*> (unsafe)** on the second screen.
    - Firefox—Click **Advanced** on the first screen and **Add Exception** on the second screen, check **Permanently store this exception**, and click **Confirm Security Exception**.
6. You will see a security warning from the browser informing you that the connection between the Web UI and the device is untrusted because the device is using a self-signed Web Certificate. This is expected and you can safely ignore the warning and proceed to the ACC ES Admin Web UI.

    The level of security provided by the certificates included with the device should be sufficient for any organization that does not deploy a Public Key Infrastructure (PKI) on its internal servers.

    Important: For organizations that deploy their own PKI, the device's certificates can be managed from the ACC ES Admin Web UI after the device is installed and powered. The default self-signed Web Certificate can be replaced, signed certificates from Certificate Authorities (CAs) that are not provided with the device can be added, and the signed certificates from CAs for public servers such as Google Mail that are provided with device can be disabled. For more information, see *Managing Certificates* on page 20
7. 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.
8. Enter `administrator` as the username and your new password.

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

    For more information see *Rebooting the Device and Managing Device Settings* on page 14.

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

    For more information, see *Connecting the Device to Users and Cameras* on page 15.

11. If a laptop was used to configure the device:
    a. Connect an Ethernet cable from the device to the *corporate network* port.
    b. Disconnect the configuring laptop from the *camera network* port.
12. Connect the cameras to the PoE ports.

For more information about the Web Interface, see *Configuring the Appliance* on page 11

You are now ready to connect the Avigilon AI Appliance to an ACC site. For more information, see *Moving the Avigilon AI Appliance to a Site* on the next page

Moving the Avigilon AI Appliance to a Site

On its own, an Avigilon AI Appliance has no functionality. At initial setup time, the ACC Client workstation must be on a network with connectivity to the Avigilon AI Appliance. After the appliance has joined the ACC site, this is no longer a requirement, although the ACC Client PC will still require network access to at least one site member.

After you log on to the ACC Client for the first time, you must move it into the site connected to the non-analytics cameras for whose feeds you want the appliance to provide analytics processing.

1. In the site Setup tab, click  .

   The Site Management tab lists all the sites that you can access and all the devices that are connected to each site.

   If you do not see the site you want, you may need to add the site.

2. Locate the ACC site in the list into which you want to move the Avigilon AI Appliance.
3. Select the Avigilon AI Appliance. You will see the available options at the bottom of the application window.
4. To add the  Avigilon AI Appliance into a site:
   - Select the  Avigilon AI Appliance and drag it into the ACC site.
   - Or, select the  Avigilon AI Appliance then click **Connect to Site...** at the bottom-right corner of the tab. In the following dialog box, select the site you want the appliance to connect to.

   Note: More than one Avigilon AI Appliance can be connected to an ACC site. Each appliance will appear separately in the system tree.

Configuring the Appliance

The Avigilon AI Appliance can be configured through the ACC ES Admin Web UI that is accessible from any compatible browser on the network. The ACC ES Admin Web UI allows you to configure the Avigilon AI Appliance server settings, set how the server keeps time, and allows you to remotely restart or upgrade the server.

Start backing up the system settings for the recorder after you configure it. These settings include the ACC password, and the settings for the camera connections. For more information on backing up the site and server configurations, see the *Avigilon ACC Client User Guide*.

Throughout this section, the term device is used to identify the appliance.

Launching the ACC ES Admin Web UI

You can access the ACC ES Admin Web UI from a network workstation with network access to the device.

The first time you access the ACC ES Admin Web UI of your device, use one of the following methods:

- **Discovering the Device**
  1. Open the Network tab in File Explorer (Windows) or Finder (Macintosh) to locate the device.

     You are looking for a network device labeled “VMA-AIA1-CGx-<serial number>".
  2. Right click and select **View Device Webpage** to open the device sign in page in your default web browser.
- **Using the IP Address or Hostname**
  1. Open a web browser from a network workstation with network access to the device.
  2. Enter its IP address or hostname into the web browser to open the device sign in page:

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

     For example: `https://169.254.100.100/` or `https://my_AvigilonDevice/` , where `my_AvigilonDevice/` is the hostname configured in the Device panel.

     > **Note:** If you forgot the IP address or hostname that was configured during the installation process, the information is listed in the ACC Client software, in the server Setup tab.

> **Tip:** Bookmark the URLof sign-in web page for the device.

To log in to and out of the ACC ES Admin Web UI:

1. To log in, enter the ACC ES Admin Web UI username and password.

   The username is always `administrator`. Use the password you configured when you logged in to the device for the first time. For more information, see *Starting the Avigilon AI Appliance for the First Time* on page 7.

   The ACC ES Admin Web UI launch page is displayed in your web browser.

2. To log out of the ACC ES Admin Web UI, click the log out icon on the right side of the top banner.

On the ACC ES Admin Web UI launch page, **Dashboard** is selected in the side navigation bar, and the Dashboard status panels are displayed:

- **System** — Displays **Ready** when the device is fully operational, and **Rebooting** then **Initializing** when the device is restarting. The panel provides technical information about your device: product name, part number, serial number, and firmware version.

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

- **Services** — Expand **ACC** in the left sidebar to navigate to
  - The **Server** page to control the ACC Server on the device. See *Managing ACC Services and Storage* on the next page
  - The **Logs** page to view ACC Server service logs. See *Providing Service Logs for Support* on the next page.
- **System** — Access the five options to configure the device and view its status:
  - **Device**. See:
    - *Rebooting the Device and Managing Device Settings* on page 14
    - *Upgrading the Firmware* on page 23
    - *Managing Certificates* on page 20
  - **Network**. See *Connecting the Device to Users and Cameras* on page 15.
  - **Logs**. See *Providing Device Logs for Support* on page 16

Managing ACC Services and Storage

On the **Server** panel use the:

- General pane:

To...	Do this...
Shut down all the services before you shut down the device.	Click **Stop**.
Start up all the services after they have been shut down.	Click **Start**.

- Service and RTP Ports panes

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

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

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

Providing Service Logs for Support

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

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

Typically, Avigilon Technical Support assists you to access and filter the logs on this panel to isolate the logs that they require. You then copy and paste the logs into a text file, save it and send it to Avigilon Technical Support.

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

1. In the drop down list, select the type of application log that you need. The options are:
   - Analytics Service **Exception Logs**
   - Analytics Service **FCP Logs**
   - Analytics Service Logs Analytics Service Logs
   - **Exception Logs**
   - **FCP Logs**
   - **Server Logs**
   - **WebEndpoint Logs**

2. In the **Maximum Logs** drop down list, select the number of log messages you want to display each time.
3. Enter text in the **Filter** field to apply a filter to the log listings.
4. Click the **Sync** button to display the updated logs.

Rebooting the Device and Managing Device Settings

On the Device panel use the:

- **General** pane to:
  - **Reboot** the device from the ACC ES Admin Web UI. You can monitor the progress of the device as it reboots from the ACC ES Admin Web UI launch page (see . For more infomation see, *Launching the ACC ES Admin Web UI* on page 11).
  - Select a **Language** for the ACC ES Admin Web UI from the drop down list.
- **Hostname** pane to enter a new **Hostname**. Click **Apply** to make the change.

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

  > **Note:** You cannot change the default *administrator* username on the ACC ES Admin Web UI, only the password.

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

  CAUTION — You will lose configuration data if you forget your password. To reset the administrator password, you must reset the device to the factory default settings. This will delete the configuration data. For more information on performing a factory restore, see *Restoring to Factory Default Settings* on page 25.
- **Time** pane to customize how the device keeps time:
  - Select your **Time Zone** from the drop-down list. The time zone that you set here is used by the recording schedules defined in the ACC Client software.
  - Select whether you want to keep synchronized time through a Network Time Protocol (NTP) server (recommended) in the NTP field.

    Select:

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

Note: The default set of NTP servers is always present in the Servers list. The default list cannot be rearranged or deleted:

- 0.pool.ntp.org
- 1.pool.ntp.org
- 2.pool.ntp.org
- 3.pool.ntp.org

Click **Apply** to save the time settings.

- **Upgrade Firmware** pane to install the latest version of the firmware on your device, or to reinstall the firmware if it becomes corrupted. For more information, see *Upgrading the Firmware* on page 23.
- **Certificates** pane to manage the certificates used by the ACC ES Admin Web UI and the device. For more information, see *Managing Certificates* on page 20.

Connecting the Device to Users and Cameras

On the Network panel, you can change network connections of the appliance. Four network connections are supported. Any of the network connections can be used to join the Avigilon AI Appliance to an existing ACC site. The appliance must be on a network where it can be discovered by the ACC Client and can be clustered to other ACC servers. Users who administrate the appliance through the ACC Client software connect to the device through this network.

Important: Before adding the appliance as a new ACC site, or merging the appliance to an existing ACC Site, first set its IP address. It is highly recommended to be in the same IP subnet as the other servers in the ACC Site.

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

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

To...	Do this...
Set how the device obtains an IP address for	In each of the panes in the Network panel, toggle **Automatic IP** on to discover connected networks automatically (the default setting), or off to manually specify the connections. Enter the appropriate values in the following fields if you are manually

To...	Do this...
each network.	entering the connection settings: • **IP Address** • **Subnet Mask** • **Default Gateway** Click **Apply** to save your changes.
Set how the device obtains a named address from a DNS server.	Toggle **Automatic DNS** on to discover connected DNS servers automatically (the default setting), or off to manually specify the DNS servers. Controls to add and delete addresses in the list, and reorder them are activated when **Automatic DNS** is toggled off.

Providing Device Logs for Support

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

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

Typically, Avigilon Technical Support assists you to access and filter the logs on this panel to isolate the logs that they require. You then copy and paste the logs into a text file, save it and send it to Avigilon Technical Support.

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

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

Advanced Features

The following list include some advanced features of the ACC Client application thatutilize the Avigilon AI Appliance. See the ACC Client application Help files for details about how to use these features.

- Displaying Site Health
  - To help you monitor the health of your site and Avigilon AI Appliance, you can access a quick overview in the Site Health tab.

    Note: If your sites are configured into a family, you will be able to see the status of all child sites if you are logged into the parent site. If you are only logged into a child site, the parent site status is displayed as unknown.

  - The following status icons identify the status of each component in the ACC software:

     The component is functioning normally.

     The component requires your attention.

     The component is unavailable or offline.

     The component status is unknown.

  - **Analytics Service**:

    An icon displays the ACC Analytics Service status:

     The ACC Analytics Service is online.

     The ACC Analytics Service was overloaded at some point in the last 3 days. Reduce the Total Server Analytics Load by disabling Face Recognition or the Avigilon Appearance Search feature on some cameras.

     The ACC Analytics Service is offline.

  - **Peak Load (Last 3 Days)**:

    The highest percent usage of the analytics service over the last 3 days.

- Avigilon Appearance Search
  - With the Avigilon Appearance Search feature, operators can search for and find all instances of a person or vehicle in recorded video quickly and easily.
  - When used with the Avigilon AI Appliance, the Avigilon Appearance Search feature can search for instances of a person or vehicle in both cameras with video analytics and cameras without video analytics.
  - See the application Help files for details about how to perform an Avigilon Appearance Search.

LED Indicators

The following tables describe what the LEDs on the Avigilon AI Appliance indicate.

Diagnostic Indicators

The diagnostic indicators on the front panel highlight system issues during system startup.

> **Note:** The diagnostic indicators only light-up when the appliance is powered.

LED Indicator	Description
 **Hard drive**	• Blinks orange — the hard drive is experiencing an error.

 **Temperature**	• Blinks orange — there is a thermal error.
	Errors include:
	  • temperature out of range
	  • fan failure
	Check that the fans are functioning correctly and the air vents are not blocked.

 **Electrical**	• Blinks orange — there is an electrical error.
	Errors include:
	  • voltage out of range
	  • failed power supply
	  • voltage regulator
	Check the power status indicator to confirm if it is an issue with the power supply.

 **Memory**	• Blinks orange — there is a memory error.
 **PCIe**	• Blinks orange — there is a PCIe card error. Restart then upgrade the device firmware if the error persists.
System health and System ID	• Blue — powered and in good health • Blinking blue — System ID mode active • Orange — fail-safe mode • Blinks orange — there is an error

Power Status Indicators

The power button on the front lights up when power is on.

Additional information about the power supply is provided by the power status indicator on the power supplies at the back. The following table describes what the LEDs indicate:

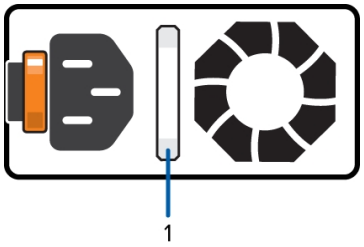


Figure 1: (1) The power status indicator.

LED Indicator	Description
Off	Power is not connected.
Green	Power is supplied.
Flashing green	The firmware update is being applied to the power supply unit.
Flashing green then turns off	The redundant power supply is mismatched. This only occurs if you have a secondary redundant power supply installed.
Flashing orange	There is a problem with the power supply.

Managing Certificates

Trusted certificates are used by the device to authenticate other servers and clients to which it needs to connect, and to secure those connections. Avigilon provides a self-signed Web Certificate to secure the connection to the ACC ES Admin Web UI and to the WebEndpoint service, and a set of system-level signed certificates from well-known trusted CAs to ensure secure connections to any needed servers. Optionally, you can provide your own certificates and CAs.

The level of security provided by the certificates included with the device should be sufficient for any organization that does not deploy a Public Key Infrastructure (PKI) on its internal servers.

The certificate management feature on the appliance controls only the appliance web certificate used by the ACC ES Admin Web UI and the ACC WebEndpoint product. Within the ACC server the certificate authorities configured by this feature are only used to validate secure email servers used by ACC Email and Central Station Monitoring features. ACC Server to ACC Server and ACC Server to ACC Client connections are not controlled or validated using the appliance certificate management feature.

For example, if your organization uses a public email server such as Google Mail, when email notifications are triggered, ACC accesses the Google Mail server and receives a certificate identifying the Google Mail server. The ACC software verifies the certificate by confirming the CA that signed the Google Mail certificate is from the list of well-known trusted CAs, and the connection is secured.

Note: The signed certificates shipped with the device are the same as those shipped with Mozilla's browser, and are publicly available from **The Debian Project**. The certificates allow SSL-based applications to check for the authenticity of SSL connections. Avigilon can neither confirm nor deny whether the certificate authorities whose certificates are included with this appliance have in any way been audited for trustworthiness or RFC 3647 compliance. Full responsibility to assess them belongs to the local system administrator.

Organizations that deploy their own PKI can use the Certificates pane of the ACC ES Admin Web UI to manage certificates on the device.

For example, you can:

- Replace the default self-signed Web Certificate with your own organization's certificate.
- Add CAs, such as internal CAs used within your organization, to the device.
- Disable (and enable) any of the system-level CA certificates.

Replacing the Web Certificate

Manage the device's Web Certificate from the Web Certificate tab on the Certificates pane. The ACC ES Admin Web UI and the WebEndpoint service use this certificate to authenticate themselves to devices that connect to them. Only one Web Certificate can be active at any time.

You can replace the default Web Certificate with a custom certificate.

Important: When you reset the device to its factory settings (also known as a factory reset), you need to reload your custom certificate.

Obtaining a new Web Certificate is a three-step process:

1. Send the certificate issuer used by your organization a Certificate Signing Request (CSR) and the issuer will return you a new certificate file and private key file (typically by email). You can generate a CSR from the Web Certificate tab, or using the certificate issuer's preferred method if they do not accept the CSR from the ACC ES Admin Web UI:
    a. Open the Web UI, click Device in the navigation bar, and scroll down to the Certificates pane.
    b. On the Web Certificate tab, click the Certificate Signing Request button.
    c. Fill in the standard CSR form with the information defined by the PKI you are using and click Generate.

       The CSR file generated.csr is saved in your Downloads folder.

    d. Send the file to your organization's certificate issuer.

       Tip: If the certificate issuer does not accept the CSR, use the certificate issuer's preferred method to generate the CSR.

2. After you receive the .crt file containing the new certificate from the certificate issuer, save it to a location accessible to the device.
3. Upload the new certificate to the device:
    a. Open the Web UI, click Device in the navigation bar, and scroll down to the Certificates pane.
    b. On the Web Certificate tab, click Upload.
    c. In the Upload Web Certificate dialog, enter a name for the certificate, and click and navigate to the .crt file or drag and drop into the Drop '.crt' certificate (pem) file here or click to uploadarea.
        - If the certificate file was created with the most recently generated CSR file from the ACC ES Admin Web UI, Upload is activated.
        - Otherwise, click and navigate to the .key file or drag and drop into the Drop '.key' private key (pem) file here or click to uploadarea. Upload is activated.

          Note: If the certificate file (.crt) was created with a CSR generated by the certificate issuer's preferred method (or was not generated using the most recent CSR file on the device), repeat this step to upload the private key file.

    d. Click Upload.

4. On the Web Certificate tab, click on the name of the uploaded certificate to enable it. This also disables the previous certificate.

Upload a Trusted CA Certificate

Manage signed certificates from internal CAs deployed in your organization's internal servers from theUser Certificate Authorities tab of the Certificates.

For example, an internal email server in an organization that deploys its own PKI may provide a certificate signed by a CA that is not in the set of well-known trusted CAs to the ACC software when it tries to access the mail server. The certificate cannot be verified unless a certificate signed by that CA is uploaded to the User Certificate Authorities tab of the Certificates pane.

If you are required to upload a signed certificate from a CA, complete the following steps:

1. Open the Web UI, click Device in the navigation bar, and scroll down to theCertificates pane.
2. Click the User Certificate Authorities tab.
3. Click Upload.
4. In theUpload User Certificate Authority dialog, enter a name for the certificate, and click or drag and drop to upload the file. You can only upload one file at a time.

Upgrading the Firmware

You can upgrade the firmware using the ACC ES Admin Web UI.

> **Note:** You can also upgrade the firmware from an ACC Client connected to an ACC-based NVR in the same site as the Avigilon AI Appliance. Refer to the procedure for upgrading servers in a site in the Help files provided with the ACC Client.

Upgrade the firmware to ensure the appliance is operating with the latest software, to upgrade from obsolete software, or to replace corrupted firmware. When you upgrade the firmware, all your current settings and all recorded video is retained.

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.

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

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

   Otherwise, from a workstation connected to the Internet, navigate to **partners.avigilon.com** and download the appropriate Avigilon AI Appliance firmware.

2. Save the file to a location accessible to the ACC ES Admin Web UI.

To upgrade the firmware from the ACC ES Admin Web UI:

1. Navigate to the Device panel.
2. If necessary, scroll to show the Upgrade Firmware pane;
3. Use one of these methods:
   - Drag-and-Drop
     1. Use Windows Explorer to navigate to the location of the downloaded firmware file.
     2. Click on the file in the Explorer window and drag it over the **Drop '.fp' file here or click to upload** area.
   - Click to upload
     1. Click in the **Drop '.fp' file here or click to upload** area. The Windows Open dialog box is displayed.
     2. Use Windows Explorer to navigate to the location of the downloaded firmware file.
     3. Click on the file in the Open dialog box and click **Open**.
4. Click **OK** to confirm you want to continue. An upload progress indicator appears. Wait while the file is uploaded and verified. After the file is verified, the device will reboot. The Web UI Communication Lost message appears while the device is rebooting. The process takes several minutes. When the

device has rebooted, the connection to the ACC ES Admin Web UI is restored in your web browser.

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

> **Note:** If an error occurs during the upload phase or the upgrade process or if the firmware becomes corrupted, you are prompted to remove the file.

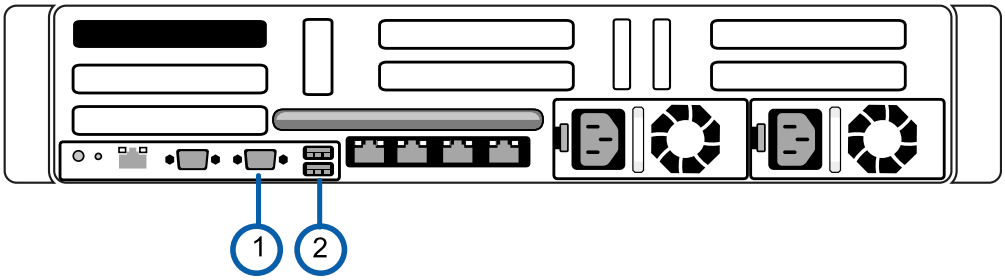
Restoring to Factory Default Settings

You may have to restore the Avigilon AI Appliance to the original factory default settings if the firmware becomes corrupted, or if you forget the administrator password and have no backup administrator account with a known password.

CAUTION — All configuration data is deleted when you restore the appliance to the factory default settings. The firmware installed on the machine at the factory before it was delivered is restored. After the appliance is restarted, you must reconfigure the appliance as though it was newly installed, and upgrade the firmware to the latest release.

To restore the factory settings:

1. Connect a monitor and keyboard to the Avigilon AI Appliance to the connections on the rear of the appliance.



❶ VGA connector (for monitor)

❷ USB connector (for keyboard)

2. Press the power button on the front of the appliance to powercycle the appliance and start the reboot process.

   The Avigilon logo and a progress bar appear on the monitor while the BIOS is loading.

3. When the progress bar indicates the BIOS loading is nearly complete, press and hold down the **f** key on the keyboard.

   Within a minute the bootloader welcome screen appears. The first progress message indicates that the factory reset button has been pressed.

4. Release the **f** key when the progress message “reset latched -- waiting for release” appears.

   Within a minute the bootloader welcome screen appears. The first progress message indicates that the factory reset button has been pressed.

5. After the Avigilon AI Appliance has completed the reboot, complete the procedure *Starting the Avigilon AI Appliance for the First Time* on page 7.

Troubleshooting

Cannot Discover the Device

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

- Access the appliance from your web browser using the URL https://VMA-AIA1-CGx-<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. Log into the site that uses this naming convention: VMA-AIA1-CGx-<serial number>.

       Note: The username and password for the Web Interface application is separate from the administrator username and password for the ACC Server.

    2. Display the server Setup tab.

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

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

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

Network Configuration

By default, the Avigilon AI Appliance acquires an IP address on the network through DHCP. If you need to set up the Avigilon AI Appliance to use a static IP address or any specific network configuration, see the *Connecting the Device to Users and Cameras* on page 15 for more information.

Checking System Health

You can check on the health of the system components in the Site Health in the ACC Client software. See **Site Health** in the *ACC Client User Guide* for more information.

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**.

For More Information

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

Technical Support

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