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)

© 2021, Avigilon Corporation. All rights reserved. AVIGILON, the AVIGILON logo, AVIGILON CONTROL CENTER and AVIGILON APPEARANCE SEARCH are trademarks of Avigilon Corporation. MacOS, FINDER and MACINTOSH are registered trademarks of Apple Inc. FIREFOX is a registered trademark of Mozilla Foundation. Other names or logos mentioned herein may be the trademarks of their respective owners. The absence of the symbols ™ and ® in proximity to each trademark in this document or at all is not a disclaimer of ownership of the related trademark. Avigilon Corporation protects its innovations with patents issued in the United States of America and other jurisdictions worldwide (see **avigilon.com/patents**). Unless stated explicitly and in writing, no license is granted with respect to any copyright, industrial design, trademark, patent or other intellectual property rights of Avigilon Corporation or its licensors.

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

Avigilon Corporation
avigilon.com

20210806

Table of Contents

Introduction

The 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 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 install the AI Appliance and configure it to provide analytics processing for the ACC system after it has been powered and is connected to the local area network.

Before You Start

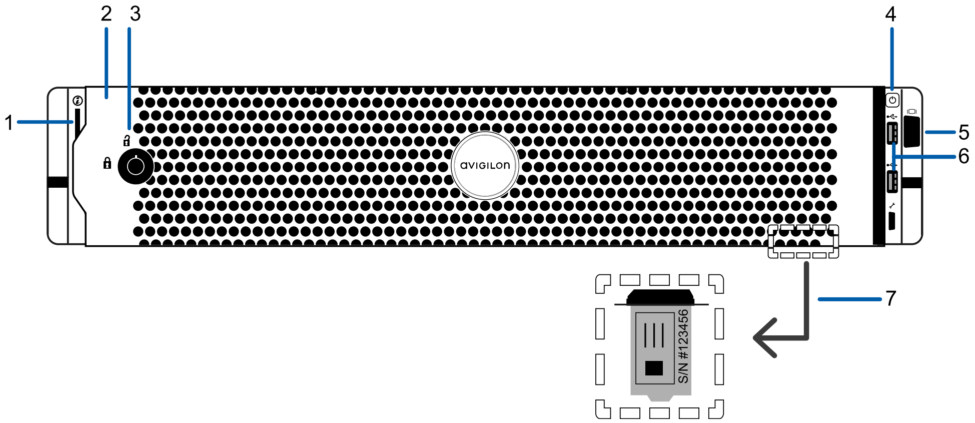
Avigilon recommends:

- 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.

  If possible, the UPS connection should include configuration to shut down the operating system on the appliance when battery power is low or there is 15 minutes of power remaining.
- 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 22.

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. Usable for interacting with the BIOS/iDRAC firmware only while the appliance is powering on.

6. **USB connectors**

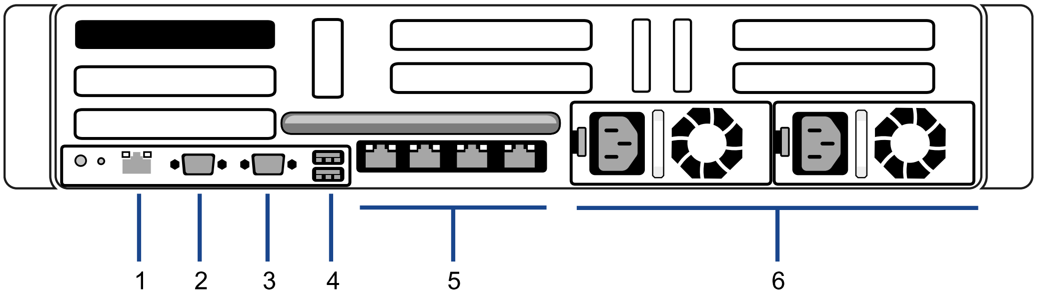
   Accepts USB connections to external devices. Enabled only while the appliance is powering on, before they are disabled by the OS.

7. **Information tag**

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

Note: The USB and video connectors (on the front and back of the appliance) are enabled only while the appliance is powering on before the OS has completed its initialization. A monitor and keyboard can be used during this interval to interrupt the OS boot-up sequence and access the BIOS/iDRAC firmware.

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.Accepts a VGA monitor connection. Usable for interacting with the BIOS/iDRAC firmware only while the appliance is powering on.

4. **USB connectors**

   Accepts USB connections to external devices.Accepts USB connections to external devices. Enabled only while the appliance is powering on, before they are disabled by the OS.

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

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

6. **Power supply**

   One (VMA-AIA2-CG1) and or two (VMA-AIA2-CG2) non-redundant power supplies.

System Recommendations

Uninterruptible Power Supply

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

Camera Frame Rate

The AI Appliance is meant to 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 AI Appliance are managed through its Server Management page, which can be accessed from the ACC Client application or a web browser on a network workstation connected to the AI Appliance.

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

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

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

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

Networking

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

- Before connecting the AI Appliance, install the latest ACC Client software on the ACC Client PC.
- At initial setup time, the AI Appliance must be on the same network as the ACC Client workstation used to used to set it up. However, after the AI Appliance has been connected to the ACC Site, this is not required.
- Install the AI Appliance so that it can communicate over the network with all the ACC Site member servers.
- To limit cross-network traffic, it is best if the AI Appliance is co-located with the ACC Server connected to the cameras on which the AI Appliance will be performing video analytics.

Passwords

The first time you start the AI Appliance you must create an administrator password for the Server Management page. Without this password you cannot configure the appliance. Additionally, without this password the AI Appliance can only be brought back into service by resetting it to its default state as it was when first delivered — updates made to the ACC Server software, and all configuration settings are lost and cannot be restored.

Certificate Management

By default, the AI Appliance is configured with a self-signed certificate, which generates a connection warning in the web browser. Organizations that deploy their own PKI can use the Certificates pane of the Server Management page to manage certificates on the device. For more information, see *Manage Certificates* on page 10.

Setting Up the AI Appliance

Package Contents

Ensure the package contains the following:

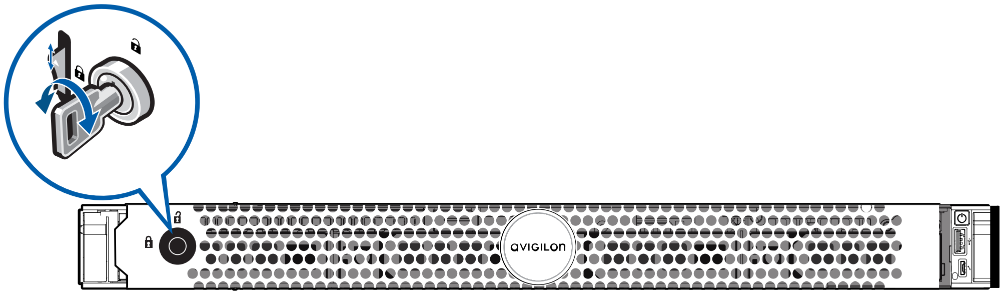
- AI Appliance
- Rack sliding rail assembly kit
- Cable management arm assembly kit
- Bezel and key
- Power cables (may be provided in a separate box)

Install the Sliding Rack Rails and Cable Management Arm

If the AI Appliance will be mounted 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.

Install the Bezel

The bezel can be installed on the front of the 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 an Ethernet port on the AI Appliance to your local network.

   Note: It is recommended that the 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 AI Appliance.

Starting the AI Appliance for the First Time

If you are adding the AI Appliance to an existing site and you use DHCP to automatically assign IP addresses to all the devices in your security network, you can use the ACC Client software on a workstation with network connectivity to the AI Appliance to discover it. Use the procedure *Connect to the AI Appliance (using DHCP)* below.

If static IP addresses are assigned to all the devices managed by ACC server software in your security network, you must use the procedure *Connect to the AI Appliance (using Static IP)* on the next page to:

1. Discover the AI Appliance in your local network.
2. Open the Server Management page in a web browser.
3. Manually set the IP address for the AI Appliance.

Connect to the AI Appliance (using DHCP)

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

1. On a workstation connected to the same network as the AI Appliance, start and log in to the ACC Client software.
2. Locate the new site in the Site Login list. You are looking for a site labeled “VMA-AIA1-CGx-<serial number>”.
3. You are prompted to enter new login credentials for the system administrator of the AI Appliance. Enter `administrator` as the username and a new password.

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

4. In the Explorer right-click on the AI Appliance and select **Setup**.
5. Click on the server below the site.
6. Click **Server Management**.
7. Click **Trust**.
8. You are prompted to log in to the Server Management.

   Enter `administrator` as the username and a new password. Use the credentials you entered for the system administrator of the AI Appliance.

   The Dashboard panel of Server Management for the AI Appliance is displayed.
9. Configure the basic settings for your new AI Appliance in Server Management, including the hostname, time zone, and language. For more information see *Using Server Management* on page 16

Connect to the AI Appliance (using Static IP)

You must use this procedure if static IP addresses are assigned to all the devices in your security network.

After powering on the AI Appliance:

1. 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-<serial number>" or the hostname you configured in the Server Management page for this device.

   If you cannot locate the appliance, see *Troubleshooting* on page 25.

2. Click to connect to the device.

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

3. Click past any connection messages displayed by the web browser. You will see two warning messages that differ slightly depending on the browser. For example, if the browser is:

   - Chrome—Click **Advanced** on the first screen and **Proceed to <*IP address*> (unsafe)** on the second screen.
   - Firefox—Click **Advanced** on the first screen and **Add Exception** on the second screen, check **Permanently store this exception**, and click **Confirm Security Exception**.

4. You are prompted to log in to Server Management. Enter `administrator` as the username and a new password. This is the username password for the system administrator of Server Management.

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

   The page refreshes and you are prompted to log in to the Server Management page.

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

   The Dashboard panel of the Server Management page is displayed.

6. On the navigation sidebar click **Network**.

7. Manually set the IP address for your new AI Appliance in the Server Management page:

   a. In each of the panes in the Network panel, click on the **IP** tab and toggle **Automatic IP** off to manually specify the connections.

   b. Enter the appropriate values in the following fields if you are manually entering the connection settings:

        - **IP Address**
        - **Subnet Mask**
        - **Default Gateway**
    c. Click **Apply** to save your changes.

8. Configure other basic settings, including the hostname, time zone, and language while you are logged in to Server Management page. For more information see *Configuring the AI Appliance for the First Time* below

Configuring the AI Appliance for the First Time

To...	From the Navigation Sidebar...	On the Card...	Setting
Change the language for Server Management	Click **Device**	**General**	Choose your language from the drop down **Language** list
Replace the default server name with a user-friendly hostname		**Hostname**	Change the **Hostname**
Set the time zone		**Time**	Specify the **Time Zone** and identify the time source in the **NTP** drop-down and **Servers** list.
	For more information, see *Manage Device Settings* on page 18.		

For more information about the other configuration settings in Server Management, see *Using Server Management* on page 16.

Manage Certificates

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

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

The certificate management feature on the appliance controls only the appliance web certificate used by Server Management and the ACC WebEndpoint product. Within the ACC server the certificate authorities configured by this feature are only used to validate secure email servers used by the ACC Email and Central

Station Monitoring features. ACC Server to ACC Server and ACC Server to ACC Client connections are not controlled or validated using the appliance certificate management feature.

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

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

Organizations that deploy their own PKI can use the Certificates pane of Server Management to manage certificates on the device.

For example, you can:

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

Replace the Web Certificate

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

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

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

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

1. Send the certificate issuer used by your organization a Certificate Signing Request (CSR) and the issuer will return you a new certificate file and private key file (typically by email). You can generate a CSR from the Web Certificate tab, or using the certificate issuer's preferred method if they do not accept the CSR from Server Management:

   a. Open Server Management, click Device in the navigation bar, and scroll down to the Certificates pane.
   b. On the Web Certificate tab, click the Certificate Signing Request button.
   c. Fill in the standard CSR form with the information defined by the PKI you are using and click Generate.

      The CSR file generated.csr is saved in your Downloads folder.
   d. Send the file to your organization's certificate issuer.

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

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

        > **Note:** If the certificate file (.crt) was created with a CSR generated by the certificate issuer's preferred method (or was not generated using the most recent CSR file on the device), repeat this step to upload the private key file.
   d. Click Upload.
4. On the Web Certificate tab, click on the name of the uploaded certificate to enable it. This also disables the previous certificate.

Upload a Trusted CA Certificate

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

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

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

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

Upgrade the Firmware

Upgrade the firmware to ensure the AI Appliance is operating with the latest software. When you upgrade the firmware, all your current settings and all recorded video are retained.

Upgrade the firmware in any of the following ways:

- You can use Cloud Remote Site Upgrade from Avigilon Cloud Services to update:
  - the firmware on the AI Appliance,
  - the firmware on all other Avigilon servers,
  - the firmware on all Avigilon cameras, and
  - the ACC Client software on all network workstations

  in the same site all at the same time.

  A subscription to the Advanced System Health feature package is required. This is the Avigilon recommended way to quickly and efficiently complete site-level upgrades. Refer to the procedure for upgrading servers in a site in the Help files provided with Avigilon Cloud Services.
- You can use Remote Site Upgrade from an ACC Client connected to all of the AI Appliances in a site at the same time. Refer to the procedure for upgrading servers in a site in the Help files provided with the ACC Client.
- You can use the Server Management page, using the following procedure.

Before you can upgrade or reinstall the firmware with the Server Management page, download the latest version of the firmware (`.fp`) file from the Avigilon **Support Community**.

From a workstation connected to the Internet:

1. Navigate to **support.avigilon.com** and search for the appropriate AI Appliance firmware.

   > **Note:** To download firmware you must have, or create an account and be logged into the Community.

2. Save the file to a location accessible to the Server Management page.

To upgrade the firmware from the Server Management page:

1. Navigate to the Device panel.

   If necessary, scroll to show the Upgrade Firmware pane.

2. In the Upgrade Firmware pane, click on **Drop '.fp' file here or click to upload** and navigate to the location where the firmware package (.fp) file was saved.

3. Click **OK** to confirm you want to continue. An upload progress indicator appears. Wait while the file is uploaded and verified.

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

   After the file is verified, the firmware upgrade automatically starts. The device will reboot several times during the upgrade. The Web UI Communication Lost message appears while the device is rebooting. When the device has rebooted, the connection to the Server Management page is restored in your web browser.

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

Adding the AI Appliance to a Site

After starting the AI Appliance for the first time, use the ACC Client software to add the AI Appliance to the site that is connected to the non-analytics cameras for whose feeds you want the appliance to provide analytics processing.

1. On a workstation connected to the same network as the AI Appliance, start and log in to the ACC Client software.
2. In the Site Login list, locate and click on the:
    - AI Appliance and log in.
    - The ACC site to which you want to attach the AI Appliance and log in.
3. With the ACC site selected in the Site Login Explorer, click the New Task ☰, and click **Site Setup**.
4. In the site Setup tab, click **Manage Site**.

    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. See *Connect to the AI Appliance (using DHCP)* on page 8 or *Connect to the AI Appliance (using Static IP)* on page 9.
5. Locate the ACC site in the list to which you want to add the AI Appliance.
6. Select the AI Appliance. You will see the available options at the bottom of the application window.
7. To add the AI Appliance into a site:
    - Select the AI Appliance and drag it into the ACC site.
    - Or, select the 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 AI Appliance can be connected to an ACC site. Each appliance will appear separately in the system tree.

Now that the appliance has been added to an ACC site, there is no requirement for the appliance to have network connectivity to the ACC Client workstation, however the ACC Client workstation still requires network access to at least one site member so that it can receive the camera feeds from the site for processing and then return the processed feeds to the site for recording.

Using Server Management

The AI Appliance is configured through Server Management, which you can access from the ACC Client application or any compatible browser on a workstation on the same network as the appliance. With Server Management you can configure the appliance server settings, set how the server keeps time, and remotely restart or upgrade the server. Throughout this section, the term device is used to identify the appliance.

Start backing up the system settings for the appliance after you configure it. These settings include the ACC password, and the settings for the camera connections. For more information on backing up the site and server configurations, see the Help files provided with the ACC Client software, or the *Avigilon ACC Client User Guide* available from the Avigilon website.

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

Starting and Stopping Server Management

Start and log in to Server Management from any network workstation with network access to the device, using any of the following methods:

- **Directly from the ACC Client software:**
  1. Start the ACC Client software.
  2. Log in to the site from the System Explorer.
  3. In the New Task menu ☰, click **Site Setup**.
  4. Select the device in the System Explorer and click **Server Management** to open the device sign-in page.
- **With a bookmark from a web browser:**

  Use one of these methods to create a bookmark:

  - Discover the device
    1. Open the Network tab in File Explorer (Windows) or Finder (Macintosh) to locate the device.
    2. You are looking for a device labeled “VMA-AIA1-CGx-<serial number>” or the hostname you configured in the Server Management page for this device.

       If you cannot locate the device, see *Troubleshooting* on page 25.
    3. Right click and select **View Device Webpage** to open the device sign in page in your default web browser.
    4. Bookmark the device sign in page
  - Use 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/` where `169.254.100.100` is the IP address configured in the Device panel.
- `https://my_AvigilonDevice/` , where `my_AvigilonDevice/` is the hostname configured in the Device panel.

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

c. Bookmark the device sign-in page.

Log out and stop Server Management by clicking the log out icon on the right of the Server Management title bar.

Manage ACC Services

On the **Server** panel use the:

- General pane:

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

- Service and RTP Ports panes to change the UDP and TCP ports used to communicate with the AI 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.

Provide Server Logs and System Logs for Support

Use the Logs panel to view the Server Logs and System Logs panes and prepare log files requested by Avigilon Technical Support to help resolve an issue.

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

By default, a log pane displays 100 warning messages from the logs.

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

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

Manage Device Settings

On the navigation bar, click Device.

To...	On the Device panel card...	Setting
Change the language for Server Management	**General**	Choose your language from the drop down **Language** list
Replace the default server name with a user-friendly hostname	**Hostname**	Change the **Hostname**. The default hostname is the same as the server name. The server name is in the form <*Model*>-<*Serial Number*>.
Set the time zone	**Time**	Specify the **Time Zone** and identify the time source in the **NTP** drop-down and **Servers** list. See *Manage Time Settings* on the next page

To…	On the Device panel card…	Setting
Change the password for the AI Appliance administrator.	**Password**	See *Change the AI Appliance Administrator Password* below.
Install the latest version of the firmware on your device.	**Upgrade Firmware**	See *Upgrade the Firmware* on page 13.
Manage the certificates used by Server Management and the AI Appliance.	**Certificates**	See *Manage Certificates* on page 10.

Change the AI Appliance Administrator Password

You can only change the password, not the default *administrator* username for Server Management.

1. On the navigation bar, click **Device**.
2. On the General panel locate the **Password** pane.
3. Enter your current password in the **Old Password** field.
4. Enter your new password in the **New Password** and **Confirm Password** fields.

   A complex password is recommended.

Remember to save the password in a secure format and location either physically or digitally so that it can be retrieved if the password is forgotten, and discard the record of the previous password.

⚠ **CAUTION —** You will lose 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 *Restore the AI Appliance to Factory Default Settings* on page 24.

Manage Time Settings

Customize how the AI Appliance keeps time:

1. Select your **Time Zone** from the drop-down list. The time zone that you set here is used by the recording schedules defined in the ACC Client software.
2. Select whether you want to keep synchronized time through a Network Time Protocol (NTP) server (recommended) in the NTP field.

   Select:

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

> **Note:** The default set of NTP servers is always present in the Servers list. However, this list is only used if NTP is enabled and not provided by your DHCP server. The default list cannot be rearranged or deleted.

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

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

Connect the Device to Cameras and ACC Client Users

On the Network panel, you can configure the network connections for the appliance. Four network connections are supported. Use one connection for the network where the AI Appliance can be discovered by other ACC servers and ACC Client PCs, so you can join it to an existing ACC site. Users who administrate the AI Appliance with the ACC Client software connect to the appliance through this network.

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

To...	Do this...
Set how the device obtains an IP address for each network.	In each of the panes in the Network panel, toggle **Automatic IP** on to discover connected networks automatically (the default setting), or off to manually specify the connections. Enter the appropriate values in the following fields if you are manually entering the connection settings: • **IP Address** • **Subnet Mask** • **Default Gateway** Click **Apply** to save your changes.
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.

LED Indicators

The following tables describe what the LEDs on the 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	• Not used.
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:

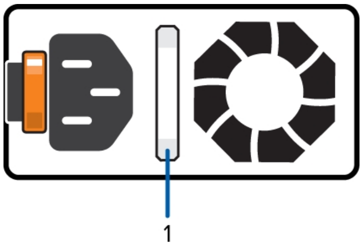


Figure 1: (1) The power status indicator.

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.

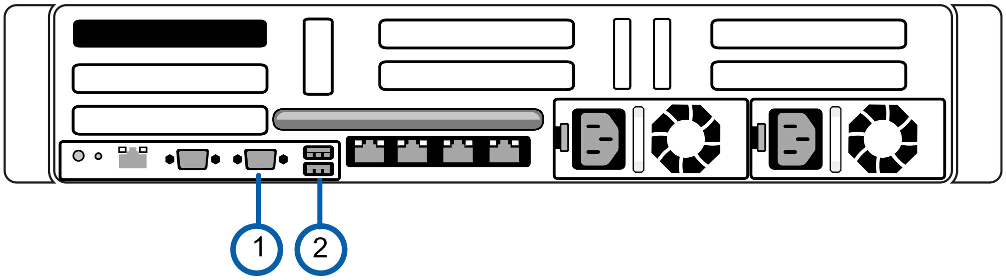
Restore the AI Appliance to Factory Default Settings

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

Important: All configuration data is deleted when you restore the AI Appliance to its 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 AI Appliance to the connections on the rear of the appliance.

   1. VGA connector (for monitor)
   2. USB connector (for keyboard)

   Tip: Alternatively, you can uhe USB connectors on the front of the appliance.

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.
5. After the AI Appliance has completed the reboot, it must be completely reconfigured. Complete the procedure *Starting the AI Appliance for the First Time* on page 8.

Troubleshooting

Accessing the Server Management page from a Web Browser

There may be cases where you want to access the Server Management page without using the ACC Client.

You can access the Server Management page from any Windows®, Apple, or mobile device using most popular web browsers.

Note: Your web browser must be configured to accept cookies or the Web Interface will not function correctly.

1. On a network workstation, discover the appliance. Use File Explorer (Windows) or Finder® (Apple).

   You are looking for a device labeled "VMA-AIA1-CGx-<serial number>" or the hostname you configured in the Server Management page for this device.
2. Click to open the device in a supported web browser.

   Important: The AI Appliance is configured with a self-signed certificate, which generates a connection warning in the web browser.
3. 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**.
4. Log in as `administrator`.

   The Dashboard panel of the Server Management page is displayed.

Cannot Discover the Device

There are several ways you can discover a device that is supposed to connected to your network from a network workstation. The recommended order to discover a device is:

- Check that the appliance is connected to the local network with an Ethernet cable.
- Check that the appliance LED indicators display the correct status. See *LED Indicators* on page 22 for more information.
- Using File Explorer (Windows) or Finder (Apple)

  You are looking for a device labeled “VMA-AIA1-CGx-<serial number>” or the hostname you configured in the Server Management page for this device.
- Discover the DHCP-assigned IP address from the ACC Client software:
  - Log into the site that uses this naming convention: 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.
- 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.

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

Network Configuration

By default, the AI Appliance acquires an IP address on the network through DHCP. If you need to set up the AI Appliance to use a static IP address or any specific network configuration, see the *Connect the Device to Cameras and ACC Client Users* on page 20 for more information.

Monitoring System Health

You can monitor the health of the system components in the Site Health in the ACC Client software. See the Help files provided with the ACC Client software, or the *Avigilon ACC Client User Guide* available from the Avigilon website for more information.

Limited Warranty

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

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**.