



AVIGILON™ UNITY

AI Appliance 2X User Guide

Contents

- Avigilon Artificial Intelligence Appliance 4
- System Recommendations 6
- Overview..... 9
- Package Contents..... 13
- Setting Up the AI Appliance 2X 14
- Starting the AI Appliance 2X for the First Time..... 16
- Adding the AI Appliance 2X to a Site 22
- Reactivating Unity Video Licenses 24
- Enabling Analytics on an AI Appliance 2X 26
- Using Management Interface 28
 - Opening Management Interface 29
 - Managing General Settings 32
 - Rebooting the AI Appliance 2X 33
 - Upgrading the Firmware 34
 - Changing the AI Appliance 2X Administrator Password 35
 - Managing Time Settings 36
 - Managing Certificates 37
 - Managing Unity Video Services 41
 - Managing Network Settings 42
 - NIC Teaming for Network Resiliency 43
 - Providing Server Logs and System Logs for Support..... 45
 - Configuring Docker IP Address Pools 47
- Troubleshooting 50
- LED Indicators..... 54
 - System Health and Identification Modes..... 61
 - Resetting the iDRAC System..... 61
- Powering Down an AI Appliance 2X 63
- Restoring the AI Appliance 2X to Factory Default Settings 64
- More Information & Support 66

Warranty.....	66
Copyright.....	67
Regulatory Notices.....	67

Avigilon AI Appliance 2X

User Guide



VMA-AIA2X-CG2 and VMA-AIA2X-CG3

The AI Appliance 2X enhances the security of your site by adding Avigilon Next-Generation Analytics on video from non-analytic cameras. The AI Appliance 2X features industry-leading hardware and is available in two models to support up to 160 cameras for site scalability and high-performance. With its Next-Generation Video Analytic capabilities, the AI Appliance 2X supports: Classified Object Detection™, Unusual Activity Detection (UAD), Occupancy Counting, No Face Mask Detection, Facial Recognition technology, and Avigilon Appearance Search™ technology. An AI Appliance 2X connected to a Unity Video server at your site can take on the real-time analytics processing of the camera feeds from non-analytics cameras, reducing the processing load on the server and increasing the analytics capacity of your Unity Video site.

The AI Appliance 2X higher capacity CG3 model supports on-premise generative AI features when configured in the appropriate AI mode. The GenAI Visual Alerts feature triggers real-time custom alerts from the field of view of any camera feeds connected to a NVR in a Unity Video site.

This guide describes how to install the AI Appliance 2X and configure it to provide analytics processing for the Unity Video system after it has been powered and is connected to the local area network.

[Avigilon Artificial Intelligence Appliance](#)

[System Recommendations](#)

[Overview](#)

[Package Contents](#)

[Setting Up the AI Appliance 2X](#)

[Starting the AI Appliance 2X for the First Time](#)

[Adding the AI Appliance 2X to a Site](#)

[Reactivating Unity Video Licenses](#)

[Enabling Analytics on an AI Appliance 2X](#)

[Using Management Interface](#)

[Troubleshooting](#)

[LED Indicators](#)

[Powering Down an AI Appliance 2X](#)

[Restoring the AI Appliance 2X to Factory Default Settings](#)

[More Information & Support](#)

System Recommendations

Uninterruptible Power Supply

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.

Camera Frame Rate

The AI Appliance 2X 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 AI Appliance 2X are managed through its Management Interface page, which can be accessed from the Unity Video Client application or a web browser on a network workstation connected to the AI Appliance 2X.

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 Management Interface 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 2X in a multi-server deployment, consider the following items:

- Before connecting the AI Appliance 2X, install the latest Unity Video Client software on the Unity Video Client PC.
- At initial setup time, the AI Appliance 2X must be on the same network as the Unity Video Client workstation used to set it up. However, after the AI Appliance 2X has been connected to the Unity Video Site, this is not required.
- Install the AI Appliance 2X so that it can communicate over the network with all the Unity Video Site member servers.
- To limit cross-network traffic, it is best if the AI Appliance 2X is co-located with the Unity Video Server connected to the cameras on which the AI Appliance 2X will be performing video analytics.

Passwords

The first time you start the AI Appliance 2X you must create new administrator passwords for both:

- The Unity Video Site running on the AI Appliance 2X.
- The Management Interface page running on the AI Appliance 2X.

Without these passwords the AI Appliance 2X can only be brought back into service by resetting it to its default state as it was when first delivered — all recorded data, updates made to the Unity Video Server software, and all configuration settings are lost and cannot be restored. For more information, see [Starting the AI Appliance 2X for the First Time](#).

Certificate Management

By default, the AI Appliance 2X 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 Management Interface page to manage certificates on the device. For more information, see [Managing Certificates](#).

Overview

Front View

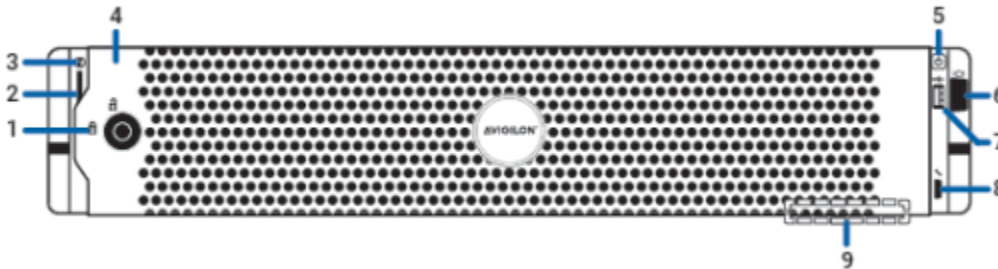


Figure 1: Front view of AI Appliance 2X with front bezel installed.

1. Bezel lock

Protects against unauthorized physical access.

2. Diagnostic indicators

Provides information about system operations.

For more information about the above LED indicators, see [LED Indicators](#).

3. System health and system identification button

Displays the system health. Also identifies a appliance deployed in a rack with other equipment.

For more information, see [System Health and Identification Modes](#).

4. Bezel

Protects against unauthorized physical access to the hard drives.

For more information, see [Setting Up the AI Appliance 2X](#).

5. Power button

Controls the power supply to the recorder.

6. Video connector

Accepts a VGA monitor connection.

7. USB 2.0 port

Disabled at run time.

8. iDRAC Direct micro USB port and iDRAC Direct LED indicator

Connects a laptop or desktop computer on the same network as the Integrated Dell™ Remote Access Controller (iDRAC) version 9.

For more information about the iDRAC web interface, see the information tag on your recorder and the [Enabling iDRAC Enterprise Features Setup Guide](#).

9. Information tag (top and bottom views are not shown)

Slides out to provide the serial number, system information, and iDRAC account credentials for initial login to the iDRAC web interface.

Back View

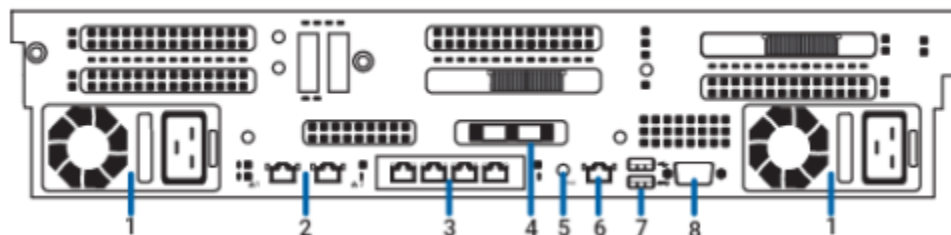


Figure 2: Back view of AI Appliance 2X. CG3 configuration is pictured.

1. Power supply connector

Accepts a power supply connection.

2. Two (2) 1 GbE Ethernet ports

Accepts Ethernet connections to multiple networks and includes LED indicators of the connections.

3. **Four (4) 1 GbE Ethernet ports**

Accepts Ethernet connections to multiple networks and includes LED indicators of the connections.

4. **Two (2) 10 GbE SFP+ Ethernet ports**

Accepts Ethernet connections to multiple networks and includes LED indicators of the connections. CG3 only.

5. **System identification button**

Identifies an appliance deployed in a rack with other equipment. Also resets the iDRAC web interface without rebooting the operating system.

For more information about the iDRAC reset, see the [Enabling iDRAC Enterprise Features Setup Guide](#).

6. **Out-of-Band Management (OOBM) port**

Accepts an OOBM RJ-45 connection and includes an LED indicator of the connection.

7. **USB 3.0 port**

Disabled at run time.

8. **Video connector**

Accepts a VGA monitor connection.

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.

Package Contents

Ensure the package contains the following hardware:

- AI Appliance 2X
- Rack sliding rail assembly kit
- Cable management arm assembly kit
- Bezel and key
- 2 x Power cables (C19 / C20)

Setting Up the AI Appliance 2X

Install the Sliding Rack Rails and Cable Management Arm

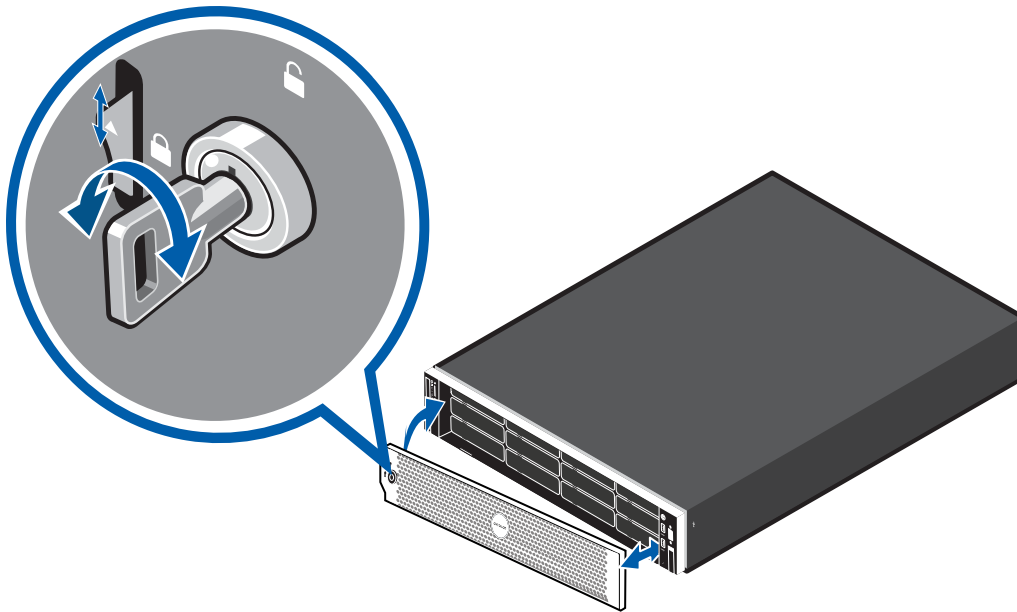
If the appliance will be mounted in a server rack, install the Sliding Rack Rails and the Cable Management Arm (CMA) provided in the appliance package. Follow the procedures outlined in the *Rack Installation Instructions* and the *CMA Installation Instructions* provided in the assembly kits.

NOTE

When rack-mounting the appliance, ensure no interference occurs from the sliding arms of adjacent equipment in the rack. Every sliding rack rail on the server rack must be aligned before you insert the appliance into the rail for a smooth installation. For more information, refer to the dimensions in your server rack design documentation.

Install the Bezel

The bezel can be installed on the front of the appliance to help protect the hard drives 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.

Connect the Cables and Power On

Refer to the diagrams in the [Overview](#) section for the location of the different connectors. Make the following connections as required:

1. Connect the AI Appliance 2X to the network by plugging an Ethernet cable into one of the Ethernet ports.



NOTE

It is recommended that the AI Appliance 2X follow a similar network configuration to the site NVRs. You can connect up to 4 Ethernet cables.

2. Connect a power cable to both of the power supplies at the back of the AI Appliance 2X.
3. Press the power button on the front of the AI Appliance 2X and wait for it to start up. Wait for the System health and System ID diagnostic LED indicator to stop blinking and turns a steady blue.

For more information on the different LED status indicators, see [LED Indicators](#).

Starting the AI Appliance 2X for the First Time

Connecting to the AI Appliance 2X for the First Time

You can connect the AI Appliance 2X to a Unity Video site using either DHCP or Static IP.

If you are adding the AI Appliance 2X to an existing site and you use DHCP to automatically assign IP addresses to all the devices in your corporate network, you can use the Unity Video Client software on a workstation with network connectivity to the AI Appliance 2X to discover it. Use the procedure [Using DHCP](#).

If static IP addresses are assigned to all the devices managed by Unity Video server software in your corporate network, you must use the procedure [Using Static IP](#) to:

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

Using DHCP

If you use DHCP to assign IP addresses in your network, the new AI Appliance 2X is immediately detected after it is connected to the corporate network. The Unity Video server software then adds it to the list of sites that is displayed in the System Explorer when you start the Unity Video Client.

1. On a workstation connected to the same network as the AI Appliance 2X, start and log in to the Unity Video Client software.
2. Locate the new site in the Site Login list. You are looking for a site labeled "VMA-AIA2X-CGx-<serial number>".
3. The `administrator` username is pre-populated along with an empty password. Leave the credentials as they are and click Log In.
4. You are prompted to enter new login credentials for the administrator user of the Unity

Video Server running on the AI Appliance 2X. Enter and confirm the new administrator password and click OK.

 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.

5. In the Explorer right-click on the AI Appliance 2X and select Setup.
6. Click to select the server below the site you right-clicked in the previous step.
7. Click  **Management Interface**.
8. Click **Trust** on the certificate message that opens.
9. You are prompted to log in to the Management Interface.

You are prompted to create a new password for the `administrator` user of the AI Appliance 2X operating system. Enter and confirm the new administrator password, then click Apply. It is recommended to not use the same credentials as the Unity Video system administrator.

 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 Dashboard panel of Management Interface for the AI Appliance 2X is displayed.

 NOTE

On subsequent logins, you will need to enter the `administrator` username and this password when logging in to the AI Appliance 2X Management Interface. The administrator is the only user that can log in to the Management Interface.

10. Configure the basic settings for your new AI Appliance 2X in the Management Interface, including the hostname, time zone, and language. For more information see [Configuring the AI Appliance 2X for the First Time](#).

To increase your network resiliency, it is recommended to use network interface controller (NIC) teaming with your network connections. For more information, see [NIC Teaming for](#)

Network Resiliency.

Using Static IP

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

After powering on the AI Appliance 2X:

1. Discover the device. Use File Explorer on a Windows computer or Finder® on a Macintosh computer on the same local network as the AI Appliance 2X.

You are looking for a device labeled VMA-AIA2X-CGx-**<serial number>**, or the hostname you configured in the Management Interface page for this device.

If you cannot locate the appliance, see [Troubleshooting](#).

2. Click to connect to the device.

Important

By default, the AI Appliance 2X 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 Management Interface page to manage certificates on the device. For more information, see [Managing Certificates](#).

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 Management Interface. You are prompted to create a new password for the `administrator` user. Enter and confirm the new administrator password, then click Apply. This is the new password for the system administrator of the AI Appliance 2X operating system.

 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 Dashboard panel of the Management Interface page is displayed.

 NOTE

On subsequent logins, you will need to enter the `administrator` username and this password when logging in to the Management Interface. The administrator is the only user that can log in to the Management Interface.

5. On the navigation sidebar click Network.
6. Manually set the IP address for your new AI Appliance 2X in the Management Interface 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:
 - a. IP Address
 - b. Subnet Mask
 - c. Default Gateway
 - c. Click Apply to save your changes.
7. If you are installing the first Avigilon appliance in your corporate network, download and install the latest Unity Video Client software on a network workstation or on the computer you are using to access the Management Interface page.

To increase your network resiliency, it is recommended to use network interface controller (NIC) teaming with your network connections. For more information, see [NIC Teaming for Network Resiliency](#).

Configuring the AI Appliance 2X for the First Time

Configure the basic settings for your new AI Appliance 2X in Management Interface, including the hostname, time zone, and language.

To...	From the Navigation Sidebar...	On the Pane...	Setting
Change the language for Management Interface	Click General	System	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.
Set AI Mode		AI Mode	Specify the AI Mode as either: • AdaptAI + UnityAI - This hybrid mode enables both GenAI based features like Visual Alerts, as well as advanced video analytics such as Classified Object Detection, Appearance Search, and Face

To...	From the Navigation Sidebar...	On the Pane...	Setting
			Recognition. • AdaptAI - This mode enables only advanced video analytics such as Classified Object Detection, Appearance Search, and Face Recognition. Refer to the Analytics Sizing Guide for performance guidance of each mode.
For more information, see Managing General Settings .			

For more information about the other configuration settings in Management Interface, see [Using Management Interface](#).

Adding the AI Appliance 2X to a Site

After starting the AI Appliance 2X for the first time, use the Unity Video Client software to add the AI Appliance 2X to the site that is connected to the non-analytics cameras for whose feeds you want the appliance to provide analytics processing.

NOTE

Options to connect will only appear if there is an active Unity Video Enterprise license on both the AI Appliance 2X and the Unity Video site that it will be added to.

1. On a workstation connected to the same network as the AI Appliance 2X, start and log in to the Unity Video Client software.
2. In the Site Login list, locate and click on the:
 - AI Appliance 2X and log in.
 - The Unity Video site to which you want to attach the AI Appliance 2X and log in.
3. With the Unity Video 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 [Using DHCP](#) or [Using Static IP](#).

5. Locate the Unity Video site in the list to which you want to add the AI Appliance 2X.
6. Select the AI Appliance 2X. You will see the available options at the bottom of the application window.
7. To add the  AI Appliance 2X into a site:
 - Select the  AI Appliance 2X and drag it into the Unity Video site.
 - Or, select the  AI Appliance 2X 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 2X can be connected to a Unity Video site. Each appliance will appear separately in the system tree.

Now that the appliance has been added to a Unity Video site, there is no requirement for the appliance to have network connectivity to the Unity Video Client workstation, however the Unity Video 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.

Reactivating Unity Video Licenses

When an AI Appliance 2X is added to or removed from a site, the site licenses become inactive and must be reactivated to confirm system changes.

If you do not reactivate the affected licenses, the site will stop normal operations.

1. In the New Task menu , click Site Setup.
2. Click the site name, then click .
3. Click **Reactivate Licenses....**

If you have Internet access:

1. Click Reactivate Licenses.
2. Click OK to confirm your changes.

If you do not have Internet access:

1. Select the **Manual** tab.
2. Click Save File... and choose where you want to save the `.key` files.
3. Copy the `.key` files to a computer with internet access:
 1. Go to activate.avigilon.com.
 2. Click **Choose File** and select the `.key` file.
 3. Click Upload. A `capabilityResponse.bin` file should download automatically.

If not, allow the download to occur when you are prompted.

4. Complete the product registration page to receive product updates from Avigilon.
5. Copy the `.bin` file to a computer running the Unity Video Client software.
4. In the License Management dialog box, click **Apply....**
5. Select the `.bin` file and click **Open**.
6. Click OK to confirm your changes.

Enabling Analytics on an AI Appliance 2X

To enable analytics processing on the video streams from cameras connected to the Unity Video site to be done by the AI Appliance 2X:

1. Open the Unity Video Client software and log in to the AI Appliance 2X.
2. In the New Task menu , click Site Setup.
3. Expand the site and click on the AI Appliance 2X.
4. In the Setup tab, click Server Analytics .
5. Select an analytics feature tab and then select the cameras to enable the feature on:
 - **Visual Alerts** (requires UNITY8-ENT licenses on CG3 model, see docs.avigilon.com/bundle/unity-video-visual-alerts)
 - Classified Object Detection (requires UNITY8-ENT licenses)
 - Appearance Search (requires UNITY8-ENT licenses)
 - Face Recognition (requires UNITY8-FACE licenses)
 - Face Mask Detection (requires UNITY8-ENT licenses)

Only cameras that you have access to that have the prerequisite analytics enabled are displayed in each tab. If you do not see a tab, it could be because your site does not have the required analytics license.

Important

The AI Appliance 2X is not suitable for:

- Classified Object Detection on thermal cameras.
- **Visual Alerts** on thermal cameras, or cameras with warped or fisheye projections.

Important

Appearance Search and Face Recognition are only available for cameras with server-side Classified Object Detection enabled.

 NOTE

If you have more than one AI Appliance 2X connected to the server, the non-analytics cameras that do not have analytics enabled are listed for both appliances. A camera with analytics enabled only appears on this Server Analytics panel of the appliance providing the analytics.

6. Click in the option box next to a camera to select or deselect the camera to enable analytics processing by the AI Appliance 2X for that camera.

As you enable (or disable) analytics for cameras, the bars at the bottom update to display the AI Appliance 2X's capacity. The percent usage of each analytics feature is displayed using the color of the analytics feature tab.

7. To exit the Server Analytics panel, click Close.

Using Management Interface

Configure the server settings of the AI Appliance 2X with Management Interface, accessed from any Unity Video Client application or compatible browser on a workstation on the same network as the appliance.

Back up the server settings for the appliance after you configure it, including the Unity Video password and connection settings. For more information on backing up the site and server configurations, see the Help files provided with the Unity Video Client software, or the *Avigilon Unity Video Client User Guide* available from the Avigilon website.

NOTE

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

[Opening Management Interface](#)

[Managing General Settings](#)

[Managing Unity Video Services](#)

[Managing Network Settings](#)

[NIC Teaming for Network Resiliency](#)

[Providing Server Logs and System Logs for Support](#)

[Configuring Docker IP Address Pools](#)

Opening Management Interface

From any network workstation with network access to the AI Appliance 2X, you can open Management Interface:

- Directly from the Unity Video Client software:
 1. Start the Unity Video 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 **Management Interface**  to open the device sign in page.
- With a bookmark from a web browser

Use one of these methods to create the 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-AIA2X-CGx- <serial number> or the hostname you configured in the Management Interface page for this device. If you cannot locate the device, see Troubleshooting. 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.  NOTE
---------------------	--

	 The bookmark may become invalid if the IP address of the appliance changes.
Use IP address or hostname	- Open a web browser and enter IP address or hostname of the AI Appliance 2X into the web browser to open the device sign in page: <code>https://<Device IP address > <Device hostname>/</code> - IP address example: <code>https://169.254.100.100/</code> - Hostname example: <code>https://my_AvigilonDevice/</code> IP address or hostname are configured on the Device panel. If you forget the IP address or hostname, it is listed in the Unity Video Client software, in the server Setup tab. - Bookmark the device sign in page.

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

Management Interface Dashboard

Unity Server	Check the operating state of the Unity Video Server software: - Running in green - Stopped in red
	View site information:

	- Site Name - Server Name - Server Version
System	View the AI Appliance 2X operating state: - Ready when it is fully operational - Rebooting when it is power-cycling - Initializing when it is restarting
	View system information: - Product Name - Part Number - Serial Number - Firmware Version - Date & Time - Secure Boot
Network	View information about the uplink ports on the device: the link speed and whether the link is active (up) or inactive (down). Click  to open the Network panel.
Accelerators	View status and location information about each accelerator device, such as a graphics card, installed in the appliance.

Managing General Settings

Under the Settings header of the Management Interface, click General and then find the desired service.

To...	On the Pane...	Setting
Reboot the AI Appliance 2X.	System	Click the Reboot button. See Rebooting the AI Appliance 2X .
Change the language for Management Interface.	System	Choose your language from the drop down Language list.
Install the latest version of the firmware on your device.	Upgrade Firmware	See Upgrading the Firmware .
Find information that may be helpful when troubleshooting.	Support	Download Device Logs, System Snapshot, and Dell Support Assist Collection to assist in troubleshooting.
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>.
Change the password for the AI Appliance 2X administrator.	Password	See Changing the AI Appliance 2X Administrator Password .
Set the time zone.	Time	Specify the Time Zone and identify the time source in the NTP drop-down and Servers list. See Managing Time Settings .

To...	On the Pane...	Setting
Manage the certificates used by Management Interface and the AI Appliance 2X.	Certificates	See Managing Certificates .

[Rebooting the AI Appliance 2X](#)

[Upgrading the Firmware](#)

[Changing the AI Appliance 2X Administrator Password](#)

[Managing Time Settings](#)

[Managing Certificates](#)

Rebooting the AI Appliance 2X

You can reboot the AI Appliance 2X from Management Interface:

1. On the navigation bar, click General.
2. On the System pane click Reboot.

Monitor the progress of the device as it reboots from the System pane of the Management Interface Dashboard. For more information see [Using Management Interface](#).

Upgrading the Firmware

Upgrade the firmware to ensure the AI Appliance 2X is operating with the latest features and bug fixes. 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 2X,
 - the firmware on all other Avigilon servers, and
 - the Unity Video 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 a Unity Video Client connected to all of the AI Appliance 2X servers in a site at the same time. Refer to the procedure for upgrading servers in a site in the Help files provided with the Unity Video Client.
- You can use the Management Interface page, using the following procedure.

Before you can upgrade or reinstall the firmware with the Management Interface page, download the latest version of the firmware (.fip) file from the Avigilon [Support Community](#).

From a workstation connected to the Internet:

1. Navigate to <https://www.avigilon.com/nvr-systems/ai-appliance?searchQuery=ai-appliance-2x> and search for the latest AI Appliance 2X 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 Management Interface client machine.

To upgrade the firmware from the Management Interface page:

1. On the navigation bar, click General. In the General panel, locate 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.
4. 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.

Changing the AI Appliance 2X Administrator Password

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

1. On the navigation bar, click General.
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 [Restoring the AI Appliance 2X to Factory Default Settings](#).

Managing Time Settings

Customize how the AI Appliance 2X keeps time:

1. On the navigation bar, click General.
2. On the General panel locate the Time pane.
3. 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 Unity Video Client software.
4. Select whether you want to keep synchronized time through a Network Time Protocol (NTP) server (recommended) in the NTP field.

 TIP

To synchronize time with ONVIF devices (that is, non-Avigilon ONVIF cameras), you can connect to port 123 on the AI Appliance 2X to use it as an NTP server. Once connected, Avigilon cameras will use the AI Appliance 2X as their NTP time source by default.

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

5. Click Apply to save the time settings.

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 Management Interface 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 Management Interface and the Unity Video WebEndpoint product. Within the Unity Video server the certificate authorities configured by this feature are only used to

validate secure email servers used by the Unity Video Email and Central Station Monitoring features. Unity Video Server to Unity Video Server and Unity Video Server to Unity Video 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 Unity Video software accesses the Google Mail server and receives a certificate identifying the Google Mail server. The Unity Video 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 Management Interface 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. Management Interface 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 Management Interface:
 - a. Open Management Interface, click General 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 Management Interface, click General 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.
 - a. If the certificate file was created with the most recently generated CSR file from Management Interface, Upload is activated.

- b. 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.

 WARNING

Passphrase-protected certificates are not supported.

- 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 Unity Video 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 Management Interface, click General 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.

Managing Unity Video Services

By expanding the Unity Server panel in the navigation bar, you will see a list of panels for the services running on the appliance.

Services can be managed using the buttons on the top-right corner of the Unity Server panel, which manages all services at once, or an individual service's panel:

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

From the Unity Server panel, the following settings can be managed:

- **General** pane to reset Unity Video configurations.
- **Files** pane to download Configurations, Server Logs, or a system snapshot.
- **Service** and **RTP** panes to change the UDP and TCP ports used to communicate with the AI Appliance 2X:
 - 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.

Managing Network Settings

On the Network panel, you can configure the network connections for the AI Appliance 2X. The AI Appliance 2X should be connected to the network where it can be discovered by other Unity Video servers and Unity Video Client PCs so that it can join an existing Unity Video site. Users who administrate the AI Appliance 2X with the Unity Video 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

To...	Do this...
	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.
Configure Docker IP Addresses (Unity Video 8.6 or later)	Click the + icon, then enter the desired default IP address Base and Size. Updates will take effect after the system has been restarted.

NIC Teaming for Network Resiliency

To further increase network resilience, it is recommended to use network interface controller (NIC) teaming with the AI Appliance 2X network connections. This can be set up using the Management Interface page.

NIC Teaming Modes

The AI Appliance 2X supports three types of NIC teaming: Active Backup, Dynamic Link Aggregation (IEEE 802.3ad), and Adaptive Load Balancing. Decide on the teaming mode to use before creating any NIC teams.

Active Backup

In this mode, one port out of the teamed network ports is designated as the primary port, and the others are set as the backup ports. While the primary network port is functioning properly, the backup ports will not be used. In the event that the primary network port fails, the backup

network ports will take over. Both network ports work as unique virtual network interfaces with a single mac address visible to other network devices.

Link Aggregation Control Protocol

In this mode, all of the teamed network ports will be aggregated into a single connection that has a combined bandwidth equal to the sum of all the teamed port's individual bandwidth. All teamed network ports will be utilized simultaneously while in this mode and all devices using the teamed ports will operate at the same speed and duplex. If one network port were to fail, then all traffic will be forced through the remaining network ports and your bandwidth will be reduced to the sum of the remaining ports' bandwidth.

NOTE

This mode requires a switch that can support Link Aggregation Control Protocol, and will require some setup on that switch.

Adaptive Load Balancing

In this mode, both network ports will be used as separate 10 Gb/s or 1 Gb/s connections, but the AI Appliance 2X will attempt to dynamically load balance the transmitted and received traffic that passes through each network port. Each network port can be connected to different network switches on the same IP subnet to increase redundancy. In the event that one network port fails, all traffic will be redirected to the working network port.

This mode provides many of the benefits of Link Aggregation Control Protocol without the need for any switch configuration or support. Additionally, this mode supports network ports of different speeds (10 Gb/s and 1 Gb/s) to be teamed together.

Creating NIC Teams

TIP

It is recommended to have teamed network ports in the same subnet.

1. Make a note of the IP addresses of all of your network ports. You may lose your connection after creating NIC teams, you may need this information to reconnect.

**TIP**

The AI Appliance 2X includes the ability to identify which network port on the back panel of your unit is linked to a network port selected in the Management Interface page. For more information, see [Identifying your Network Ports](#).

2. On the Network panel, click New Connection in the bottom-right corner. Then, click **Team**.

The New Team window opens.

3. Use the Add Member drop-down list to select 2 or more network ports to add to the team. Network ports that are added will display in the Members area.
4. Select the NIC Teaming mode from the Mode drop-down list. Available modes are Active Backup, Dynamic Link Aggregation (IEEE 802.3ad), and Adaptive Load Balancing.
5. If you are using Active Backup mode, use the Primary Member drop-down list to select the primary network port. All other ports in the team will be set as backup. If you select Automatic, the first port to transmit data after teaming will automatically be the primary member.
6. Click Apply to create the team. It may take a couple minutes for the NIC team to configure. Once complete, the teamed ports will no longer appear on the Network panel and will be replaced by a new team pane.

After a team is created, you can edit the team options on the Teaming tab of the team's pane, or click Remove Team to restore the individual network port configuration.

Providing Server Logs and System Logs for Support

Typically, Avigilon Technical Support assists you to access the logs that they require.

i Important

It is recommended to download all of the Device Logs at once from the **Support** service pane in the **General** panel. The package downloaded this way will include all Server Logs and System Logs. For more information, see the table in [Managing General Settings](#).

To access individual Server Logs and System Logs:

- Individual Server Logs can be viewed from their respective services under the Unity Server drop-down menu. All Server Logs can be downloaded at once from the Files service on the Unity Server panel.
- System Logs are accessed from the Logs panel under the Settings header.

This table below shows all of the logs that can be generated in Management Interface:

Server Logs	Service	Logs
	Daemon	Service, Exception, Metrics
	Web Endpoint	Service
	API Gateway	Service, Boot
	Cloud Bridge	Service, Boot
	Core	Service, Boot
	Device Management	Service, Boot
	Local Update	Service, Boot
System Logs	System, Boot, Web Server	

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.
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.

Configuring Docker IP Address Pools

You can configure custom Docker IP Address Pools on Unity Video 8.6 or later. For earlier Unity Video generations, contact Avigilon support at support.avigilon.com/s/contactsupport.

To configure Docker IP Address Pools on Unity Video 8.6 or later:

1. On the navigation sidebar of Management Interface, click **Network**.
2. Scroll down to find the **Docker** pane.

The screenshot shows the 'Docker' configuration pane in the Management Interface. It is divided into two main sections: 'Current Docker Networks' and 'Configured Address Pools'.

Current Docker Networks: A table with three columns: Label, Address, and Mask.

Label	Address	Mask
Docker Daemon	172.16.0.0	255.255.255.0
Docker Daemon	172.16.1.0	255.255.255.0
Docker Swarm	172.17.0.0	255.255.255.0

Configured Address Pools: A section with a header bar containing a plus icon, a refresh icon, and a help icon. Below the header is a table with three columns: Assignment, Address Range (CIDR), and Pool Size.

Assignment	Address Range (CIDR)	Pool Size
Assignment Docker Daemon ▼	Range 172.16.0.0/16	Size 24
Assignment Docker Swarm ▼	Range 172.17.0.0/16	Size 24

At the bottom right of the 'Configured Address Pools' section is a 'SUBMIT' button with a checkmark icon.

3. The following fields can be assigned from this pane:
 - **Assignment:** The assignment determines which application the pool is assigned to. All assignments should have address pools configured.
 - **Address Range:** The primary network range in CIDR notation from which subnets will be allocated. This range must be in a private IP address range.

 WARNING

These addresses will take priority over external connections, so overlaps within your network must be avoided.

- **Pool Size:** The size of the subnets that will be allocated. The size is the number of bits in the subnet mask. All subnets must have at least 256 addresses. Each assignment must have at least 32 subnets available, this is a cumulative total for all configured ranges for a given assignment. Configured address pools cannot overlap.

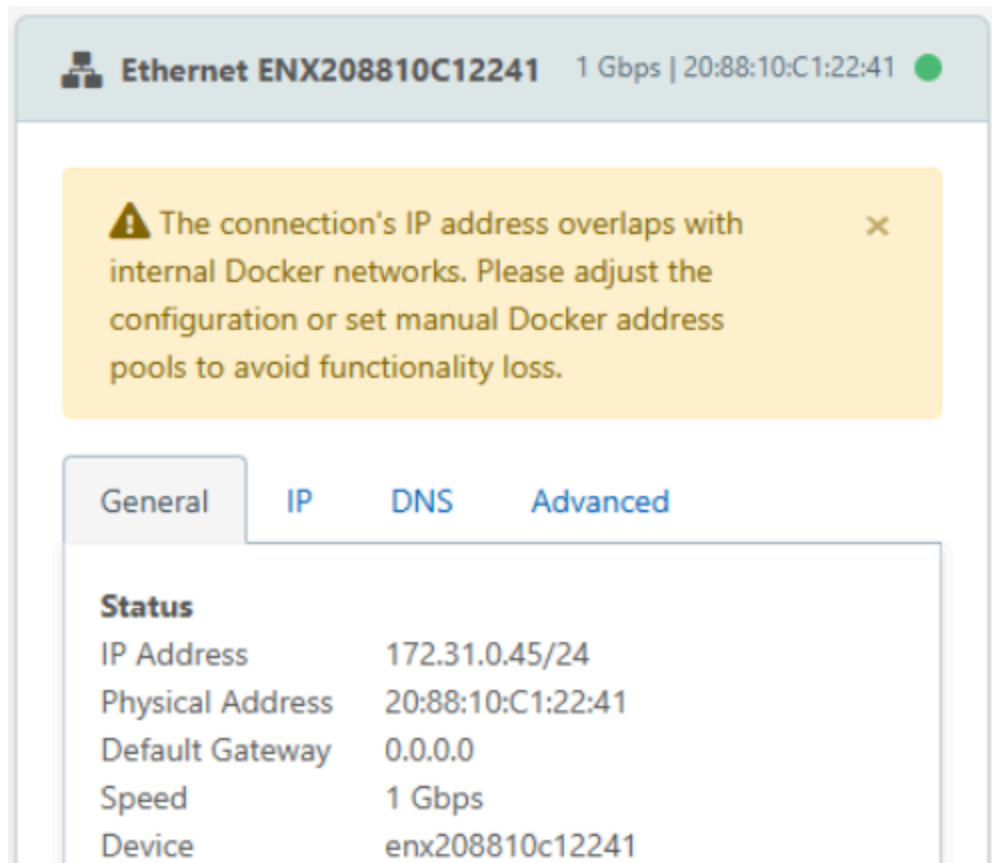
 NOTE

For example, if you create an address range with 172.31.0.0/16 and a size of 24, this will allow Docker to create 256 networks each with 256 addresses. The first network created will be assigned 172.31.0.1/24, the next will be assigned 172.31.1.1/24, and so on.

4. After assigning values, click **Submit**. You will be warned that changing the Docker address pools will restart the appliance. Click **OK** to restart the appliance and apply your changes.
5. After the system restarts, you may view your changes in the same place by navigating to the **Docker** pane of the **Network** page again.

To verify that your settings do not overlap with an existing active network connection:

1. On the navigation sidebar of Management Interface, click **Network**.
2. On the **Network** page, you will see a warning notification  at the top of any connection pane for which IP addresses overlap with the Docker network.



 NOTE

The overlap warning on the **Network** pane only detects direct IP address conflicts. It does not detect scenarios where the Docker network and the host network reach the same IP range indirectly, for example, by using different default gateways or overlapping routed subnets.

3. Correct overlapping IP addresses by navigating to the **Docker** pane again, and reassigning the **Address Range** to an unused IP address range.

Troubleshooting

Accessing the Management Interface page from a Web Browser

There may be cases where you want to access the Management Interface page without using the Unity Video Client.

You can access the Management Interface 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-AIA2X-CGx-<serial number>" or the hostname you configured in the Management Interface page for this device.

2. Click to open the device in a supported web browser.

Important

The AI Appliance 2X 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 Management Interface page is displayed.

Do Not Re-Image AI Appliance 2X

Important

Do not attempt to re-image your AI Appliance 2X. This may permanently disable your unit and void your warranty. Please contact Avigilon technical support if further troubleshooting is required.

If you have to restore the AI Appliance 2X to the original factory default settings, see [Restoring the AI Appliance 2X to Factory Default Settings](#) for instructions. This may be necessary if you forget the administrator password or if the firmware becomes unusable.

Cannot Discover the Device

There are several ways you can discover a device that is supposed to be 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](#) for more information.
- Using File Explorer (Windows) or Finder® (Macintosh)

You are looking for a device labeled VMA-AIA2X-CGx-<serial number> or the hostname you configured in the Management Interface page for this device.

- Discover the DHCP-assigned IP address from the Unity Video Client software:
 - Log into the site that uses this naming convention: VMA-AIA2X-CGx-<serial number>.

NOTE

The username and password for the Web Interface application is separate from the administrator username and password for the Unity Video Server.

- Access the appliance from your web browser using the URL <https://VMA-AIA2X-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 2X acquires an IP address on the network through DHCP. If you need to set up the AI Appliance 2X to use a static IP address or any specific network configuration, see [Using Static IP](#) for more information.

Monitoring System Health

You can monitor the health of the system components in the Site Health page in either the Unity Video Client software or Avigilon Cloud Services (ACS). See the Help files provided with the Unity Video Client software, the *Avigilon Unity Video Client User Guide*, or the *Avigilon Cloud Services Client User Guide* available from the Avigilon website for more information.

Identifying your Network Ports

The AI Appliance 2X includes the ability to identify which network port on the back panel of your unit is linked to a network connection selected in the Management Interface page. To identify a network port:

1. Open the Network panel on the Management Interface page.
2. Toggle the Identify switch on for the network connection that you want to identify.
3. Visually check the back panel of the AI Appliance 2X. The network port LEDs will be flashing for the network connection you have selected to Identify.



NOTE

 The Identify toggle will automatically switch off after 10 minutes to avoid continuously flashing LEDs.

LED Indicators

The following tables describe what the LEDs on the Network Video Recorder 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
 System health and System ID	• Steady blue – The system is powered on and healthy. System health mode is active. • Blinking blue – System identification mode is active. • Steady amber – The system is in fail-safe mode.  NOTE If the system health indicates a degraded or critical state, contact Avigilon Technical Support for assistance. • Blinking amber – The system is experiencing a fault. Check the System Event Log.
 Hard drive	• Not used.

LED Indicator	Description
 Temperature	- Steady amber — A thermal error has occurred. Possible errors include: - Temperature out of range - Fan failure Check that the fans are functioning correctly and the air vents are not blocked.
 Electrical	- Steady amber — An electrical error has occurred. Possible 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, and reseal the power supply unit, if the error persists.
 Memory	Steady amber — A memory error has occurred. Check the System Event Log and reset the memory module, if the error persists.
	Steady amber — A PCIe card error has

LED Indicator	Description
PCIe	occurred. Restart the system, upgrade the device firmware and reinstall the card, if the error persists.

iDRAC Direct LED Indicators

The iDRAC Direct LED indicates if the iDRAC port is connected to a laptop or desktop computer.



Figure 3: (1) The iDRAC Direct LED indicator

LED Indicator	Description
Off	The device is unplugged from the port.
Green for 2 seconds	The device is connected to the port.
Flashing green — on for 2 seconds and off for 2 seconds	The device is recognized by the port.

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:

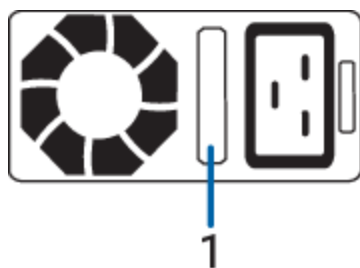


Figure 4: (1) The power status indicator.

LED Indicator	Description
Off	Power is not connected.
Green	Power is supplied.
Blinking amber	There is a problem with the power supply.
Blinking green	A firmware update is being applied to the power supply unit.  CAUTION To prevent malfunction of the power supply unit, do not disconnect the power cord or unplug the power supply unit when updating firmware.
Blinking green and turns off	The redundant power supply is mismatched. This only occurs if you have a secondary

LED Indicator	Description
	redundant power supply installed.  CAUTION To prevent power supply mismatches, do any of the following: • Avoid mixing power supply units from previous generations of servers even if the units have the same power rating. • Replace only the power supply unit with the blinking indicator.

LED Indicator	Description
	• Identical power supply units must receive the same input voltages, be of the same type and support the same maximum power output. • Combining AC and DC power supply units is not supported.

Network Link Status Indicators

When the AI Appliance 2X is connected to the network, the appliance's connection status LEDs above the Ethernet port display the appliance's connection status to the network. The following table describes what the LEDs indicate:



Figure 5: (1) Link LED. (2) Connection activity LED.

LED Indicator	Description
Off	The appliance is not connected to a network.
Link LED – green Connection Activity LED – blinking green	The appliance is connected to a network at the maximum port speed.
Link LED – orange Connection Activity LED – blinking green	The appliance is connected to a network at less than the maximum port speed.
Link LED – green Connection Activity LED – off	The appliance is connected to a network at the maximum port speed and data is not being sent or received.
Link LED – orange Connection Activity LED – off	The appliance is connected to a network at less than the maximum port speed and data is not being sent or received.

System Health and Identification Modes

Resetting the iDRAC System

System Health and Identification Modes

In the front left panel of the appliance, you can switch between system health and system identification modes:

- Press the  button to enable the system identification mode, which is used to identify an appliance deployed in a rack with other equipment.

The blue indicator starts blinking.

- Press the  button again to switch back to system health mode.

The blue indicator stops blinking.

For more information about the LED indicators, see [LED Indicators](#).

Resetting the iDRAC System

To reboot the iDRAC web interface without rebooting the operating system:

1. Go to the front left panel of the appliance.
2. Press and hold the  system health and system identification button for 16 seconds until the cooling fans start spinning at full speed.

The iDRAC system restarts without changing any saved settings. It may take a minute or longer until the remote controller restarts.

For information about using the iDRAC web interface to perform the reset, see the [Enabling iDRAC Enterprise Features Setup Guide](#).

.

Powering Down an AI Appliance 2X

To perform a soft shutdown of the AI Appliance 2X, press the power button on the front panel of the appliance. Restarts caused by firmware updates always trigger soft shutdowns.

Restoring the AI Appliance 2X to Factory Default Settings

i Important

Do not attempt to re-image your AI Appliance 2X. This may permanently disable your unit and void your warranty. Please contact Avigilon technical support if further troubleshooting is required.

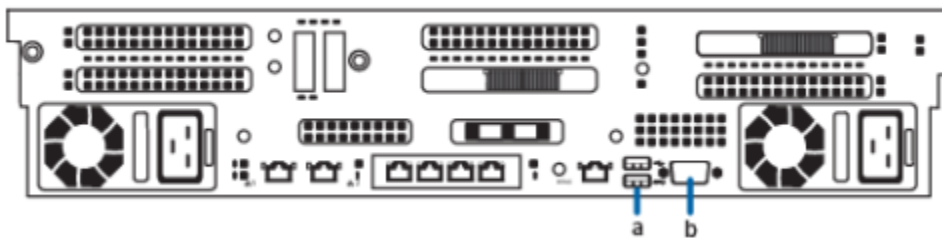
You may have to restore the AI Appliance 2X to the original factory default settings if you forget the administrator password or if the firmware becomes unusable.

i Important

All configuration data and recorded data is deleted when you restore the AI Appliance 2X 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 to the connections on the rear of the appliance.



- a. USB connector (for keyboard)
- b. VGA connector (for monitor)

TIP



Alternatively, you can use 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 2X has completed the reboot, it must be completely reconfigured, starting from [Starting the AI Appliance 2X for the First Time](#).

More Information & Support

For product user guides, visit the Downloads page: <https://docs.avigilon.com/>.

For information about recommended network architectures, see the Deploying Avigilon Solutions: A Guide to Networking Best Practices guide: <https://docs.avigilon.com/bundle/networking-best-practices/>.

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

Technical Support

Contact Avigilon Technical Support at support.avigilon.com/s/contactsupport.

[Warranty](#)

[Copyright](#)

[Regulatory Notices](#)

Limited Warranty

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

© 2025, Avigilon Corporation. All rights reserved. MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. 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

HTML-AIA2X-A
Revision: 1 – EN
20251008



UK Product Security and Telecommunications Infrastructure (PSTI) Act

Avigilon appliances comply with the PSTI requirements. For more information, see the published [PSTI Statement of Compliance](#).

Disposal and Recycling Information

When this product has reached the end of its useful life, please dispose of it according to your local environmental laws and guidelines.

Risk of fire, explosion, and burns. Do not disassemble, crush, heat above 100 °C (212 °F), or incinerate.

European Union:



This symbol means that according to local laws and regulations your product should be disposed of separately from household waste. When this product reaches its end of life, take it to a collection point designated by local authorities. Some collection points accept products for free. The separate collection and recycling of your product at the time of disposal will help conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment.

More Information & Support

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

Contact Avigilon Technical Support at support.avigilon.com/s/contactsupport.

©2025, Avigilon Corporation. All rights reserved. MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. 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.

Avigilon Corporation
avigilon.com

PDF generated on 12/4, 2025

See the Motorola Solutions terms of use at motorolasolutions.com/en_us/about/terms-use.html



MOTOROLA SOLUTIONS