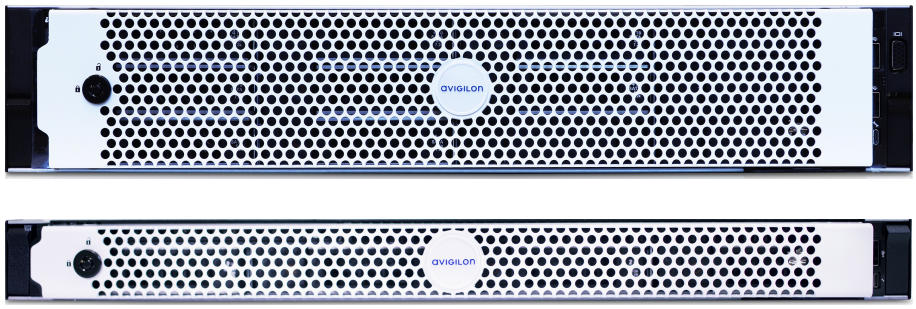
User Guide



Avigilon AI NVR

AINVR-STD-24TB, AINVR-STD-32TB, AINVR-STD-48TB

AINVR-VAL-6TB, AINVR-VAL-12TB

Avigilon Corporation
avigilon.com

20210708

Table of Contents

Introduction

The Avigilon AI NVR is a network security appliance that provides all of the functionality of an Avigilon Network Video Recorder with:

- Avigilon Hardened OS, Avigilon's secure, managed, embedded OS.
- Avigilon Control Center server software.
- Integration of existing multi-megapixel IP cameras in your network that are not already analytic-enabled with most of the features available on Avigilon analytic cameras:
    - Object Detection — Detects and classifies people or vehicles to help operators verify and respond faster. Unusual Activity Detection (UAD) automatically detects atypical behavior of learned objects. Requires an ACC7-VAC license.
    - Avigilon Appearance Search™ — Quickly locates a specific person or vehicle of interest across an entire site using a sophisticated deep-learning AI search engine.
    - Face Recognition — Detects matches from managed watchlists to alert operators of people of interest. Requires Appearance Search and an additional ACC7-FACE license.
    - No-Face-Mask Detection — Detects when a person is not wearing a face mask, with the ability to set-up alarms in ACC's Focus of Attention interface, Radio Alert and ACC Mobile 3 app.

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 NVR 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 NVR 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 NVR.

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 NVR in a multi-server deployment, consider the following items:

- Before connecting the AI NVR, install the latest ACC Client software on the ACC Client PC.
- At initial setup time, the ACC Client PC must have network access to the AI NVR. After a multi-server site is created, the ACC Client PCs require network access to at least one site member. For more information, see *Download and Install the Latest ACC Client Software* on page 16
- The AI NVR only requires a single network connection to achieve its maximum recording throughput, but up to four network connections are available to accommodate advanced site networking deployments.
- The only requires a single network connection to achieve its maximum throughput, but up to four network connections are available to accommodate advanced site networking deployments.
- Install the AI NVR so that it can communicate over the network with all the ACC Site member servers.
- Do not connect cameras to the AI NVR until after the appropriate network configuration has been set up.

Passwords

The first time you start the AI NVR you must create new administrator passwords for both:

- The ACC Site running on the AI NVR.
- The Server Management page running on the AI NVR .

Without these passwords the AI NVR 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 ACC Server software, and all configuration settings are lost and cannot be restored.

Certificate Management

By default, the AI NVR 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 28.

Package Contents

Ensure the package contains the following:

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

Overview of the AI NVR Standard Models

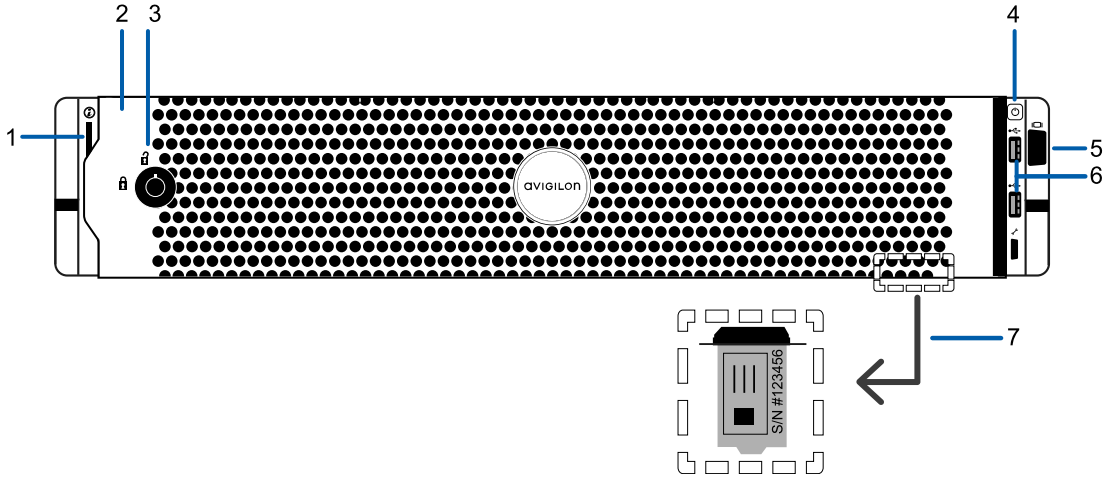


Figure 1: Front view of AI NVR Standard showing information tag (accessible after removing front bezel)

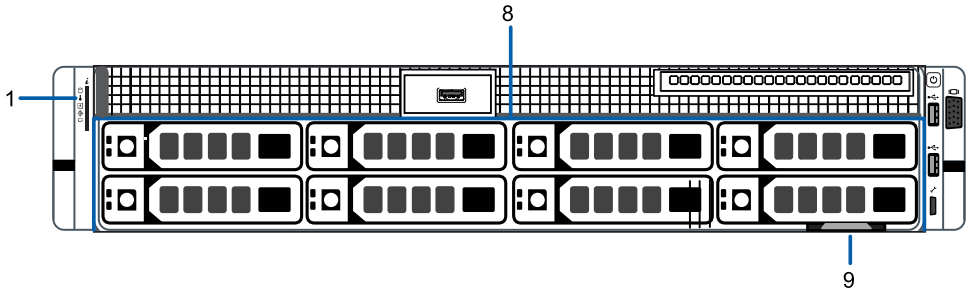


Figure 2: Front view of AI NVR Standard with bezel removed.

1. **Diagnostic indicators**

   Provides information about system operations.

   For more information, see *LED Indicators* on page 41.
2. **Bezel**

   Protects against unauthorized physical access to the hard drives. The bezel must be removed to access the front of the recorder.
3. **Bezel Lock**

   Protects against unauthorized physical access.
4. **Power button**

   Controls the power supply to the appliance.
5. **Video connector**

   Accepts a VGA monitor connection.

6. **USB connectors**

   Disabled at run time.

7. **Information tag**

   Details of the pull-out tag that provides the serial number, product service details and support information.

8. **Hard drive caddies**

   Provides access to hot-swappable hard drives. The LED indicators on each hard drive caddy indicate the status of the hard drive.

   The AINVR-STD-24TB and AINVR-STD-48TB models are equipped with eight hard drives. The AINVR-STD-32TB, model is equipped with six hard drives.

9. **Pull-out tab for the information tag**

   Location of pull-out tab.

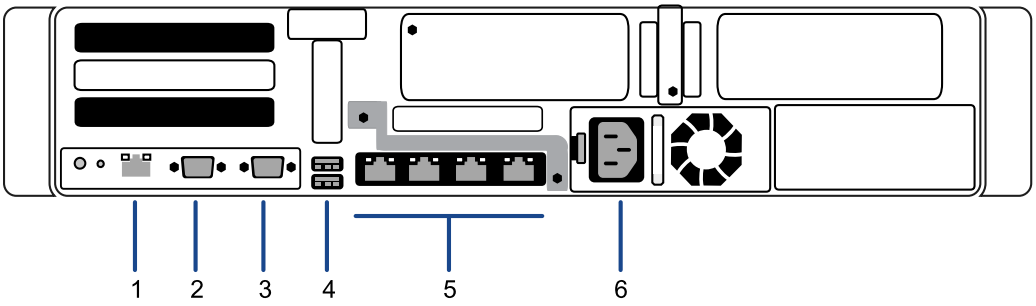


Figure 3: Back view of the AI NVR Standard

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

   Accepts an OOBM RJ-45 Ethernet connection to the management network.

2. **Serial connector**

   Accepts connections to serial devices.

3. **Video connector**

   Accepts a VGA monitor connection.

4. **USB connectors**

   Disabled at run time.

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

   Use these ports to connect to the network of security cameras and ACC Client workstations.

   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* on page 13.

6. **Power supply**

   Power supply.

Overview of the AI NVR Value Models

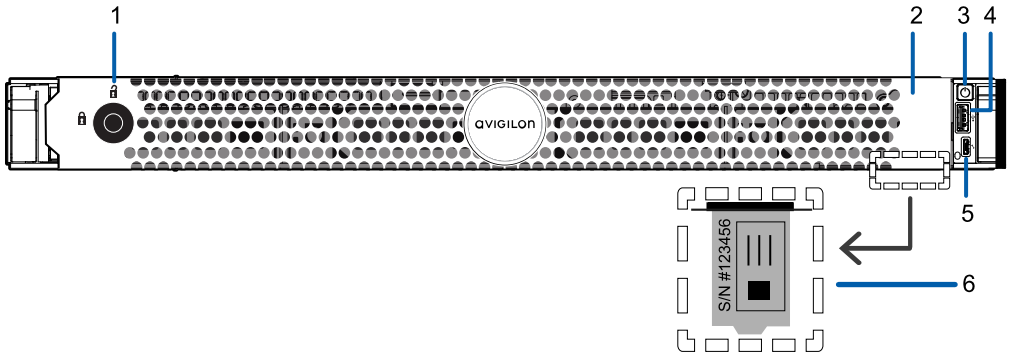


Figure 4: Front view of AI NVR Value showing information tag (accessible after removing front bezel).

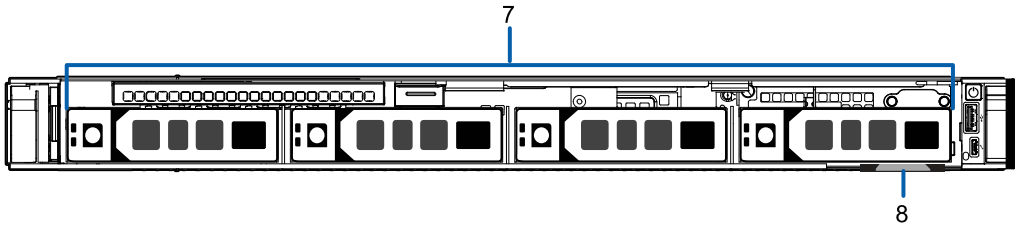


Figure 5: Front view of AI NVR Value with bezel removed.

1. **Bezel Lock**

   Protects against unauthorized physical access.
2. **Bezel**

   Protects against unauthorized physical access to the hard drives. The bezel must be removed to access the front of the recorder.
3. **Power button**

   Controls the power supply to the appliance.
4. **USB connectors**

   Disabled at run time.
5. **Micro USB port**

   Provides access to the Out-of-band (OOB) Management Network interface.
6. **Information tag**

   Details of the pull-out tag that provides the serial number, product service details and support information.
7. **Hard drive caddies**

   Provides access to hot-swappable hard drives. The LED indicators on each hard drive caddy indicate the status of the hard drive.

   The AINVR-VAL-6TB and AINVR-VAL-12TB models are equipped with four hard drives.
8. **Pull-out tab for information tag**

   Location of pull-out tab.

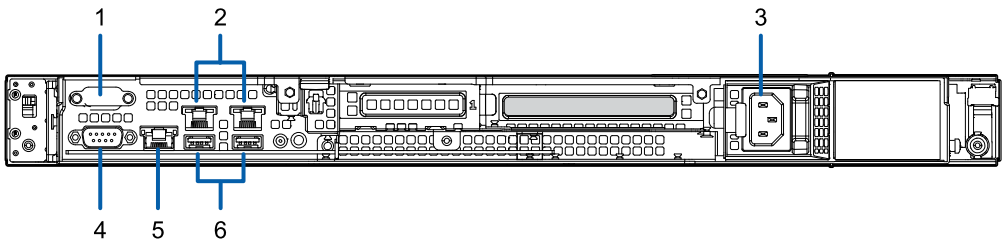


Figure 6: Back view of the AI NVR Value

1. **Serial connector**

   Accepts connections to serial devices.

2. **Two (2) RJ-45 1 Gbps Ethernet ports**

   Use these ports to connect to the network of security cameras and ACC Client workstations.

   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* on the next page.

3. **Power supply**

   Primary power supply. An optional secondary power supply is available.

4. **Video connector**

   Accepts a VGA monitor connection.

5. **Out-of-band management (OOBM) connector**

   Accepts an OOBM RJ-45 Ethernet connection to the management network.

6. **USB connectors**

   Disabled at run time.

NIC Teaming for Network Resiliency

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

> **Tip:** Since the AI NVR Value only has two network ports, if NIC teaming is used, you will no longer be able to separate recording and playback traffic with IP subnets.

The AI NVR supports three types of NIC teaming. For more information, see *NIC Teaming Modes* below.

NIC Teaming Modes

The AI NVR supports three types of NIC teaming: Active Backup, Dynamic Link Aggregation (IEEE 802.3ad), and Adaptive Load Balancing.

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.

Dynamic Link Aggregation (IEEE 802.3ad)

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 IEEE 802.3ad Dynamic Link Aggregation, 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 NVR 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 even that one network port fails, all traffic will be redirected to the working network port.

This mode provides many of the benefits of Dynamic Link Aggregation 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.

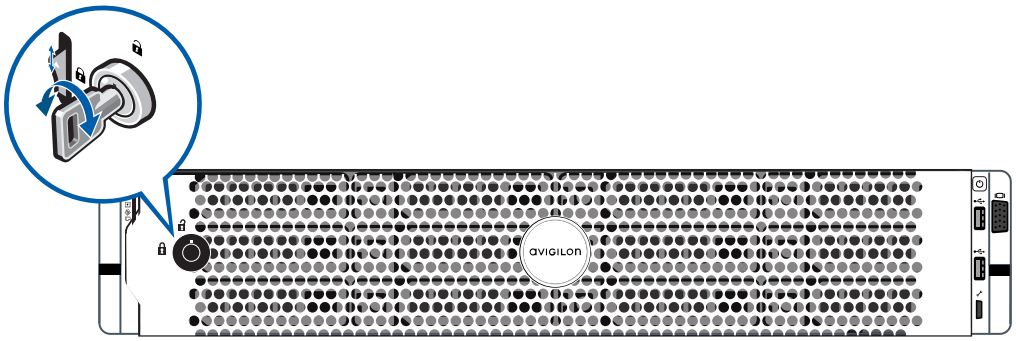
Setting Up the AI NVR

Install the Sliding Rack Rails and Cable Management Arm

If the AI NVR 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 recorder 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 NVR to the network by plugging an Ethernet cable into one of the Ethernet ports.
2. Connect a power cable to the power supply at the back of the AI NVR.
3. Press the power button on the front of the AI NVR 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* on page 41.

Download and Install the Latest ACC Client Software

Install the latest version of the ACC Client software (from **avigilon.com/support/software**) on a workstation connected to the same network on which you are going to connect the new AI NVR.

1. Click through to locate the installation software for the latest version of the ACC Client software.
2. If necessary, copy the installation software to transferable media and then to a network workstation with network access to the device, following the security protocols in force for your organization.

> **Note:** The first time you access the web site from which you download the software you will be prompted to register. Enter all of the required information and click **Complete Registration**. Your registration is automatically accepted and you will proceed to the web site.

Connect to the AI NVR (using DHCP)

If you use DHCP to assign IP addresses in your network, the new AI NVR 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 NVR, 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 “AINVR-STD-xxTB-<serial number>” or “AINVR-VAL-xxTB-<serial number>”.
3. You are prompted to enter new login credentials for the system administrator of the AI NVR. 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 NVR 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 NVR.

The Dashboard panel of Server Management for the AI NVR is displayed.

9. Configure the basic settings for your new AI NVR in Server Management, including the hostname, time zone, and language. For more information see *Using Server Management* on page 23

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* on page 13.

Connect to the AI NVR (using Static IP)

You must use this procedure if:

- This is the first appliance that will run the ACC Server software in your security network, or
- Static IP addresses are assigned to all the devices managed by ACC software in your security network

After powering on the AI NVR:

1. Discover the appliance. Use File Explorer on a Windows computer or Finder® on a Macintosh computer.

   You are looking for a device labeled “AINVR-STD-xxTB-<serial number>” or “AINVR-VAL-xxTB-<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 39.

2. Click to connect to the device.

   Important: By default, the AI NVR 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 28.

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 NVR 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. If you are installing the first Avigilon appliance in your security network, use the procedure *Downloading and Installing the Latest ACC Client Software* on page 1 to install the ACC Client software on a network workstation or on the computer you are using to access the Server Management 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* on page 13.

Activate the ACC Software and Connect to Avigilon Cloud Services

After you have deployed your AI NVR , activate your ACC software and feature licenses and connect to Avigilon Cloud Services.

Activate ACC Software and Feature Licenses

You can activate, deactivate, and reactivate product or feature licenses. Licenses are called Product Keys in the ACC system, and Activation IDs in the licensing portal.

Important: When a new server is added to or removed from a multi-server site, the existing site licenses become inactive and must be reactivated to confirm system changes. See *Reactivating a License* on page 20

- **Initial ACC™ System Setup and Workflow Guide**
- **ACC 7 Help Center**

Printable versions of these guides are available on the Avigilon website: **avigilon.com/support/software/**.

Once your license is activated, you can immediately use the new licensed features.

Connect to Avigilon Cloud Services

After activating your ACC software, you can connect your ACC site to the cloud, which may require a subscription, and take advantage of the capabilities and features that provide centralized access across distributed systems.

To connect your site to Avigilon Cloud Services, see **help.avigilon.com/cloud**.

For information about the cloud services, see **Avigilon Cloud Services Support**.

You can start to back up the system settings for your new site in the ACC Client software after it is configured. These settings include the ACC password, and the settings for the camera connections. For more information on backing up the site and server configurations, see the *Avigilon ACC Client User Guide*.

Activating a License

Once your license is activated, you can immediately use the new licensed features.

> **Tip:** Finish organizing your multi-server site before activating a new license to avoid reactivating the site license each time a new server is added.

Online Activation

If you have internet access, use online activation. However, if your site is large and contains hundreds of licenses, the server may time out. See *Offline Activation* below instead.

1. In the New Task menu  , click **Site Setup**.
2. Select your new site, then click  .
3. Click **Add License...**.
4. Enter your product keys.

   If you copy and paste more than one comma-separated product key, the system will format it automatically.

   - To remove the last product key, click **Remove Last Key**.
   - To clear all the product keys, click **Clear**.
5. Click **Activate Now**.
6. Click **OK**.

Offline Activation

Offline licensing involves transferring files between a computer running the ACC Client software and a computer with internet access.

In the ACC Client:

1. In the New Task menu , click **Site Setup**.
2. Select your new site, then click .
3. Click **Add License...**.
4. Select the **Manual** tab.
5. Enter your product keys.

   If you copy and paste more than one comma-separated product key, the system will format it automatically.

   - To remove the last product key, click **Remove Last Key**.
   - To clear all the product keys, click **Clear**.
6. Click **Save File...** and choose where you want to save the `.key` file. You can rename the file as required.
7. Copy the `.key` file to a computer with internet access.

In a browser:

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 ACC Client software.

In the ACC Client:

1. In the License Management dialog box, click **Apply...**.
2. Select the `.bin` file and click **Open**.
3. Click **OK** to confirm your changes.

Reactivating a License

FOR ENTERPRISE EDITION

When servers are 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 ACC 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 NVR

To enable analytics processing on the video streams from cameras connected to the ACC site to be done by the AI NVR:

1. Open the ACC Client software and log in to the AI NVR.
2. In the New Task menu  , click **Site Setup**.
3. Select a server, then click **Server Analytics**  .
4. Select an analytics feature tab and then select the cameras to enable the feature on:
   - Classified Object Detection
   - Appearance Search
   - Face Mask Detection
   - Face Recognition

   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 AI NVR does not support that analytic or your site does not have the required analytics license.
5. Click in the option box next to a camera to select or deselect the camera to enable analytics processing by the AI NVR for that camera. An estimate of the resource cost is shown on the left of each camera row.

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

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

Using Server Management

Configure the AI NVR with Server Management, accessed from any ACC Client application or compatible browser on a workstation on the same network as the appliance. With Server Management you can configure the server settings.

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.

Open Server Management

From any network workstation with network access to the AI NVR, you can open Server Management:

- **Directly from the ACC Client software:**
  a. Start the ACC Client software.
  b. Log in to the site from the System Explorer.
  c. In the New Task menu , click **Site Setup**.
  d. 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 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 “AINVR-STD-xxTB-<serial number>” or “AINVR-VAL-xxTB-<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 39.
  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 IP address or hostname

1. Open a web browser and enter IP address or hostname of the AI NVR into the web browser to open the device sign in page:
   https://*<Device IP address >*|*<Device hostname>*/
   - IP address example: `https://169.254.100.100/`
   - Hostname example: `https://my_AvigilonDevice/`

   IP address or hostname are configured on the Device panel.

   If you forget the IP address or hostname, it is listed in the ACC Client software, in the server Setup tab.
2. 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.

Server Management Dashboard

ACC Server	Check the operating state of the ACC Server software: - **Running** in green - **Stopped** in red
	View site information: - Site Name - Server Name - Server Version
System	View the AI NVR 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
Storage	View information about the storage capacity of the device. When storage is on a RAID array of disks, a single virtual disk and the total storage capacity is listed. Otherwise, each storage disk and its storage capacity is listed. Click ⚙ to open the **Storage panel**.
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**.

Access Server Management Features

To...	Do...		See
Manage the services of the ACC Server	Expand the **ACC** section and...	...click on the **Server** panel	*Manage ACC Services* on page 33
Reboot the AI NVR.	In the **System** section and...	...click on the **Device** panel	*Manage Device Settings* on the next page
Upgrade the AI NVR firmware.			*Upgrade the Firmware* on page 31
Manage certificates.			*Manage Certificates* on page 28
Monitor and manage the storage on the device.		... click on the **Storage** panel	*Manage Storage* on page 34
Connect to cameras and the ACC Clients.		... click on the **Network** panel	*Connect the Device to Cameras and ACC Client Users* on page 37
Prepare service logs from the ACC Server. and system log files from the AI NVR for Avigilon Technical Support.	Click the **Logs** and...	... click on the **Server Logs** tab	*Provide Server Logs and System Logs for Support* on page 37
		... click on the **System Logs** tab	

Create NIC Teams

The AI NVR 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. *NIC Teaming Modes* on page 13.

> **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 NVR includes the ability to identify which network port on the back panel of your unit is linked to a network port selected in the Server Management page. For more information, see *Identifying your Network Ports* on page 40.

2. On the Network panel, click **New 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**.

   For more information on the mode options, see *NIC Teaming Modes* on page 13.

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.

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* below
Change the password for the AI NVR administrator.	**Password**	See *Change the AI NVR Administrator Password* below.
Install the latest version of the firmware on your device.	**Upgrade Firmware**	See *Upgrade the Firmware* on page 31.
Manage the certificates used by Server Management and the AI NVR.	**Certificates**	See *Manage Certificates* on the next page.

Change the AI NVR 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 NVR to Factory Default Settings* on page 43.

Manage Time Settings

Customize how the AI NVR 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.

   > **Tip:** To synchronize time with ONVIF devices (that is, non-Avigilon cameras), you can connect to port 123 on the AI NVR to use it as an NTP server.

   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.

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 NVR 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 NVR,
  - 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 NVRs 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 website: **partners.avigilon.com**. From a workstation connected to the Internet:

1. Navigate to **partners.avigilon.com** and download the appropriate AI NVR firmware.
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.

Reboot the AI NVR

You can reboot the AI NVR from Server Management:

1. Open the Device panel
2. On the **General** pane click **Reboot**.

   Monitor the progress of the device as it reboots from the **System** pane of Server Management Dashboard. For more information see *Using Server Management* on page 23).

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 NVR	Click **Reset**
Format the storage drive.	Click **Reinitialize** to delete all configuration and recorded video data.
Download and install the ACC Client software version provided with the AI NVR on the computer you are using to access Server Management.	Click **Download**. After the download is complete, open the installer as you would any application downloaded with a web browser to install the software.

> **Tip:** The version of the ACC Client software provided with the AI NVR firmware may not be the most recent. To ensure you are using the latest version of the ACC Client software for the ACC system used by your security team, see *Download and Install the Latest ACC Client Software* on page 16.

- Network Storage Management pane to enable ACC Client application users to archive video from the AI NVR. See *Enable ACC Client Users to Archive Video* below
- Service and RTP Ports panes to change the UDP and TCP ports used to communicate with the AI NVR:
  - 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.

Enable ACC Client Users to Archive Video

To allow users of the ACC Client application to archive video from the AI NVR:

1. From the navigation bar, open the **Server** panel.
2. In the Network Storage Management pane, click **Enabled**
3. From the Protocol drop down list, select one of the following:
    - **CIFS** — Common Internet file system. The network path is typically in this format: //*<hostname or IP>* / *<path>*
    - **NFS** — Network file system. The network path is typically in this format: *<hostname or IP>* : *<path>*
4. In the **Network Path** field, enter the path to the preferred video archiving location.
5. If the network location requires authentication, enter the credentials in the **Username** and **Password** fields.
6. Click **Apply**.

Manage Storage

On the **Storage** panel of the AI NVR you can:

- Monitor the storage capacity and the status of the virtual disks configured on the device on the Virtual Disks panel, and the physical disks installed on the device on the Physical Disks panel.
- Expand a virtual disk on the Virtual Disks panel to monitor the status of the physical disks that are members of that virtual disk.
- View details about each physical disk, including capacity, model, and serial number on the Physical Disks panel.
- Set the status of a physical disk to Offline before removing it from the appliance for replacement if it ever fails.

    Important: The storage physical disk is a hard disk drive (HDD) that must be replaced with an HDD of the same capacity.

Click **Storage** on the navigation bar to open the Virtual Disks and Physical Disks panels.

In the...	To...	You can...
Virtual Disks panel	View the capacity and status of a virtual disk	View information about the virtual disk, including its label, the RAID mode in use, and its capacity. When a virtual disk is: • Correctly working, **Ready** is displayed. • Not correctly working, one of several error states is displayed.
	Complete maintenance on a virtual disk	Click  to check consistency of the virtual disk.
	Monitor the status of the physical disk members of a virtual disk	Click  to display information about all the physical disks that are members of the virtual disk and  to hide the information. When the member disks are displayed, the status of each disk is listed. When a physical disk is: • Correctly working, **Ready** is displayed. • Not correctly working, one of several error states is displayed.
Virtual Disks and Physical Disks panel	Prepare to replace a physical disk	Click  . You are prompted to **Eject** or **Cancel**. The status changes to **Offline** and  changes to  , indicating all services have stopped. For more information on replacing a physical disk, see *Replace Hard Disk Drives* below.
Physical Disks panel	View the capacity and status of each physical disk.	View information about each physical disk, including its label, capacity, model, serial number and status is listed. When a physical disk is: • Correctly working, **Ready** is displayed. • Not correctly working, one of several error states is displayed.
	Rebuild the virtual disk after replacing a failed member physical disk.	Click  to rebuild the virtual disk. **Note:** An HDD in a RAID that has been taken offline has to be rebuilt to return it to service.

Replace Hard Disk Drives

The hard disk drives (HDDs) on the AI NVR are set up in a RAID configuration. This allows information to be

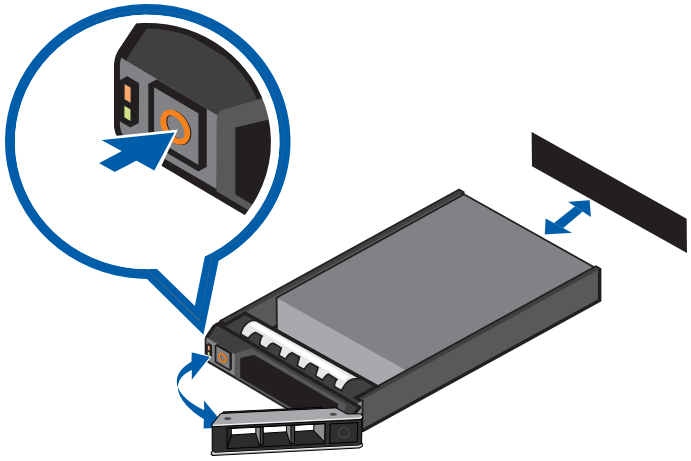
recorded across several HDDs. If one HDD fails on an AI NVR VAL or up to two HDDs fail on an AI NVR STD, there is enough information on the other HDDs for the recorder to continue recording video. This allows you to replace a failed HDD without any downtime. If two disks have failed on an AI NVR STD, they have to be replaced one at a time.

To replace a failed HDD:

1. In the Server Management page, open the Storage panel.
2. In the Physical Disks panel, click . You are prompted to **Eject** or **Cancel**. The status changes to **Offline** and changes to , indicating all services have stopped.

   Important: An HDD in a RAID that has been taken offline has to be rebuilt to return it to service. If you decide not to remove the HDD after ejecting it, click to rebuild the RAID with this HDD. The progress of the rebuilding is displayed in the Physical Disks panel. This may take several hours.

3. You can now remove the HDD from the appliance:
   1. Locate the failed hard drive at the front of the recorder.

   2. Press the release button on the front left of the hard drive.
   3. When the handle is released, pull the hard drive out of the recorder.
   4. Remove the four screws from the side of the hard drive carrier.
   5. Lift the failed hard drive out of the carrier.
   6. Insert a new hard drive into the carrier then screw it into place. The hard drive connectors should face the back.
   7. When the hard drive is secured in the carrier, insert the hard drive back into the recorder.
   8. Once the hard drive is inserted all the way in, push the handle against the hard drive to lock it into place.

   The AI NVR immediately starts rebuilding the hard drive. The progress of the rebuilding is displayed in the Physical Disks panel. This may take several hours.

Connect the Device to Cameras and ACC Client Users

When connecting an ONVIF device to the camera network, configure it to use the appliance as its time/NTP server.

On the Network panel, you can configure the network connections for the appliance. Four network connections are supported on the AI NVR STD models and two network connections on the AI NVR VAL models. Use one connection for the network where the AI NVR 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 NVR with the ACC Client software connect to the appliance through this network. Use another network connection to connect to the camera network monitored by your security team.

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.

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.

Troubleshooting

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 41 for more information.
- Using File Explorer (Windows) or Finder (Apple)

  You are looking for a device labeled “AINVR-STD-xxTB-<serial number>” or “AINVR-VAL-xxTB-<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: AINVR-STD -<serial number> or https://AINVR-VAL-<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 https://AINVR-STD-<serial number> or https://AINVR-VAL-<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 NVR acquires an IP address on the network through DHCP. If you need to set up the AI NVR to use a static IP address or any specific network configuration, see the *Connect to the AI NVR (using Static IP)* on page 17 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.

Identifying your Network Ports

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

1. Open the Network panel on the Server Management 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 NVR. 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

Diagnostic Indicators

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

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

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

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

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

Power Status Indicators

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

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

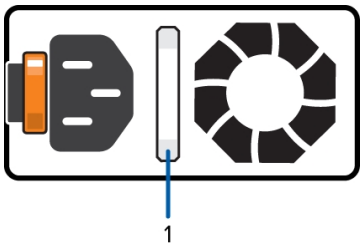


Figure 7: (1) The power status indicator.

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.

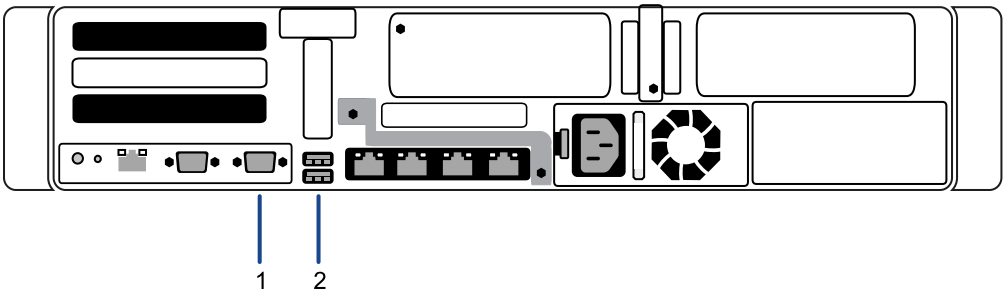
Restore the AI NVR to Factory Default Settings

You may have to restore the AI NVR 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 and recorded data is deleted when you restore the AI NVR 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 NVR 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 NVR has completed the reboot, it must be completely reconfigured, starting from *Download and Install the Latest ACC Client Software* on page 16.

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**.