avigilon™
a Motorola Solutions Company

User Manual

Avigilon NVR4X Premium - FIPS Series

NVR4X-PRM-FIPS-64TB, NVR4X-PRM-FIPS-96TB,
NVR4X-PRM-FIPS-128TB, and NVR4X-PRM-FIPS-157TB

Avigilon Corporation
avigilon.com

PDF-NVR4FIPS-A

Revision: 1 - EN

20201007

Table of Contents

Introduction

The Avigilon Network Video Recorder is preloaded with the Avigilon Control Center software and is configured for maximum performance and reliability. The Network Video Recorder can be easily integrated into any existing Avigilon security system, or act as the base of a new site.

Before You Start

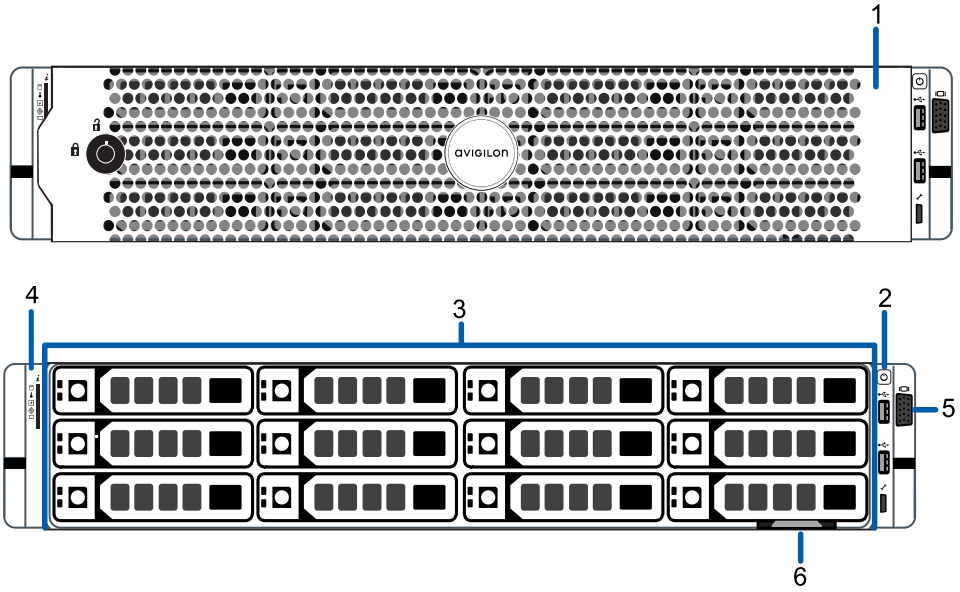
Avigilon recommends the use of an uninterruptible power supply (UPS) system to protect your video surveillance system hardware. A UPS system is used to protect critical equipment from mains supply problems, including spikes, voltage dips, fluctuations and complete power failures using a dedicated battery.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

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

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

Overview

Front View



1. **Bezel**

   Protects against unauthorized physical access to the hard drives.

2. **Power button**

   Controls the power supply to the recorder.

3. **Hard drives**

   Provides access to hot-swappable hard drives. There are LED indicators on each hard drive.

   Some drives may contain an empty hard drive tray.

4. **Diagnostic indicators**

   Provides information about system operations.

   For more information, see *LED Indicators* on page 17.

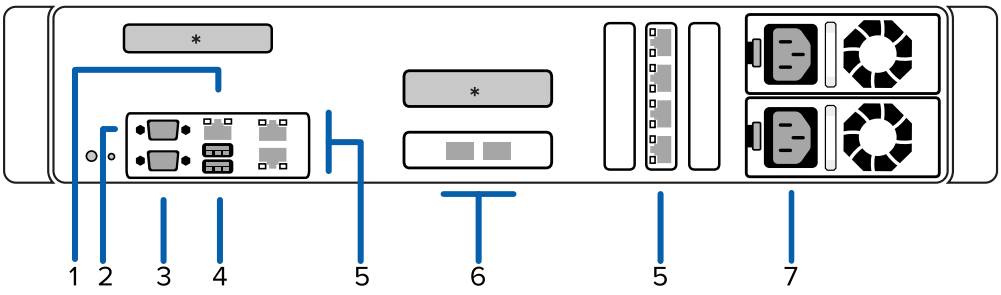
5. **Video connector**

   Accepts a VGA monitor connection.

6. **Pull-out information tab**

   Provides the product service details and support information.

Back View



* = Expansion slots in use

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

   Accepts an OOBM RJ-45 connection. Port is disabled when shipped.

2. **Serial connector**

   Accepts connections to serial devices.

3. **Video connector**

   Accepts a VGA monitor connection.

4. **USB connectors**

   Accepts USB connections to external devices.

5. **RJ-45 1 Gbps Ethernet ports (6)**

   Accepts Ethernet connections to multiple networks.

6. **Two(2) SFP+ 10 Gbps Ethernet ports**

   Accepts Ethernet connections to multiple networks.

7. **Power supply (2)**

   Two hot swappable redundant power supply.

Installation

Package Contents

Ensure the package contains the following:

- Avigilon Network Video Recorder
- Rack sliding rail assembly kit
- Cable management arm assembly kit
- Bezel and key
- Blank USB key for OS recovery image
- Power cables (may be provided in a separate box)

Installing the Sliding Rack Rails and Cable Management Arm

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

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

Connecting Cables

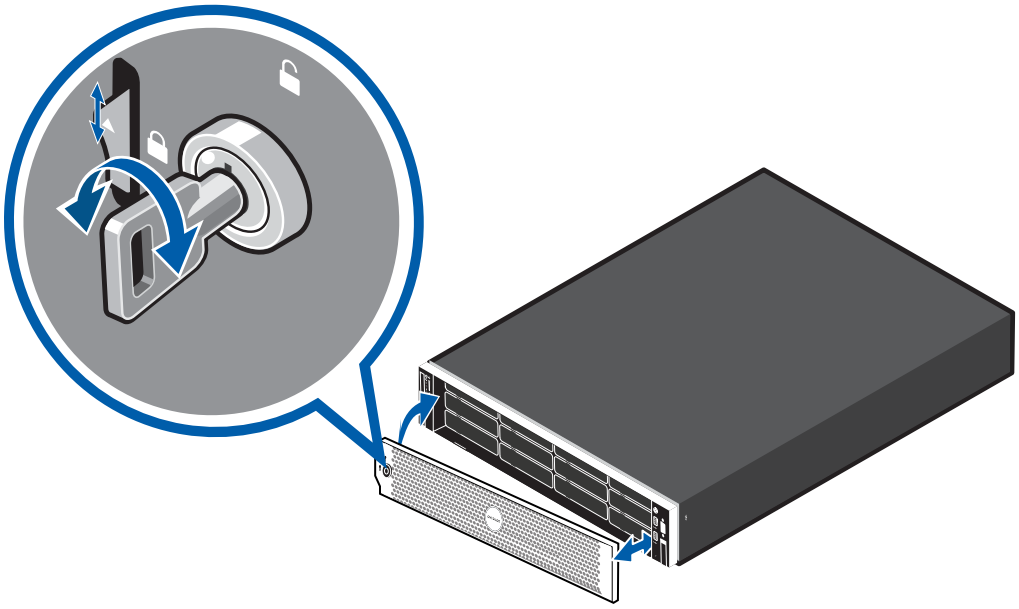
Refer to the diagrams in the Overview section for the location of the different connectors. Make the following connections as required:

1. Connect a KVM switch or separate keyboard, mouse and monitor to the recorder.
    - The keyboard and mouse can be connected to any USB port on the recorder.
    - The monitor can be connected to any video connector at the front or back of the recorder.
2. Connect the recorder to your network by plugging an Ethernet cable into one of the Ethernet ports.
3. Connect a power cable to each power supply at the back of the recorder.
4. Press the power button on the front of the recorder. Check that the recorder LED indicators display the correct status. For more information on the different LED status indicators, see *LED Indicators* on page 17.

Installing 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.

Logging into Windows Server for the First Time

After the recorder powers up, you will need to configure the Windows operating system for the first time:

1. On the first screen, scroll through the list and select your preferred language.

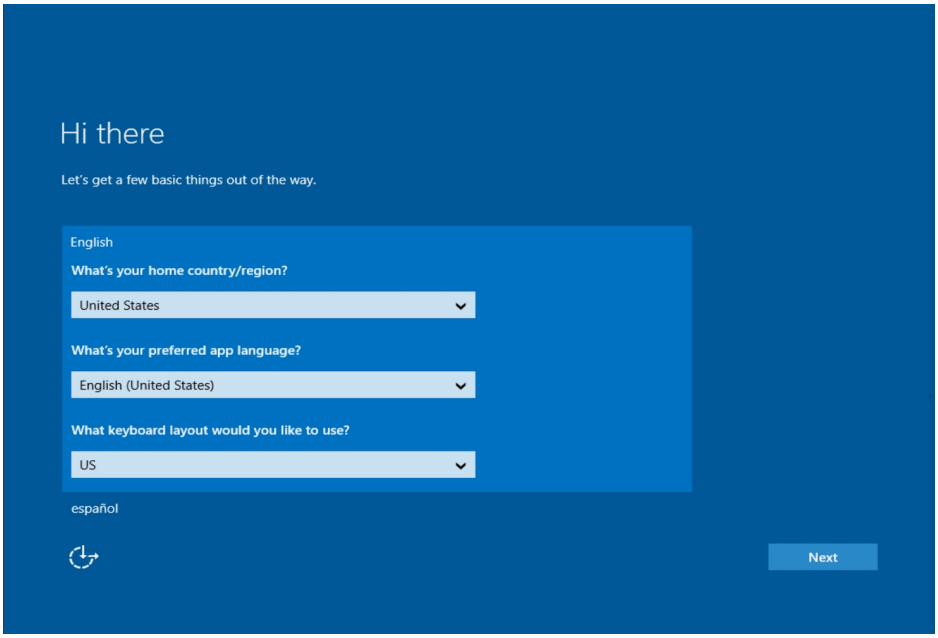


Figure 1: The language selection screen during initial Windows software set up. (Used with permission from Microsoft.)

2. Select the country/region, preferred app language, and keyboard layout, then click **Next**.
   NOTE: If a language other than English is selected, the server will restart. This is a normal Windows behavior, please proceed with step 3 once the server has finished restarting.
3. The End User License agreements are displayed. Review the terms then click **Accept**.
4. On the Customize settings screen, set a password for the local administrator account.
   The password must meet the following complexity and policy requirements:
   - Have a minimum length of 14 characters.
   - Have at least one of each of the following: lowercase character, uppercase character, symbol, and number.
   - You cannot reuse your last 24 passwords.
   - The password will expire in 60 days.
   - The password must be a minimum age of 1 day before it can be changed.
5. Press Ctrl+Alt+Delete to unlock and login:
   - User name: *Administrator*
   - Password: created in the previous step.
6. Once logged in, the recorder will go through initial system setup, and then start Bitlocker encryption, some configuration and applying of hardening policies.
7. The Setup dialog will start configuring the system storage. This process may take up to 5- 20 minutes depending upon the size of the storage volume.
8. The Avigilon Control Center Software will start running automatically and the NVR Analytics Kit will be configured.

9. Once the setup procedure is complete, the system will restart.

   Important: After this reboot, as part of the applied hardening policies, your *Administrator* account user name will have been automatically changed to ***MotoSec***.

10. Login with the *MotoSec* user name and the password you created previously. The user name is not case sensitive.

    Once logged in, proceed to deploying the recorder using an active directory or standalone. For more information, see the **ACC Initial System Setup and Workflow Guide**.

    To continue protecting your system, you will need to create a backup Bitlocker recovery key, create a USB recovery stick, and disable USB ports. For more information on these security procedures, see the **Avigilon System Hardening Guide**.

Connecting to ACC Software

Once you have deployed your NVR, you should activate your ACC software.

Activating and Configuring ACC Software

- **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/**.

Troubleshooting

Network Configuration

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

Checking System Health

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

Operating System Recovery by External USB

If you need to recover the Windows operating system on the Network Video Recorder you will need to have created a USB Recovery Image during recorder setup. For more information, see **Hardening the Avigilon NVR4X Premium - FIPS Series**.

The general steps are:

1. Plug the USB recovery device into the recorder.

   Note: USB ports must be enabled to complete the OS recovery. See **Hardening the Avigilon NVR4X Premium - FIPS Series** for more information on enabling USB ports.

2. Reboot the NVR.
3. Press the F11 key while the server is booting up to open the Boot Manager.
4. Select **One-shot UEFI Boot Menu** from the Boot Manager Main Menu.
5. On the UEFI Boot menu, select to boot from the USB recovery device.
6. Click **Recover** on the Recovery window.
7. Wait for the recovery process to complete. This may take 20-30 minutes. Once the recovery process is complete, it will ask you to remove the USB and reboot the NVR.
8. Go through the initial setup process. For more information, see *Logging into Windows Server for the First Time* on page 5.

Unlocking the Storage Volume

After the OS recovery is complete, you will need to unlock the storage volume that has been encrypted with BitLocker.

1. Plug the USB recovery device into the recorder.

   Important: The BitLocker recovery key files (BEK files) should have been backed up to your USB device as part of completing the NVR setup. For more information, see **Hardening the Avigilon NVR4X Premium - FIPS Series**.

3. Open Windows Explorer and locate the storage volume with the locked icon.
4. Click the storage volume. Windows will ask you for a Recovery Key. Click to **Load Key From USB Drive**. The storage volume should now be unlocked.
5. Click on the **Windows Start** button and type *Manage BitLocker*. Open the Manage BitLocker application.
6. Click on **Storage** and select **Turn on auto-unlock**.

Re-installing the ACC Software

Download and install your version of the ACC software on the NVR. After installing, the system will start configuring system storage and hardening of the recorder.

Replacing the Motherboard

Your recorder uses a Trusted Platform Module (TPM) to secure your hardware with integrated cryptographic keys. To maintain security, the TPM cannot be reused with a new motherboard if the motherboard needs to be replaced. If the motherboard needs to be replaced, this will require a new TPM.

You will be required to enter your Bitlocker recovery key when booting to the Operating system after replacing the motherboard. As part of the initial setup, administrators should backup their Bitlocker recovery key. This key can then be used to restore Bitlocker on a new TPM if the motherboard is replaced.

Important: Make sure you have the Bitlocker recovery key prior to replacing the motherboard. It is also advised that you decrypt the hard drive prior to replacing the motherboard.

1. After replacing the motherboard and signing in with the Bitlocker recovery key, navigate to Control Panel > System and Security > Bitlocker Drive Encryption.
2. Choose to Suspend protection from the Manage Bitlocker window. A message should appear stating that Bitlocker protection has been suspended.
3. Reboot the system and go into the BIOS to enable and activate the TPM.
4. Click Apply and Exit.
5. Boot back into Windows and ensure that Bitlocker is turned back on in the Bitlocker manager console.

Advanced Features

Checking System Health

You can check your system health through the ACC Client Site Health or with the Server Administrator software.

ACC Client Site Health

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

Server Administrator Software System Health

The Server Administrator software is pre-installed on the recorder. The software provides information about the recorder's system operation status, and gives you remote access to the recorder for recovery operations.

Important:
To comply with hardening policies, the FIPS Series NVR will not allow the Server Administrator software to open with its default self-signed certificate. To use the Server Administrator software, you have two options:

- To fix the self-signed certificate: generate a certificate signing request, get it signed by a trusted certificate authority, and upload the CA-signed certificate to the Server Administrator. For more information, see the **Server Administrator Software Certificate Management section of the System Hardening Guide**.
- To workaround the self-signed certificate: use the Windows Registry Editor to edit the key to allow temporarily allow self-signed certificates. Using this method will leave your system exposed until you change the registry key back to its previous state. For more information, see the **Server Administrator Software Registry Key section of the System Hardening Guide**.

If one of the LED indicators on the recorder is flashing an error warning, the Server Administrator will display details about the problem. For more information about the LED indicators, see *LED Indicators* on page 17.

1. Open the Server Administrator.
    - To open the Server Administrator locally, double-click the **Server Administrator** shortcut icon on the desktop.
    - To open the Server Administrator remotely, open a web browser and enter this address: `https://<recorder IP Address>:1311/`.

      For example: `https://192.168.1.32:1311/` or `https://localhost:1311/`.

    If you are using an intranet connection, your browser may display an error message. Allow the browser to ignore the certificate warnings.
2. If asked to log in, enter the Windows software administrator username and password that was configured for the recorder.
3. On the Server Administrator home page, the health of the system components are displayed in the workspace on the right.
    - To see the health of other system components, expand and select a different component from the System Tree on the left.
    - The table displayed in the workspace lists system components and their status:

	The system component is running normally.
	The system component has a non-critical warning.
	The system component has a critical failure.
	The system component status is unknown.

    - To see the details of a system component, select the system component from the workspace.

The Server Administrator is also used to customize the Redundant Array of Independent Disks (RAID) settings, assign a hot spare and remotely monitor the system health. For more information about the features in the Server Administrator, see the Help system provided in the software.

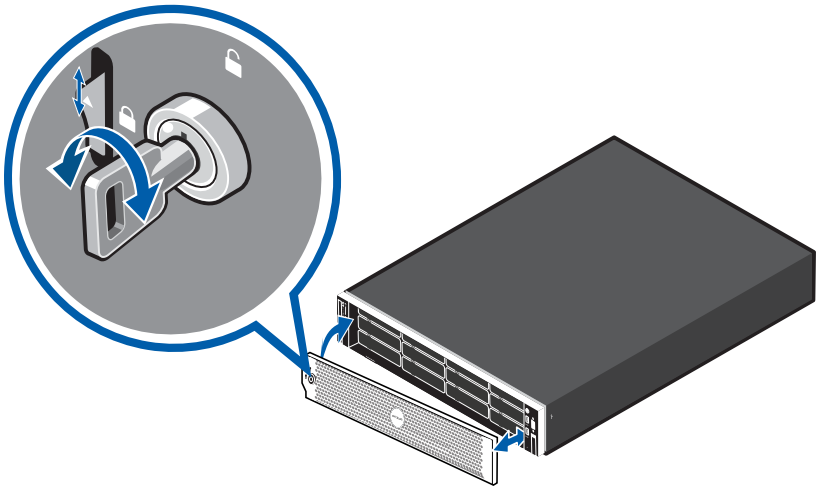
Replacing a Hard Drive Blank

The hard drives on the Network Video Recorder are set up in a RAID configuration. This allows information to be recorded across several hard drives.

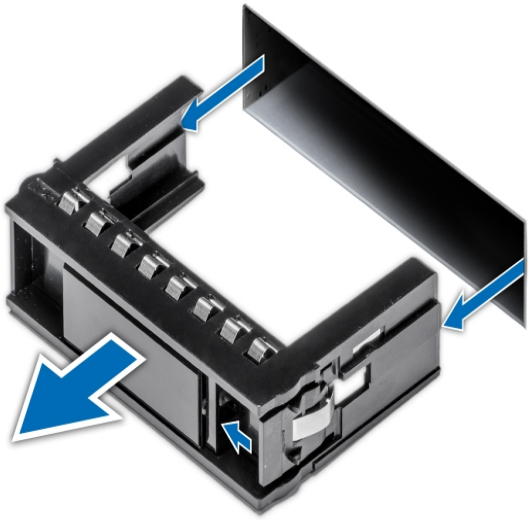
If one or two hard drives fail, there is enough information on the other hard drives for the recorder to continue recording video.

Depending on the recorder model, there may be hard drive blanks at the front of the recorder. You can replace the blanks with hard drives as required.

1. Remove the bezel.



   a. Unlock the bezel.
   b. Push the release button next to the lock.
   c. Pull the left end of the bezel then unhook the right end to remove the bezel.
2. Press the release button and slide the blank out of the hard drive slot.



3. Insert the hard drive all the way into the recorder then push the handle against the hard drive to lock it into place.
4. Open the Server Administrator application and expand the System Tree.

   The new hard drive should be automatically added to the Physical Disks list. The list is typically available here: **System > Storage > PERC H740P Mini (Embedded) > Connector 0 (RAID) > Enclosure (Backplane) > Physical Disks**.

5. Assign a task to the new hard drive or allow it to exist as an extra storage drive.

   It is recommended to use the new hard drive as a hot spare. Hot spares are hard drives that are available on standby in the event of a hard drive failure in the RAID. If that occurs, you can configure the system to automatically redirect recording to the unused hard drive.

   To assign the new hard drive as a hot spare:

   a. In the Task list, select **Assign and Unassign Global Hot Spare**.
   b. Click **Execute**.

If the new hard drive is not displayed in the Server Administrator, try one of the following:

- Refresh the browser.
- Reboot the recorder.

Replacing Hard Drives

The operating system and the Avigilon Control Center software are mirrored on two hard drives at the back of the recorder. If one of the hard drives fail, you can replace the failed drive while the recorder continues to run from the other.

If your recorder is still under warranty, contact Avigilon Technical Support to replace the failed hard drive.

If more than two hard drives fail at the same time, contact Avigilon Technical Support immediately for recovery instructions.

Only replace a hard drive if the hard drive LED indicator and the Server Administrator displays an error.

1. Open the Server Administrator.
2. Check which hard drive has failed, then disconnect the drive through the Server Administrator software.

   Hard drives are installed at the front, back and in the middle of the recorder. Be sure you can identify which hard drive needs to be replaced.

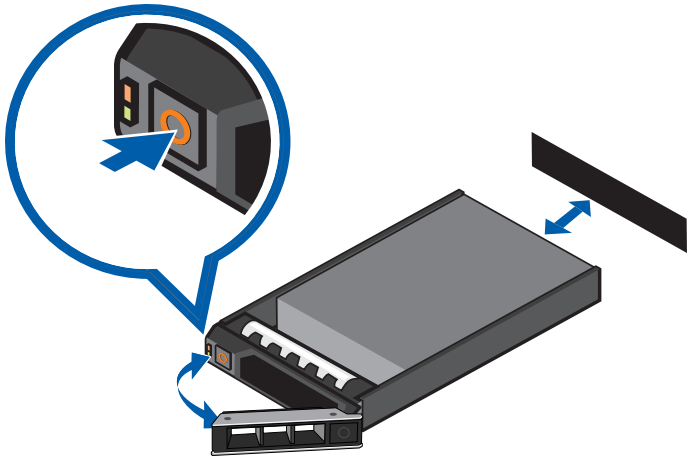
3. If you are replacing a hard drive at the center of the recorder, shut down the recorder then disconnect all cables.

   Note: Skip this step if you plan to hot-swap a hard drive at the front or back of the recorder.

4. Remove the bezel.
5. Depending on where the hard drive is located, perform one of the following procedures:

Replacing Front or Back Hard Drives

1. Locate the failed hard drive at the front or back 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.

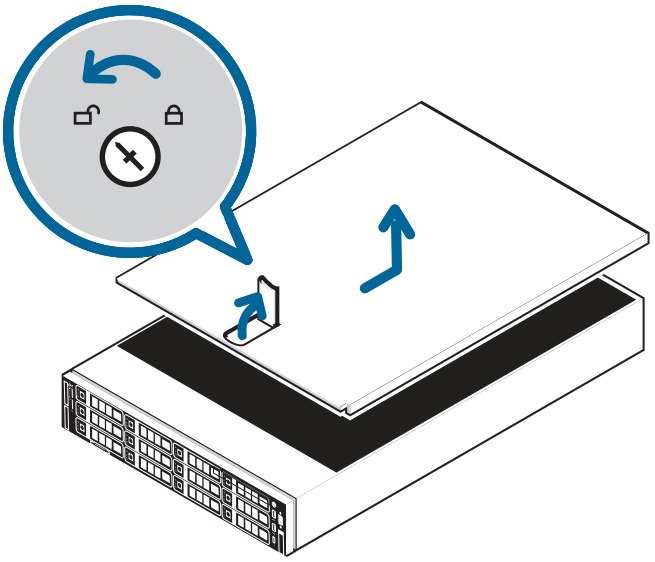
The recorder immediately starts rebuilding the hard drive. The progress is displayed in the Server Administrator. This may take several hours.

Replacing Center Hard Drives

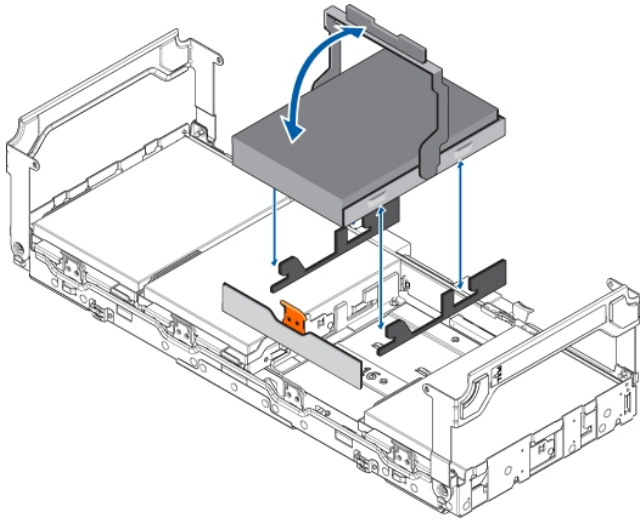
To replace a hard drive stored in the middle of the recorder, complete the following steps:

1. At the top of the recorder, unlock the latch release then lift and rotate the latch towards the back of the recorder.

   The cover slides back and is released from the recorder body.



2. Hold the cover from both sides and lift it off the recorder.
3. Locate the failed hard drive on the center hard drive tray.
4. Lift the handles on either side of the hard drive tray.



5. Press the orange release tab on the hard drive tray then lift up the hard drive carrier handle to release the hard drive.
6. Hold the handle and lift the hard drive out of the tray.
7. While holding the handle, pull the edges of the carrier away from the hard drive to remove the failed hard drive from the carrier.
8. Align the slots on the new hard drive to the tabs on the hard drive carrier.

9. Pull the edges of the carrier over the slots on the hard drive.
10. Place the new hard drive into the tray and push the handle down until the hard drive clicks into place.
11. Fold down the handles on the hard drive tray. Close and lock the recorder cover.
12. Reconnect all the cables to the recorder and power it.

After the operating system starts up, the recorder immediately starts rebuilding the hard drive. The progress is displayed in the Server Administrator. This may take several hours.

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 recorder is powered.

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

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

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

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

Power Status Indicators

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

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

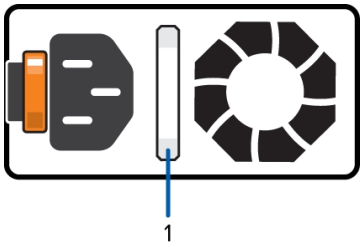


Figure 2: (1) The power status indicator.

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.

Network Link Status Indicators

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

Figure 3: (1) Link LED. (2) Connection activity LED.

LED Indicator	Description
Off	The recorder is not connected to a network.
Link LED — green **Connection Activity LED — blinking green**	The recorder is connected to a network at the maximum port speed.

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

Hard Drive RAID Status Indicators

Each hard drive has its own set of LED indicators to show its activity and status.

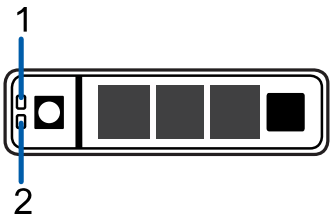


Figure 4: (1) Status LED. (2) Activity LED.

The Activity LED flashes green when the hard drives are working. The following table describes what the Status LEDs indicate:

LED Indicator	Description
Green	The hard drive is online.
Off	The hard drive is disconnected from the recorder.
Two short green flashes every second	The system is identifying a new hard drive, or preparing a hard drive for removal.
Flashes green, orange, then off	The hard drive is predicted to fail.
Four short orange flashes per second	The hard drive has failed.
Flashes green slowly	The hard drive is rebuilding.
Blinks green for three seconds, orange for three seconds, and off for six seconds	The hard drive rebuild has been aborted.

Limited Warranty and Technical Support

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

Warranty service and technical support can be obtained by contacting Avigilon Technical Support:

avigilon.com/contact.

For More Information

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

Technical Support

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