



**NVR6-PRM-
FIPS-FORM-
D-72TB
Network
Video
Recorders**



MOTOROLA SOLUTIONS NVR6-PRM-FIPS-FORM-D-72TB Network Video Recorders User Guide

[Home](#) » [Motorola Solutions](#) » **MOTOROLA SOLUTIONS NVR6-PRM-FIPS-FORM-D-72TB Network Video
Recorders User Guide** 

Contents

- [1 MOTOROLA SOLUTIONS NVR6-PRM-FIPS-FORM-D-72TB Network Video
Recorders](#)
- [2 Product Information](#)
- [3 Product Usage Instructions](#)
- [4 Models](#)
- [5 Introduction](#)
- [6 Overview](#)
- [7 Package Contents](#)
- [8 Installation](#)
- [9 Maintenance](#)
- [10 LED Indicators](#)
- [11 For More Information](#)
- [12 Limited Warranty](#)
- [13 Documents / Resources](#)
 - [13.1 References](#)



MOTOROLA SOLUTIONS

MOTOROLA SOLUTIONS NVR6-PRM-FIPS-FORM-D-72TB Network Video Recorders



Product Information

The Avigilon NVR6 Premium Form D FIPS Series is preloaded with Avigilon Control Center (ACC) software and is configured for exceptional performance and reliability. It can be easily integrated into any existing Avigilon surveillance system or act as the base of a new site.

Specifications

- NVR6-PRM-FIPS-FORM-D-72TB
- NVR6-PRM-FIPS-FORM-D-96TB
- NVR6-PRM-FIPS-FORM-D-120TB
- NVR6-PRM-FIPS-FORM-D-160TB
- NVR6-PRM-FIPS-FORM-D-200TB

Product Usage Instructions

Installation

Follow these steps for installation:

1. Connect Cables
2. Install the Sliding Rack Rails and Cable Management Arm
3. Install the Bezel

Configuration

To configure the operating system:

1. Log into Windows Server for the First Time
2. Activate the ACC Software and Connect to Avigilon Cloud Services
3. Activate ACC Software and Feature Licenses
4. Connect to Avigilon Cloud Services (Non-FIPS Compliant)
5. Reactivating a License

Troubleshooting

If you encounter issues, refer to the troubleshooting section for guidance on network configuration, monitoring system health, operating system recovery, storage volume unlocking, software reinstallation, and motherboard replacement.

Maintenance

Regular maintenance includes checking system health, ACC client site health, and server administrator software system health. Guidelines for replacing hard drives and components are also provided.

Front View Features

The front view of the NVR6 Premium Form D FIPS Series includes:

- Bezel lock for physical access protection
- Diagnostic indicators for system operations
- System health and identification button for system status
- The power button for controlling the power supply
- Video connector for VGA monitor connection
- USB 2.0 port for external devices
- iDRAC Direct micro USB port and LED indicator for iDRAC connection
- Front hard drive bay with hot-swappable drives and LED indicators

FAQ

- **How can I troubleshoot network configuration issues?**

If you are facing network configuration problems, check the settings on your NVR6 device and ensure proper connectivity with other network components.

- **Can I replace hard drives on my own?**

Yes, the user manual provides guidelines for replacing hard drives and components. Follow the instructions carefully to ensure successful replacement.

Models

- NVR6-PRM-FIPS-FORM-D-72TB
- NVR6-PRM-FIPS-FORM-D-96TB
- NVR6-PRM-FIPS-FORM-D-120TB
- NVR6-PRM-FIPS-FORM-D-160TB
- NVR6-PRM-FIPS-FORM-D-200TB

Copyright

© 2024, Avigilon Corporation. All rights reserved. AVIGILON, the AVIGILON logo, AVIGILON CONTROL CENTER, and ACC are trademarks of Avigilon Corporation. Microsoft and Windows are trademarks of the Microsoft group of companies. Dell is a trademark of Dell Inc. Other names or logos mentioned herein may be the trademarks of their respective owners. The absence of the symbols ™ and ® in proximity to each trademark in this document or at all is not a disclaimer of ownership of the related trademark.

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.

Introduction

The Avigilon Network Video Recorder (NVR6 Premium Form D – FIPS Series) is preloaded with Avigilon Control Center (ACC) software and is configured for exceptional performance and reliability. The Network Video Recorder can be easily integrated into any existing Avigilon surveillance 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 a 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

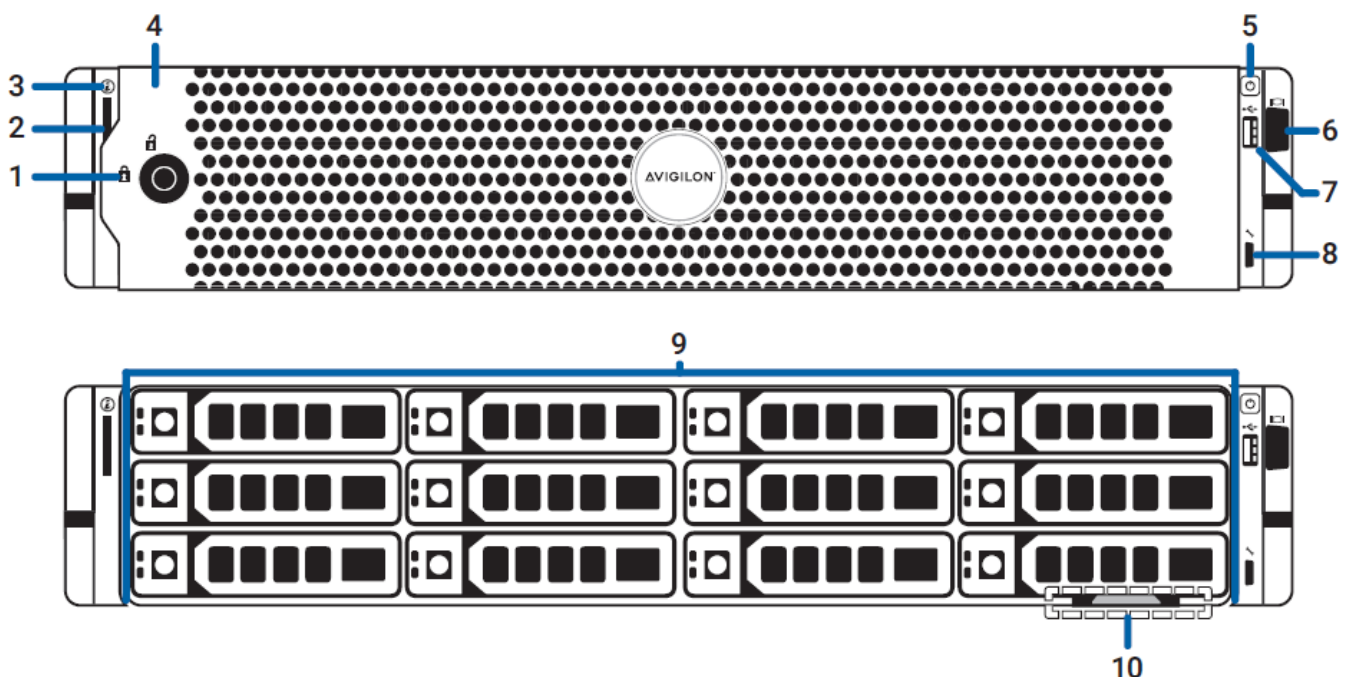


Figure 1: Front view of NVR6 Premium Form D – FIPS Series with the front bezel removed

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 on page 19.

3. System health and system identification button

- Displays the system's health. Also identifies a recorder 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 Install the Bezel.

5. Power button

Controls the power supply to the recorder.

6. Video connector

Accepts a VGA monitor connection.

7. USB 2.0 port

Accepts USB connectors to external devices.

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. Front hard drive bay

- Provides access to hot-swappable hard drives. There are LED indicators on each hard drive.
- Some drives may contain an empty hard drive tray.

10. 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

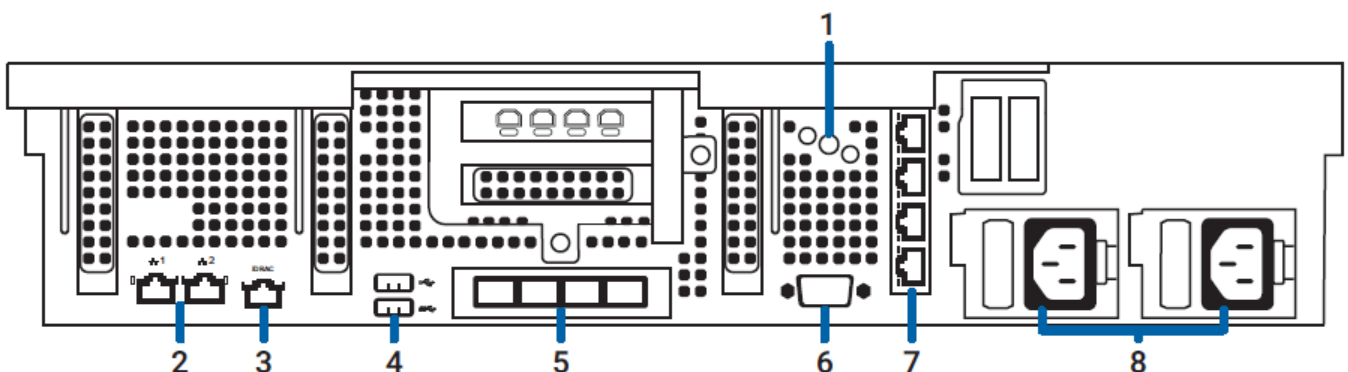


Figure 2: Back view of NVR6 Premium Form D – FIPS Series

1. System identification button

Identifies a recorder 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](#).

2. **Two (2) 1 Gbps Ethernet ports**

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

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

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

4. **Keyboard port and mouse port**

Accepts connectors to a keyboard and mouse.

5. **Four (4) 10/25 GbE SFP 28 Ethernet ports**

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

6. **Video connector**

Accepts a VGA monitor connection.

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

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

8. **Power supply connector**

Accepts a power supply connection.

Package Contents

Ensure the package contains the following:

- Avigilon NVR6 Premium Form D – FIPS Series Recorder
- Rack sliding rail assembly kit
- Cable management arm assembly kit
- Bezel and key
- Blank USB key for OS recovery image
- Power cables
 - C13 / C14
 - NEMA 5-15P / C13

Installation

Connect 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. For out-of-band management access and functionality, connect the Ethernet cable to the OOBM connector.
4. Connect a power cable to each power supply at the back of the recorder.
5. 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.

Install the Sliding Rack Rails and Cable Management Arm

If the recorder will be mounted in a server rack, install the Sliding Rack Rails and the Cable Management Arm

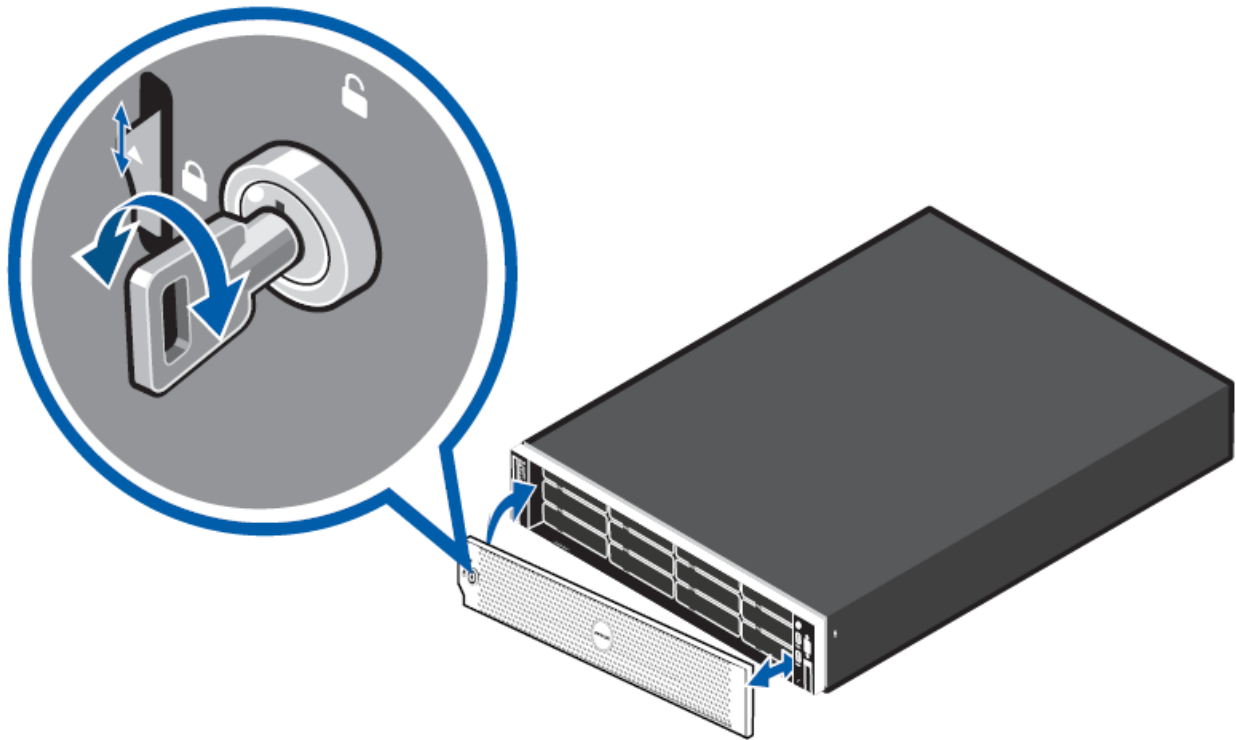
(CMA) provided in the recorder package. Follow the procedures outlined in the Rack Installation Instructions and the CMA Installation Instructions provided in the assembly kits.

NOTE

When rack-mounting the recorder, 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 recorder 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 NVR6 Premium Form D – FIPS Series 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.

Configure the Operating System

Configure the preloaded Windows Server 2019 operating system.

Log 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.

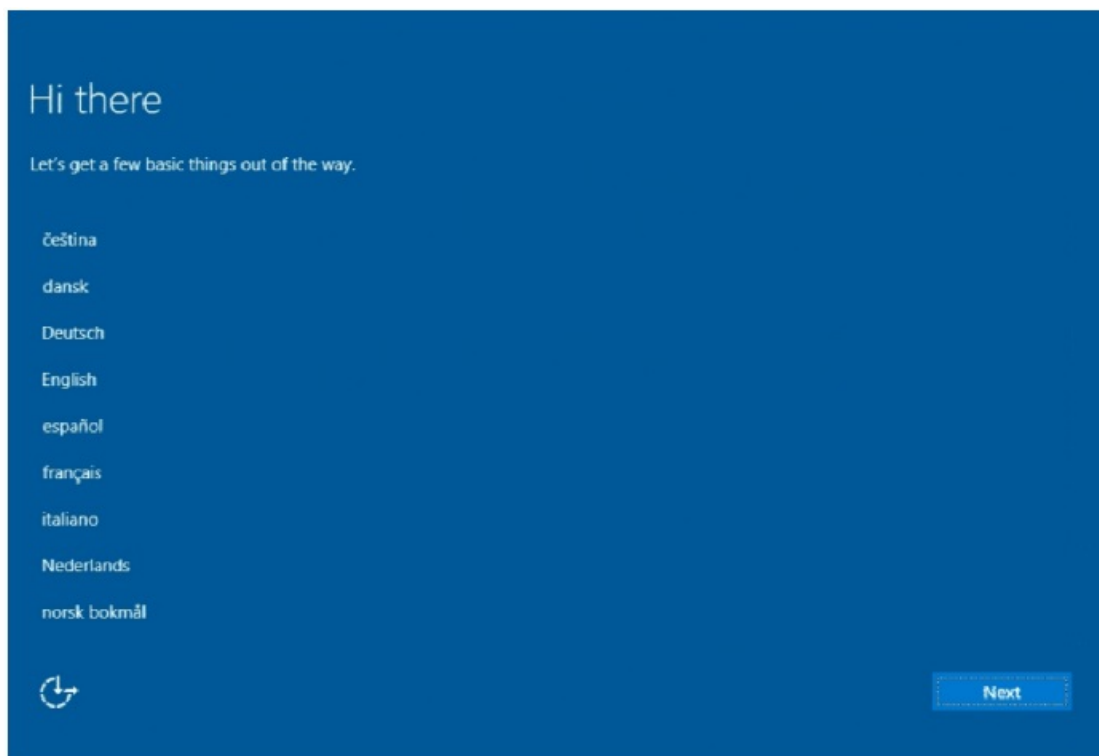


Figure 3: The language selection screen during initial Windows software setup. (Used with permission from Microsoft.)

2. Select the country/region, preferred app language, and keyboard layout, and then click Next.

NOTE

If a language other than English is selected, the server will restart. This is normal Windows behavior. Proceed with step 3 once the server has finished restarting.

3. The End User License agreements are displayed. Review the terms and click Accept.
4. On the Customize settings screen, set a password for the local administrator account and click Finish. The password should:
 - Have a minimum length of 7 characters.
 - Meet complexity requirements. See <https://technet.microsoft.com/en-ca/library/cc956977.aspx> for details.
 - You cannot reuse your last 24 passwords.
 - The password will expire in 42 days.
5. Press Ctrl+Alt+Delete to unlock and type in the credentials created in the previous step.
6. After you are logged in, the recorder will go through the initial system setup.
7. The Setup dialog will start configuring the system storage. This process may take up to 30 minutes depending on the size of the storage volume.
8. After 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.

9. Log in with the MotoSec user name and the password you created previously. The user name is not case-sensitive.
 - Once logged in, proceed to deploy 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 [Securing Servers section of the Avigilon System Hardening Guide](#).

Proceed to activate the license for the Avigilon Control Center software on your Network Video Recorder.

Activate the ACC Software and Connect to Avigilon Cloud Services

After you have deployed your NVR6 Premium Form D – FIPS Series recorder, activate your ACC software and feature licenses and, optionally, connect to Avigilon Cloud Services.

WARNING

Enabling Cloud Services on a FIPS server will cause the server to lose its FIPS compliance.

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](#).

- [Initial ACC™ System Setup and Workflow Guide](#)
- [ACC 7 Help Center](#)

Printable versions of these guides are available on the Avigilon website: avigilon.com/product-documentation. Once your license is activated, you can immediately use the new licensed features.

Connect to Avigilon Cloud Services (Non-FIPS Compliant)

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/avigilon-unity/video/cloud.


For information about the cloud services, see help.avigilon.com/cloud. 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.

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:

- Select the Manual tab.
- Click Save File... and choose where you want to save the .key files.
- 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.
- In the License Management dialog box, click Apply....
- Select the .bin file and click Open.
- Click OK to confirm your changes.

Troubleshooting

Network Configuration

By default, the NVR6 Premium Form D – FIPS Series acquires an IP address on the network through DHCP. If you need to set up the NVR6 Premium Form D – FIPS Series to use a static IP address or any specific network configuration, see the Windows Help and Support files for more information.

WARNING

Enabling Cloud Services on a FIPS server will cause the server to lose its FIPS compliance.

Monitoring System Health

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

Operating System Recovery By Avigilon Recovery Partition

If you need to recover the Windows operating system, the NVR6 Premium Form D – FIPS Series includes an onboard recovery partition that is separate from the operating system partition. The advantage of using the Avigilon recovery partition is that you do not need an internet connection to download the recovery image and you do not need to create a bootable USB recovery device.



IMPORTANT

Your operating system drive will be erased and restored to factory settings. Before you proceed with operating system recovery, complete any necessary backups of custom ACC configuration and video recordings.

NOTE

After operating system recovery, you need to reinstall the previously installed ACC software. Depending on when your NVR6 Premium Form D – FIPS Series was shipped, it is recommended that you connect to the network when possible to install updates for Windows and ACC Client software after system recovery is completed.

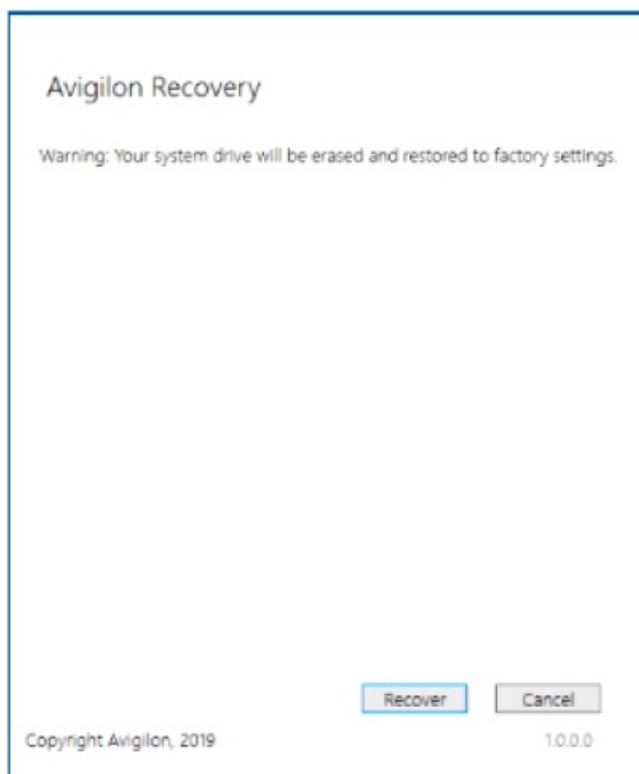
1. Start operating system recovery in one of the following ways:

- On your Windows desktop, select  and then hold down the Shift key and select Restart.
- On your locked Windows screen, select  and then hold down the Shift key and select Restart.
- During direct boot of the operating system, repeatedly press the down-arrow key and select the partition.

2. On the Choose an option screen, select Use another operating system.

3. Select the OS Recovery partition.

4. On the Avigilon Recovery window, select Recover.



Allow up to half an hour for the recovery to complete.

5. After the system reboots, complete the Windows setup process.

6. Navigate to C:\Avigilon\Control Center Installation Files, and run the ACC installer for the version of ACC software in use at your site.

If needed, connect to the internet and download the required ACC installers.

7. After reinstalling the ACC software, reactivate the ACC licenses.

For more information about reinstalling and reactivating the ACC software, see [avigilon.com/recovery](https://www.avigilon.com/recovery).

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 the [Creating the OS Recovery USB Drive section of the Avigilon System Hardening Guide](#).

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 the [Enabling and Disabling USB Ports section of the Avigilon System Hardening Guide](#) 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 Log into Windows Server for the First Time.

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 the [Avigilon System Hardening Guide](#).

2. Open Windows Explorer and locate the storage volume with the locked icon.
3. 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.
4. Click on the Windows Start button and type Manage BitLocker. Open the Manage BitLocker application.
5. 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.

Maintenance

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 Certificate Management for the Server Administrator Software section of the Avigilon System Hardening Guide.
- To workaround the self-signed certificate: use the Windows Registry Editor to edit the key to 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 Workaround section of the Avigilon 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 19.

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/>.
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 is 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 disk (RAID) settings, assign a hot spare, and remotely monitor the system health. For more information about the features of the Server Administrator, see the Help system provided in the software.

Replacing Hard Drives

NOTE

Before powering down the recorder for any upgrade, recovery, or maintenance, back up critical recorder data and programs. For more information, see the Windows™ Upgrade and Recovery Guide for Avigilon Systems ([link](#)).

- If one of the hard drives fails, you can replace the failed drive while the recorder continues to run. If more than two hard drives fail at the same time, contact Avigilon Technical Support immediately for recovery instructions.
- If your recorder is still under warranty, contact Avigilon Technical Support to replace the failed hard drive.

IMPORTANT

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

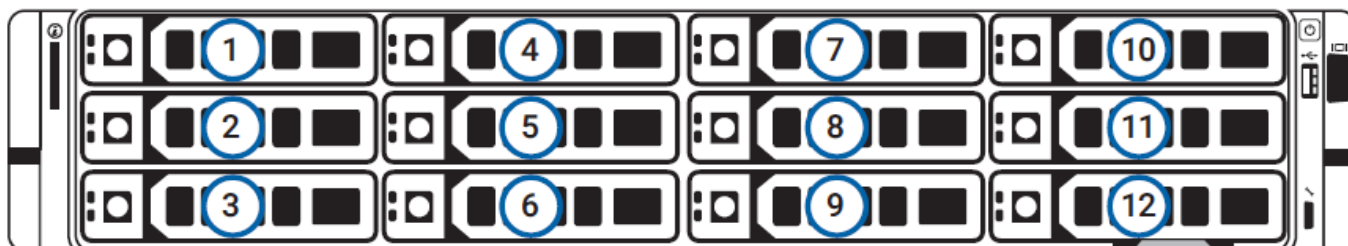
1. Open the Server Administrator.
2. Check which hard drive has failed, then disconnect the drive through the Server Administrator software.
3. Remove the bezel.
4. Perform the following procedures.

Guidelines

When replacing hard drives, observe the following general guidelines:

If only one drive is used, install the drive in the drive bay with the lowest device number.

For example:



• WARNING

Opening or removing the system cover while the system is powered on may expose you to a risk of electric

shock.

- **CAUTION**

Do not operate the system without the cover for a duration exceeding five minutes. Operating the system without the system cover can result in component damage.

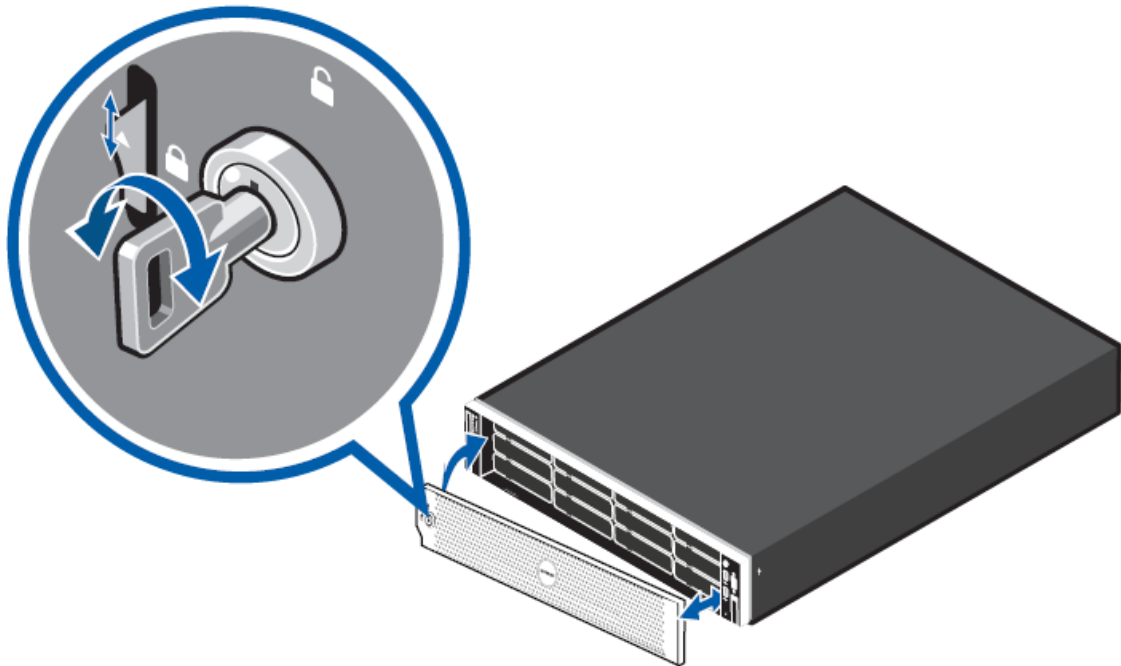
- **CAUTION**

To ensure proper operation and cooling, all bays in the system and system fans must be always populated with a component or a blank.

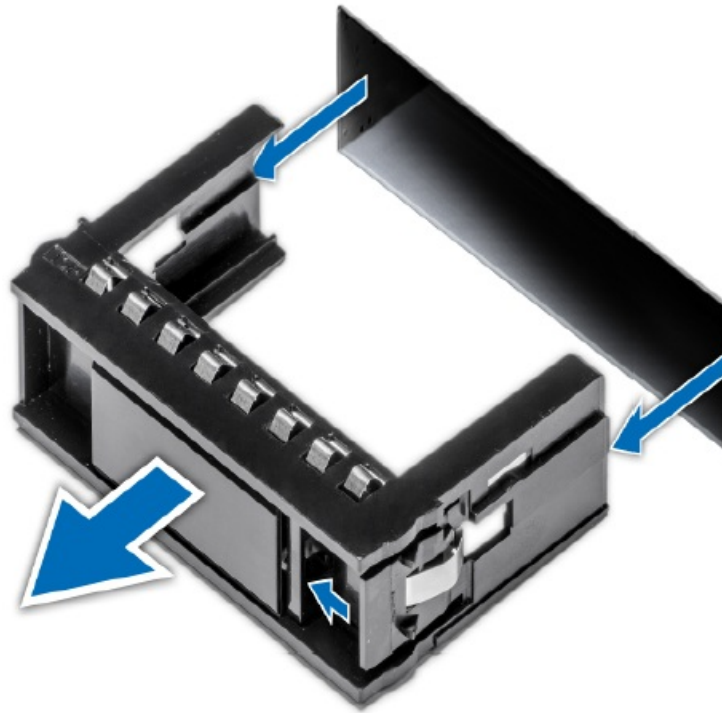
Replacing a Hard Drive Blank

- The hard drives on the NVR6 Premium Form D – FIPS Series are set up in a RAID configuration. This allows information to be recorded across several hard drives.
- If one hard drive fails, 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 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 H*** > 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 the recording to the unused hard drive.

To assign the new hard drive as a hot spare:

- In the Task list, select Assign and Unassign Global Hot Spare.
- Click Execute.

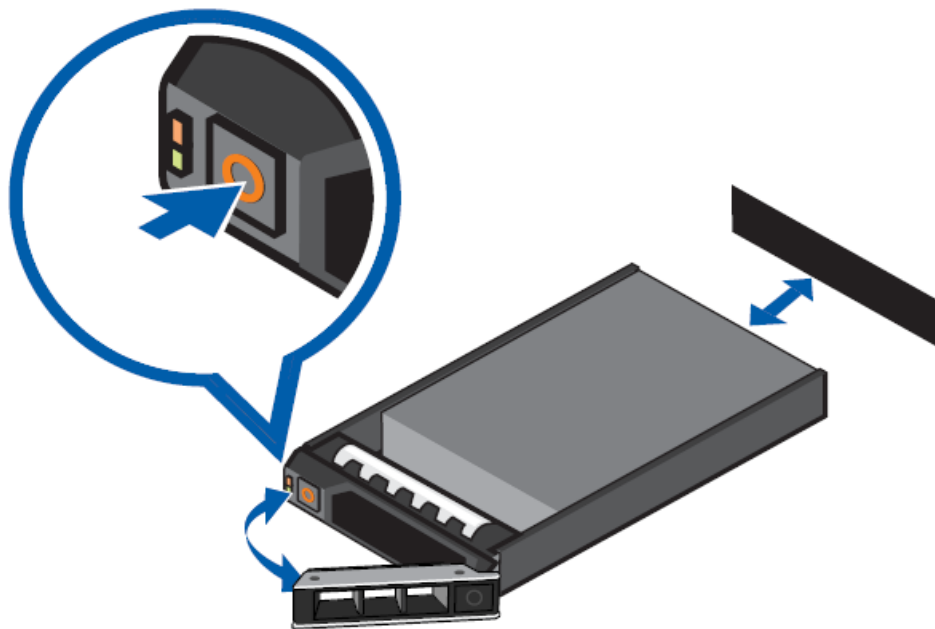
If the new hard drive is not displayed in the Server Administrator, try one of the following:

- Refresh the browser.
- Reboot the recorder.

Replacing Front Hard Drives

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

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 the replacement hard drive into the carrier and 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. After the hard drive is inserted in, push the handle against the hard drive to lock it into place.

The recorder will immediately start rebuilding the hard drive. The progress of the rebuilding is displayed in the Physical Disks panel or 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
---------------	-------------

 System health and System ID	<p>Steady blue — The system is powered on and healthy. System health mode is active.</p> <p>Blinking blue — System identification mode is active.</p> <p>Steady amber — The system is in fail-safe mode.</p> <p>NOTE</p> <p>If the system health indicates a degraded or critical state, contact Avigilon Technical Support for assistance.</p> <p>Blinking amber — The system is experiencing a fault. Check the System Event Log. For more information, see System Health and Identification Modes.</p>
 Hard drive	<p>Steady amber — The hard drive is experiencing an error. Check the System Event Log.</p>
 Temperature	<p>Steady amber — A thermal error has occurred. Possible errors include:</p> <ul style="list-style-type: none"> o Temperature out of range o Fan failure <p>Check that the fans are functioning correctly and the air vents are not blocked.</p>
 Electrical	<p>Steady amber — An electrical error has occurred. Possible errors include:</p> <ul style="list-style-type: none"> o Voltage out of range o Failed power supply o Voltage regulator <p>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.</p>
 Memory	<p>Steady amber — A memory error has occurred.</p> <p>Check the System Event Log and reset the memory module, if the error persists.</p>
 PCIe	<p>Steady amber — A PCIe card error has occurred.</p> <p>Restart the system, upgrade the device firmware, and reinstall the card, if the error persists.</p>

iDRAC Direct LED Indicators

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



Figure 4: (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:

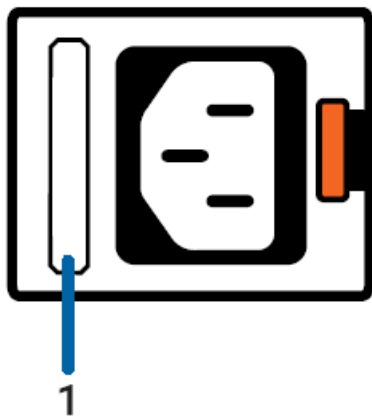


Figure 5: (1) The power status indicator for 96TB-200TB recorders

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

	<p>CAUTION</p> <p>To prevent power supply mismatches, do any of the following:</p> <p>Avoid mixing power supply units from previous generations of servers even if the units have the same power rating.</p> <p>Replace only the power supply unit with the blinking indicator.</p> <p>Identical power supply units must receive the same input voltages, be of the same type and support the same maximum power output.</p> <p>Combining AC and DC power supply units is not supported.</p>
--	---

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 6: (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.
Link LED — amber 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 — amber 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.

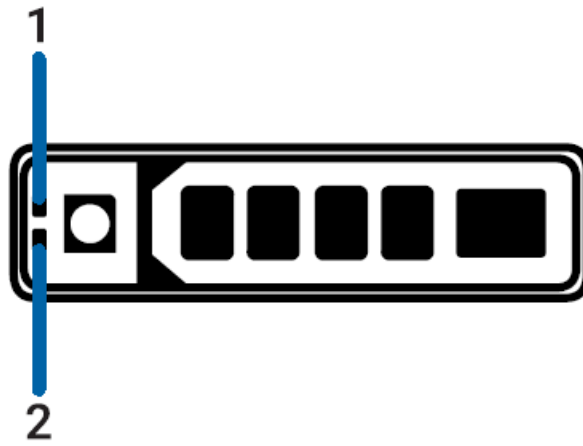


Figure 7: (1) Status LED. (2) Activity LED.

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	<p>The hard drive is ready for removal from the recorder.</p> <p>NOTE</p> <p>The indicator remains off until all drives are initialized after the system is turned on. Drives are not ready for removal during this time.</p>
Two short green flashes every second	The system is identifying a new hard drive, or preparing a hard drive for removal.
	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.

System Health and Identification Modes

- In the front left panel of the recorder, you can switch between system health and system identification modes:
 - Press the **i** button to enable the system identification mode, which is used to identify a recorder deployed in a rack with other equipment.
The blue indicator starts blinking.
 - Press the **i** 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 recorder.
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](#).

For More Information

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.

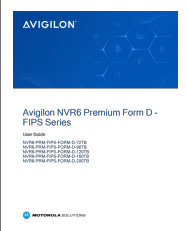
Additional Documentation

- [Windows Upgrade and Recovery Guide for Avigilon](#)
- [Enabling iDRAC Enterprise Features Setup Guide](#)
- [Avigilon System Hardening Guide](#)

Limited Warranty

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

Documents / Resources

	<p>MOTOROLA SOLUTIONS NVR6-PRM-FIPS-FORM-D-72TB Network Video Recorders [pdf] User Guide NVR6-PRM-FIPS-FORM-D-72TB Network Video Recorders, NVR6-PRM-FIPS-FORM-D-72TB, Network Video Recorders, Video Recorders, Recorders</p>
---	--

References

-  [LicenseServer](#)
-  [LicenseServer](#)
-  [Avigilon Documentation](#)
-  [Avigilon Support Community](#)
-  [Avigilon Support Community](#)
-  [Avigilon Documentation](#)
-  [Avigilon Documentation](#)

- [!\[\]\(eae20f1adff742df783f6f7e3bbe72d1_img.jpg\) Avigilon Documentation](#)
- [!\[\]\(43c6e08c5a1618d745b54da5c843274e_img.jpg\) Avigilon Documentation](#)
- [!\[\]\(f5ee48910650695cea680b2433c1d60d_img.jpg\) Avigilon Documentation](#)
- [!\[\]\(da0f02caffeb5a74776a1d5d1892b059_img.jpg\) Avigilon Documentation](#)
- [!\[\]\(edb096eed27f3ac1241ba8d18d05acad_img.jpg\) Avigilon Documentation](#)
- [!\[\]\(554d866cfdb5a2c8f73998019542d337_img.jpg\) Avigilon Documentation](#)
- [!\[\]\(c1170582320733ace24db86bc6d97423_img.jpg\) Avigilon Support Community](#)
- [!\[\]\(51c4b897e692428305845816e97ca71e_img.jpg\) Avigilon Support Community](#)
- [!\[\]\(810c0da19263e18e2f95623517bed1dc_img.jpg\) Passwords must meet complexity requirements of the installed password filter | Microsoft Learn](#)
- [User Manual](#)

[Manuals+](#), [Privacy Policy](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.