



IndigoVision

Compact NVR-AS 4000

User Guide

THIS MANUAL WAS CREATED ON WEDNESDAY, NOVEMBER 24, 2021.

DOCUMENT ID: IU-NVR-MAN018-22

Legal Considerations

LAWS THAT CAN VARY FROM COUNTRY TO COUNTRY MAY PROHIBIT CAMERA SURVEILLANCE. PLEASE ENSURE THAT THE RELEVANT LAWS ARE FULLY UNDERSTOOD FOR THE PARTICULAR COUNTRY OR REGION IN WHICH YOU WILL BE OPERATING THIS EQUIPMENT. INDIGOVISION LTD. ACCEPTS NO LIABILITY FOR IMPROPER OR ILLEGAL USE OF THIS PRODUCT.

Copyright

COPYRIGHT © INDIGOVISION LIMITED. ALL RIGHTS RESERVED.

THIS MANUAL IS PROTECTED BY NATIONAL AND INTERNATIONAL COPYRIGHT AND OTHER LAWS. UNAUTHORIZED STORAGE, REPRODUCTION, TRANSMISSION AND/OR DISTRIBUTION OF THIS MANUAL, OR ANY PART OF IT, MAY RESULT IN CIVIL AND/OR CRIMINAL PROCEEDINGS.

INDIGOVISION IS A TRADEMARK OF INDIGOVISION LIMITED AND IS REGISTERED IN CERTAIN COUNTRIES. INDIGOULTRA, INDIGOPRO, INDIGOLITE, INTEGRA AND CYBERVIGILANT ARE REGISTERED TRADEMARKS OF INDIGOVISION LIMITED. CAMERA GATEWAY IS AN UNREGISTERED TRADEMARK OF INDIGOVISION LIMITED. ALL OTHER PRODUCT NAMES REFERRED TO IN THIS MANUAL ARE TRADEMARKS OF THEIR RESPECTIVE OWNERS.

SAVE AS OTHERWISE AGREED WITH INDIGOVISION LIMITED AND/OR INDIGOVISION, INC., THIS MANUAL IS PROVIDED WITHOUT EXPRESS REPRESENTATION AND/OR WARRANTY OF ANY KIND. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAWS, INDIGOVISION LIMITED AND INDIGOVISION, INC. DISCLAIM ALL IMPLIED REPRESENTATIONS, WARRANTIES, CONDITIONS AND/OR OBLIGATIONS OF EVERY KIND IN RESPECT OF THIS MANUAL. ACCORDINGLY, SAVE AS OTHERWISE AGREED WITH INDIGOVISION LIMITED AND/OR INDIGOVISION, INC., THIS MANUAL IS PROVIDED ON AN "AS IS", "WITH ALL FAULTS" AND "AS AVAILABLE" BASIS. PLEASE CONTACT INDIGOVISION LIMITED (EITHER BY POST OR BY E-MAIL AT TECHNICAL.SUPPORT@INDIGOVISION.COM) WITH ANY SUGGESTED CORRECTIONS AND/OR IMPROVEMENTS TO THIS MANUAL.

SAVE AS OTHERWISE AGREED WITH INDIGOVISION LIMITED AND/OR INDIGOVISION, INC., THE LIABILITY OF INDIGOVISION LIMITED AND INDIGOVISION, INC. FOR ANY LOSS (OTHER THAN DEATH OR PERSONAL INJURY) ARISING AS A RESULT OF ANY NEGLIGENT ACT OR OMISSION BY INDIGOVISION LIMITED AND/OR INDIGOVISION, INC. IN CONNECTION WITH THIS MANUAL AND/OR AS A RESULT OF ANY USE OF OR RELIANCE ON THIS MANUAL IS EXCLUDED TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAWS.

Contact address



IndigoVision
Caledonian Exchange,
1st Floor, 19a Canning Street,
Edinburgh,
EH3 8EG

TABLE OF CONTENTS

	Legal Considerations	2
	Copyright	2
	Contact address	2
1	About This Guide	1
	Safety notices	1
2	Hardware Description	3
	Overview	3
	Metrics	4
	Connections	4
	Video	5
	USB	5
	LAN	6
	Serial port	6
	Power	6
	Power requirements	6
3	Getting Started	7
	Package contents	7
	Front connections	7
	Rear connections	8
	Additional items	8
	Power	8
	Power on	8
	Power off	9
	Remote power on	9
	Remote power off	9
	Complete the initial system setup	9
	Configuration	10
	DHCP	10
	Using a monitor and keyboard	10
	Using the Serial port	11
	Configure the License Server	11
	Edge Storage Retrieval	12
	NVR Footage Retrieval	13

4	Installation	15
	Attach the device to the network	15
	Rack mount installation	15
	Web Configuration pages	15
	Attach the device to the network	16
5	Operations	17
	Protect recordings	17
	Format a disk	17
	Configure network redundancy	17
	Power off	18
	Backup a recording	18
	Install a new license or update an existing license	18
	Create and send a fingerprint file	19
	Apply a license file	19
6	Configuration	21
	Web Configuration pages	21
	Home	21
	Network	22
	Date & Time	23
	Disk	23
	NVR	24
	Alarms	25
	Status Monitoring	25
	Network Security	26
	Email	28
	Bandwidth Management	29
	License	29
	Firmware Upgrade	30
	Diagnostics	30
7	Troubleshooting	33
	Monitor recordings	33
	NVR Alerts	33
	Recording failure alerts	33
	Network failure alerts	33
8	Hardware Specification	35
	Video	35
	Audio	35
	Network	35
	Storage	35

	Performance	35
	Environment	36
	Regulatory	36
A	General Public License	37

1 ABOUT THIS GUIDE

This guide is written for users of Compact NVR-AS 4000 devices. It provides installation and configuration information for the device, as well as a description of the hardware and specifications.

Please ensure you read the instructions provided in the guide before using the device.

Safety notices

This guide uses the following formats for safety notices:



Indicates a hazardous situation which, if not avoided, could result in death or serious injury.



Indicates a hazardous situation which, if not avoided, could result in moderate injury, damage the product, or lead to loss of data.



Indicates a hazardous situation which, if not avoided, may seriously impair operations.



Additional information relating to the current section.

2

HARDWARE DESCRIPTION

This chapter details the Compact NVR-AS 4000 device's connections, weight and dimensions.

Overview

The Compact NVR-AS 4000 is a standalone video and audio recorder. It contains a disk, which allows you to store recordings and play them back at a later date. It provides a powerful and integrated recording and playback system for video and audio from cameras, transmitters, and receivers.

Each Compact NVR-AS 4000 in a system can record from up to 40 cameras or transmitters while simultaneously playing back up to 20 recordings, all at full frame rate. The Compact NVR-AS 4000 is managed and configured by the Control Center application. Video can be played back to PCs, analog monitors, and standard VCRs.

The Compact NVR-AS 4000 allows the following:

- Recording and playing back MJPEG, MPEG-4, and H.264 video and audio streams
- Third party camera support
- Redundant network connections
- Powerful and distributed alarm management
- Digital Signatures and Tamper Protection of recordings



Figure 1: Compact NVR-AS 4000 (Standard)



Figure 2: Compact NVR-AS 4000 (Slimline)

Metrics

Dimensions

- 200 mm (W) x 144 mm (D) x 70.5 mm (H)
- 198 mm (W) x 144.8 mm (D) x 48 mm (H) (Slimline)

Weight

- 1.56 Kg
- 1 Kg (Slimline)

Connections

There are connections on the front and rear of the device.

Notice *Not all ports are supported, and not all should have devices connected to them.*

► For more information, see "Package contents" on page 7

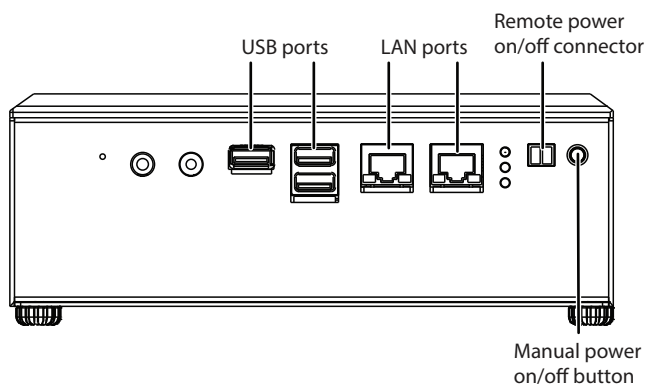


Figure 3: Front connections - Standard variant

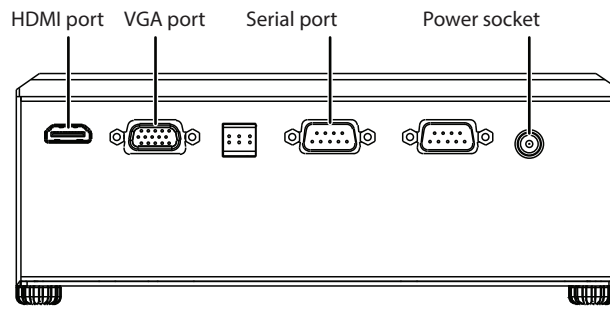


Figure 4: Rear connections - Standard variant

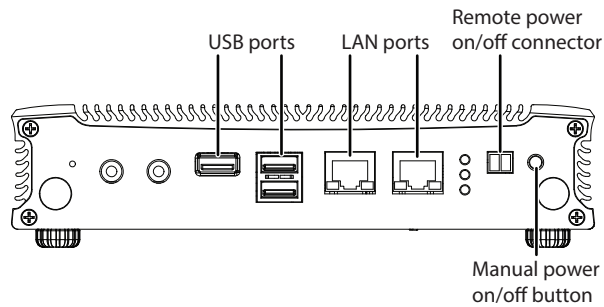


Figure 5: Front connections - Slimline variant

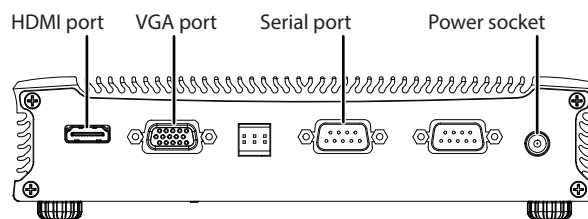


Figure 6: Rear connections - Slimline variant

Video

There are two video connections.

- HDMI
- VGA

Notice *A monitor should only be connected for initial configuration.*

USB

There are three USB connection ports.

- 2 x USB 2.0
- 1 x USB 3.0

Notice *Only USB keyboards are supported for initial network configuration. No other USB devices should be connected to the Compact NVR-AS 4000.*

LAN

- 2 x RJ-45 10/100/1000 Mbps adaptive Ethernet interface

Serial port

There is one RS-232 Serial port.

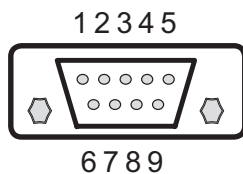


Figure 7: RS-232 Serial port

Item	Description
1	Data Carrier Detect (DCD #)
2	Receive Data (RXD)
3	Transmit Data (TXD)
4	Data Terminal ready (DTR #)
5	Ground (GND)
6	Data Set Ready (DSR #)
7	Request To Send (RTS #)
8	Clear To Send (CTS #)
9	Ring Indicator (RI #)

Power

In addition to the front panel power button, it is possible to remotely power on the NVR by connecting a pair of switch contacts to the PS_ON connector.

To power on or off the NVR, momentarily short and then open pins 1 and 2 of PS_ON.

Power requirements

The Compact NVR-AS 4000 is powered using a universal mains powered PSU which supplies 12V DC +/- 5% at 5A maximum. The maximum power consumed by the product is 21W.

3

GETTING STARTED

This chapter describes the initial steps required to start using the Compact NVR-AS 4000 device.

Package contents

Before continuing, please check that you have been shipped the items listed for your device.

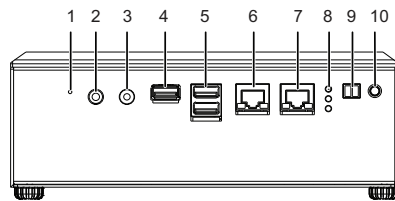


Figure 8: Front connections - Standard variant

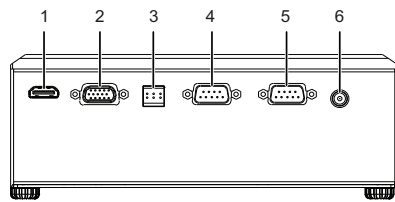


Figure 9: Rear connections - Standard variant

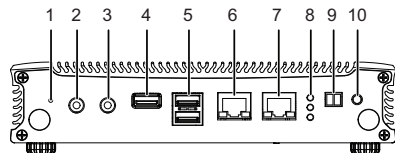


Figure 10: Front connections - Slimline variant

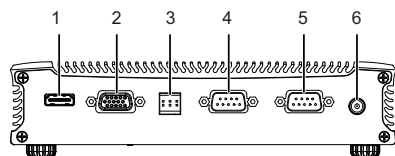


Figure 11: Rear connections - Slimline variant

Front connections

- | | |
|---------------------------------------|---------------------------------------|
| 1. Reset switch | 2. MIC IN (currently not supported_ |
| 3. LINE OUT (currently not supported) | 4. USB 3.0 port |
| 5. 2 x USB 2.0 ports | 6. Network connection 10/100/1000Mbps |

- | | | |
|---|-------------------------|---|
| 7. Network connection
10/100/1000Mbps port
(LAN1) | port (LAN2) | 8. Status LED indicators (HDD and
Power)(3G currently not supported) |
| 9. Remote power on/off
connector (PS_ON) | 10. Power on/off button | |

Rear connections

- | | |
|--|--|
| 1. HDMI port | 2. VGA
port |
| 3. DIO (currently not supported) | 4. RS-232
Serial
Port
(COM1) |
| 5. RS-232 Serial Port (COM2) (currently not supported) | 6. Power
adapter
socket
(DC_IN) |

Additional items

- 2 x Terminal blocks
- 12V Power supply with regional IEC mains lead

Regulatory

- | | |
|-------------------------|-----------------|
| • EN 55032 | • EN 60068-2-6 |
| • EN 55035 | • EN 60068-2-30 |
| • EN 55024 | • EN 60068-2-1 |
| • FCC Part 15 Subpart B | • EN 60068-2-2 |
| • EN 60068-2-29 | • UL |
| • EN 60068-2-64 | • NOM-001 |



In accordance with the EC Waste Electrical and Electronic Equipment (WEEE) directive 2002/96/EC this product must be sent to a recycling plant for proper disposal at the end of its use.

Power

The Compact NVR-AS 4000 can be powered on and off either manually or remotely.

Power on

The Compact NVR-AS 4000 can be powered on by pressing the manual power on/off button.

When power is applied to the NVR it will automatically power up. No button press is required.

Power off

The Compact NVR-AS 4000 can be powered off by briefly pressing the manual power on/off button.

Notice *Continuously holding the button causes the NVR to shut down instantly, and can cause data loss.*

After the power button LED has turned red, the mains power can be disconnected.

Notice *Removing the mains power while the power button LED is green can result in data loss.*

Remote power on

To remotely power on the Compact NVR-AS 4000, momentarily apply a short circuit across pins 1 and 2 of PS_ON.

- For more information, see "Power" on page 6

Remote power off

To remotely power off the Compact NVR-AS 4000, momentarily apply a short circuit across pins 1 and 2 of PS_ON.

- For more information, see "Power" on page 6

Complete the initial system setup

Before you can configure the rest of the Compact NVR-AS 4000 settings the appliance administrator password must be set. This is done by accessing the web interface on the device, the first time you do so you will be prompted to set the appliance administrator password.

When first powered on the Compact NVR-AS 4000 is set to use DHCP.

In order to get the IP address of the system, which is required to access the web interface, you can do one of the following:

1. Query your DHCP server to find which IP address has been assigned to the system
2. Configure the system to use a static IP address.

- For more information, see "Using a monitor and keyboard" on page 10



Until the appliance administrator password is set you will not be able to discover the Compact NVR-AS 4000 in Control Center or perform any further configuration.

Configuration

Initial configuration can be done using one of the following methods:

- DHCP (default method)
- Monitor and keyboard connected directly to the device
- Serial connection

After initial configuration is complete, further device configuration and setup is completed using the Web Configuration pages.

► For more information, see *"Configuration" on page 21*

DHCP

If your network supports DHCP connections, attach the device to the network and a valid IP address is automatically assigned. The Compact NVR-AS 4000 can then be discovered using the Control Center front-end application.

If your network does not support DHCP, the device will not be assigned an IP address and you must follow either the monitor and keyboard or serial port instructions.

Using a monitor and keyboard

The Compact NVR-AS 4000 device can be configured by connecting a monitor to the VGA or HDMI port and a keyboard to one of the USB ports.

1. Connect the keyboard and monitor to the device and press **Enter**.

You should see the following prompt:

```
IndigoVision Compact NVR-AS 4000 [standaloneNVR]
login:
```

2. Log in to the device using the username `config` and password `config`.

The device prompts you to enter the new configuration values.

3. At each prompt, press **Enter** to accept the current value.
 - **DHCP** - Enter `Y` or `N` to choose between a DHCP or static IP configuration.
 - **IP Address** – Enter the IP address for the unit's network connection.
 - **Subnet Mask** – Enter the IP network subnet mask for the unit's network connection.
 - **Gateway** – Appropriate default gateway for remote network access: this is only required if the unit is to communicate with devices on a different subnet.
 - **Preferred/Alternate Name Server Address** – Enter the IP address of the DNS server used to convert network names into numerical IP addresses. You only need to enter a name server if you wish to specify NTP or SMTP server addresses as names and not as IP addresses.
 - **NVR name** – Enter a name to describe the unit.
 - **NVR location** – Enter a name to describe the location of the unit.
 - **Reset network security** – Enter `Y` to reset all passwords used to access device, disable IP Access Restrictions, and reset the device to HTTP use only by deleting any HTTPS certificate or certificate request.

You are now ready to attach the device to the network.



The VGA and HDMI ports go into sleep mode after a period of inactivity. To bring back out of sleep mode, press any key.

Using the Serial port

To configure the Compact NVR-AS 4000 using the serial port, you require an RS-232 Null Modem serial cable.

1. Connect the serial cable between the device (COM 1) and the PC.
2. On the PC, use a Terminal Emulation program such as Windows HyperTerminal, and set the serial port parameters as follows:
 - 115200 baud
 - 8 bits
 - No parity
 - 1 stop bit
 - Flow Control: None

3. Connect to the device and press **Enter**.

You should see the following prompt:

```
IndigoVision Compact NVR-AS 4000 [standaloneNVR]
login:
```

4. Log in to the device using the username "config" and password "config".
The device prompts you to enter the new configuration values.
5. At each prompt, press **Enter** to accept the current value.
 - **DHCP** - Enter **Y** or **N** to choose between a DHCP or static IP configuration.
 - **IP Address** – Enter the IP address for the unit's network connection.
 - **Subnet Mask** – Enter the IP network subnet mask for the unit's network connection.
 - **Gateway** – Appropriate default gateway for remote network access: this is only required if the unit is to communicate with devices on a different subnet.
 - **Preferred/Alternate Name Server Address** – Enter the IP address of the DNS server used to convert network names into numerical IP addresses. You only need to enter a name servers if you wish to specify NTP or SMTP server addresses as names and not as IP addresses.
 - **NVR name** – Enter a name to describe the unit.
 - **NVR location** – Enter a name to describe the location of the unit.
 - **Reset network security** – Enter **Y** to reset all passwords used to access device, disable IP access restrictions, and reset the device to HTTP use only by deleting any HTTPS certificate or certificate request.

You are now ready to attach the device to the network.

Configure the License Server

To complete the NVR-AS setup and allow it to record, you must configure the Compact NVR-AS 4000 to use an IndigoVision License Server. You can do this by using the device web configuration pages.

- For more information, see "License" on page 29

Edge Storage Retrieval

The Compact NVR-AS 4000 supports Edge Storage Retrieval from compatible cameras using ONVIF Profile G. This functionality is enabled in the NVR Configuration tab of the Web Configuration.

- For more information, see "Network" on page 22.

Notice *When Edge Storage Retrieval is enabled, it is enabled for all compatible cameras connected to the NVR. It is not possible to enable it per camera or per recording job.*

Notice *Edge Storage Retrieval cannot be done on a Failover NVR.*

Edge Storage Retrieval improves the robustness of a system to allow it to cope with:

- Network interruptions between cameras and NVRs.
- Loss of power to an NVR.

Edge Storage Retrieval is limited to Video and Audio only. The following cannot be retrieved:

- Metadata.
- Missed events.
- Alarms.

In addition to streaming to an NVR, cameras are also set-up to record to their internal storage. After loss of power to the NVR or a network interruption, when restored, the NVR requests missing recordings from the camera(s). The NVR attempts to retrieve available recordings on the camera from the last 24 hours and stores them alongside previously recorded footage. The recordings can then be played back and exported from Control Center as normal with no distinction between recorded and retrieved footage.

Notice *The time period when a job is disabled is not remembered, so if a job is disabled then re-enabled, the NVR can retrieve footage from the time period where the job had been disabled.*

To prevent the NVR repeatedly checking cameras, the results of the camera Profile G compatibility check are stored in the NVR's memory. Once this information is stored the NVR will not check a camera's Profile G compatibility again until the NVR restarts.

Notice *If a firmware upgrade is applied to a camera to provide Profile G support, the NVR must be restarted for this change to take effect.*

To use this functionality, cameras must have on board storage and must be configured with a single active on board recording job. Missing recordings are checked for when:

- The NVR starts.
- The camera network connection is restored.

- Manually triggered by **Start Edge Storage Search** on the Control Center Playback menu.

Notice *On board recording cannot be configured in Control Center. The camera must be configured to record to the SD card through the camera's web interface. Cameras must have a single active on board recording job.*

NVR Footage Retrieval

The Compact NVR-AS 4000 supports footage retrieval from an IndigoVision source NVR that is configured to be part of the same site. This functionality is enabled when you add one or more source NVRs to the currently selected (destination) NVR in Control Center.

Notice *To enable NVR Footage Retrieval, Control Center 18.0 or later must be used.*

- For more information, refer to the Control Center help.

NVR Footage Retrieval permits the automatic transfer of recordings from the source NVR to a destination NVR. NVR Footage Retrieval is intended for instances when a smaller NVR is outside of network coverage during operation, for example, when on a vehicle; when the source NVR reconnects to the network, the footage is automatically retrieved. When retrieved by the destination NVR, recordings from the last 7 days will be retrieved by the destination NVR. These recordings can then be played back and exported from Control Center as normal with no distinction between recorded and retrieved footage..

If the transfer of footage is interrupted, for example, the network connection is lost, the transfer is re-attempted when the connection to the source NVR is established.

Notice *Any digital watermarking (source or incident authentication) that a Source NVR adds to the footage will be preserved as part of the transfer.*

Notice *Do not use NVR Footage Retrieval as a replacement to NVR redundancy. Use the existing Failover functionality if that solution is required.*



Enabling this feature can necessitate large transfers of recorded footage. If there is a footage retention policy in place, users must make sure there is enough storage in place on the destination NVR.

Use the **NVR Configuration** tab of the Web Configuration to configure the NVR Footage Retrieval settings:

- **Maximum Simultaneous Sources:** The maximum number of NVRs that footage will be retrieved from at any one time.

This setting can be set to a lower value to decrease the impact on active recording jobs on the NVRs and network.

- **Time Limit:** Sets new retrieval tasks to happen only in a specific time window.

To decrease the impact on active recording jobs on the NVRs and network, you can allow NVR Footage Retrieval when fewer recordings are scheduled.

- **Start Time:** Specifies the NVR Footage Retrieval start time.
- **End Time:** Specifies the NVR Footage Retrieval end time.

4 INSTALLATION

Attach the device to the network

You can connect the NVR-AS to the Ethernet network using a standard CAT5 Ethernet cable. Connect either LAN port 1 or LAN port 2 on the front of the device to an Ethernet switch.

The NVR-AS has redundant Ethernet capability. If you connect both Ethernet ports to the network, and a link is not detected on one port, the NVR-AS automatically switches over to use the other port. To use this feature connect both ports to (preferably) different network switches.

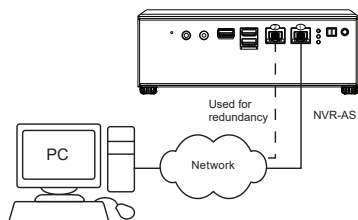


Figure 12: Connecting a device to the network

Rack mount installation

Use the following steps to fit a Compact NVR-AS 4000 in the rack mount:

1. Mount the Compact NVR-AS 4000 to the rack mount with the longer edge of the NVR running front to back.
Ensure all connections and power button are on the left and right sides when the rack mount is fitted into the server rack.
2. Remove the rubber feet one at a time and replace each with a black flat head screw from the kit contents.
3. Fix the Compact NVR-AS 4000 to the rack mount using the black screws with attached washers from the kit contents.
4. Fit the rack mount into a server rack.

A suitable 19-inch rack mount can be ordered separately (Part number: 110372).

Web Configuration pages

To access the Web Configuration pages, enter the IP address of your device into a web browser.

If an appliance administrator password has not been previously defined for the device you will be prompted to set a password. The password must contain between 8 and 32 printable ASCII (7-bit US-ASCII) characters. Enter the password again to confirm it.

You will also be prompted to configure a username and password required for Control Center to authenticate with the NVR-AS. The password must have 8 or more characters.



IndigoVision recommends that unauthenticated access is disabled.

► For more information, see the Network Security configuration page

The login page is then displayed. Use the web access password to log in, and the Home page is displayed.

Notice

The appliance administrator password must be configured before the NVR is capable of performing any authenticated network services, including recording.

To access any of the other configuration pages, click the required option in the menu on the left of each page.

To save the changes made on any page, click **Submit** before navigating away from that page.

Attach the device to the network

You can connect the NVR-AS to the Ethernet network using a standard CAT5 Ethernet cable. Connect either LAN port 1 or LAN port 2 on the front of the device to an Ethernet switch.

The NVR-AS has redundant Ethernet capability. If you connect both Ethernet ports to the network, and a link is not detected on one port, the NVR-AS automatically switches over to use the other port. To use this feature connect both ports to (preferably) different network switches.

5 OPERATIONS

This chapter describes common tasks required for the operation of the Compact NVR-AS 4000 device.

Protect recordings

To protect all recordings on the disk:

1. Enter the IP address of the NVR-AS containing the recordings into the URL field of a web browser, or view the **Configure** tab for the NVR-AS in Control Center.
2. Click **Disk** in the menu on the left. The **Disk Configuration** page opens.
3. Click **Protect All** to protect all recordings on the disk. (Similarly, click **Unprotect All** to allow all recordings to be deleted.)
4. Click **OK** to perform the operation, or click **Cancel**.



Please be aware that if you protect all recordings, you lose the ability to identify the recordings that were previously protected. If you unprotect all recordings, then all of the footage becomes available for reaping.

Format a disk

To format the current disk:

1. Enter the IP address of the NVR-AS containing the disk into the URL field of a web browser.
2. Select **Disk** from the menu on the left.
The **Disk Configuration** page opens.
3. Click **Format**.



All of the recording files, zones, detectors, alarm history, bookmarks, and other configuration information is erased when the disk is formatted.

Configure network redundancy

You can configure the Compact NVR-AS 4000 to provide redundant network connectivity. Connect both of the network ports to connections on the same IP network. Should one

network connection fail, the IP address of the device migrates to the other network connection.

Notice *The NVR-AS does not route traffic between independent networks.*

IndigoVision recommends that each network port on the device is connected to a separate switch. This ensures that network connectivity is maintained if one of the network switches fails.

NVR-AS network redundancy does not require the Spanning Tree Protocol to be enabled on the network switches it is attached to.

Power off

To prevent damage to the Compact NVR-AS 4000 and recordings on the disk, the device must be powered off in a controlled manner.

1. Briefly press the power on/off button on the front of the device.
Continuously holding down the button can cause data loss.
2. Wait for the power LED on the front power switch to change from green to red.
3. Remove the mains power cable from the NVR-AS power supply.
4. After removing mains power, remove the DC power connector from the NVR-AS.

Notice *There is also an option to power off the device remotely through the Web Configuration page.*

► For more information, see "Diagnostics" on page 30.

Backup a recording

To back up recordings, use a Secure File Transfer Protocol (SFTP) client to copy the recordings from the **/storage/VideoLibrary** directory. To access the SFTP site, log in as support (recommended), with the support user password, or as root using your appliance administrator password.

Install a new license or update an existing license

You can configure the Compact NVR-AS 4000 to act as a License Server for IndigoVision products.

Notice *Each IndigoVision site should only have a single License Server. If you configure the Compact NVR-AS 4000 to act as a License Server, make sure that there are no other License Servers active in your site.*

-
- Notice** *The Compact NVR-AS 4000 can not be used as a License Server within a site using License Federation.*
- For more information about the details of that feature, see the License Server Administrator's Guide.
-

The Compact NVR-AS 4000 comes with a 45-day trial of an IndigoUltra license. This allows you to access all features and use up to five cameras and one third-party Windows NVR-AS in your site.

The trial period starts when you first configure the Compact NVR-AS 4000 to act as a License Server.

Use the following steps to upgrade to a full license:

1. Create a fingerprint file and send it to IndigoVision with your IndigoVision order acknowledgment number.
2. Apply the license file from IndigoVision to the Compact NVR-AS 4000.

Create and send a fingerprint file

To upgrade to a full IndigoVision licence, you must first send a fingerprint file to IndigoVision.

1. Access the Compact NVR-AS 4000 Web Configuration pages, and navigate to **License**.
2. Click the **Download** button located under **License Management**.
3. When prompted, save the file.
4. Send the fingerprint file to IndigoVision Sales Order with your IndigoVision order acknowledgment number.

IndigoVision then provides a license file.

Apply a license file

To use your IndigoVision license, you must apply it to the Compact NVR-AS 4000.

1. Access the Compact NVR-AS 4000 Web Configuration pages, and navigate to **License**.
2. Click the **Browse** button located under **License Management**.
3. Select the IndigoVision license file, and click **Upload**.

A notification is displayed, confirming that the license is applied.

The new license is applied.

6

CONFIGURATION

This section explains the various configuration options provided by the Web Configuration pages.

Web Configuration pages

To access the Web Configuration pages, enter the IP address of your device into a web browser.

If an appliance administrator password has not been previously defined for the device you will be prompted to set a password. The password must contain between 8 and 32 printable ASCII (7-bit US-ASCII) characters. Enter the password again to confirm it.

You will also be prompted to configure a username and password required for Control Center to authenticate with the NVR-AS. The password must have 8 or more characters.



IndigoVision recommends that unauthenticated access is disabled.

► For more information, see the Network Security configuration page

The login page is then displayed. Use the appliance administrator password to log in, and the Home page is displayed.

Notice

The appliance administrator password and NVR-AS access credentials must be configured before the NVR is capable of performing any authenticated network services, including recording.

Notice

IndigoVision devices support Microsoft Internet Explorer (version 8 or higher).

To access any of the other configuration pages, click the required option in the menu on the left of each page.

To save the changes made on any page, click **Submit** before navigating away from that page.

Home

This section is read-only and provides a basic configuration overview of the Compact NVR-AS 4000 device and its operational status.

- **NVR-AS License Status** – This label shows the current status of the Compact NVR-AS 4000 license.

If the label is set to **Licensed**, then the Compact NVR-AS 4000 is currently connected to a License Server which is online and has a valid license.

If the label is set to **Not Licensed**, then the Compact NVR-AS 4000 is not connected to a License Server with a valid license.

Network

Use this page to configure the network settings.

- **NVR Name** – Enter a name to identify the NVR device.
- **Compact NVR-AS 4000 Location** – Enter a location to identify the device.
- **Use DHCP** – Check this to enable DHCP for the NVR device. When this is enabled, the IP address, subnet mask, gateway, and name servers are obtained from the DHCP server on the network. The options for these items are grayed out.

Notice *After switching to DHCP, you need to specify the new IP address of the network device in the web browser. Query the DHCP server to find the assigned IP address, then use this IP address in the web browser to navigate to the device.*

The NVR device chooses the first two DNS servers that the DHCP server specifies. If at least one NTP server is specified by the DHCP server then the NVR device will attempt to synchronize with these NTP servers. The Date and Time page will not list these servers and additional NTP servers can still be manually added.

Notice *If the NVR device fails to receive any configuration settings from a DHCP server on the network, it will not be accessible on the network and you will have to use a keyboard and monitor to set a static IP address.*

► For more information, see "Configuration" on page 10.

- **IP Address** – Enter the unit's IP address.
- **Subnet Mask** – Enter the unit's IP network subnet mask.
- **Gateway** – Appropriate default gateway for remote network access: this is only required if the unit is to communicate with devices on a different subnet.
- **Broadcast Address** – This value is read-only.
- **Preferred/Alternate Name Server Address** – The IP address of the DNS server used to convert network names into numerical IP addresses. You only need to enter a name server(s) if you need to specify the SMTP Server Address or NTP Server Addresses as a name and not as an IP address.

The above options are not available for editing if DHCP is enabled.

NVR-AS supports Edge Storage Retrieval from compatible cameras using Profile G.

► For more information, see "Edge Storage Retrieval" on page 12

- **Edge Retrieval**: Enable the functionality on the NVR.

Notice *When **Edge Retrieval** is selected, the functionality is enabled globally for all compatible recording jobs on the NVR. It is not possible to enable the functionality per camera or per job.*

- **Edge Retrieval Stream Limit:** The maximum number of streams that are continuously retrieved at any one time.
This setting can be set to a lower value to limit the impact on active recording jobs on the NVR and the network.
- **Edge Retrieval Rate Limit:** Sets the transfer speed of a recording to the NVR.
If this setting is selected, the transfer of a recording is set at 1x speed.
It takes 1 minute to transfer 1 minute of footage to the NVR.
If this setting is not selected, the transfer of a recording is as fast as the camera and the NVR can manage.
Select this setting to limit the impact on active recording jobs on the camera, the NVR, and the network.
- **Edge Retrieval Time Limit:** Sets new retrieval tasks to happen only in a specific time window.
You can allow retrieval of missing recordings when fewer recordings are scheduled, to limit the impact on active recording jobs on the camera, the NVR, and the network.
 - a. **Edge Retrieval Start Time:** The start time of the specified time window to be used if **Edge Retrieval Time Limit** is checked.
 - b. **Edge Retrieval End Time:** The end time of the specified time window to be used if **Edge Retrieval Time Limit** is checked.

Date & Time

Use this page to configure the Date and Time settings for the NVR device.

- **NTP Servers** - This is a list of up to five NTP Servers that the NVR device will synchronize with.
Servers can be specified as IP addresses or resolvable hostnames, if at least one name server has been specified.
Add new servers by entering the server address in the text field and click **Add**.
Remove servers by highlighting them in the list and click **Remove**.
Changes are applied when you click **Submit**.
- **Timezone** - Select the timezone for the NVR device from the list.
- **Primary Time Server** - Check this option if the NVR-AS device is expected to serve as a primary time source on a local area network when the configured NTP servers are not available.
- **Hardware Clock** - The date and time for the NVR-AS device can be directly edited using this form. This should not be required when there is an upstream NTP server.

Disk

Use this page to view the disk status and update its configuration.

- **Disk Status** – This indicates the overall status of the disk. The status can be as follows:
 - **Disk OK** – The disk is functioning normally.

- **Disk Blank** – The disk has not been formatted. This status may be seen if you are in the process of replacing the disk. Press **Format** to format the disk and the status should change to **OK**.
- **Disk Error** – There is a fault with the disk. Contact Technical Support.
- **Storage Space** – This figure indicates the total storage space on the disk.
- **Used Space** – Shows the percentage of disk space currently used.
- **Disk Temperature** – Shows the current disk temperature in Celsius and the maximum operating temperature for the disk.
- **Disk Maintenance:**
 - **Format Disk** – Reformats the disk.
- **Protection:**
 - **Protect All** – Click **Protect All** to protect all recordings on the disks.
 - **Unprotect All** – Click **Unprotect All** to unprotect all recordings on the disk. This allows them to be deleted according to the reaping regime.



If you protect/unprotect all recordings, you lose the ability to identify recordings that were individually protected/unprotected by the user in Control Center.

NVR

Use this menu to configure the NVR parameters.

- **Reaping by:**
 - Space** – Recordings are only deleted when the NVR disk is becoming full.
 - Time and Space** – Recordings are deleted either when the NVR disk is becoming full, or when recordings reach a specified age (max age).
- **Max Age** – This specifies the length of time that recordings are stored on the NVR before they are automatically deleted.
- **Enable Tamper Protection on recordings** – The NVR will embed digital signatures in every recording file allowing the authenticity and integrity of that footage to be verified at any point in the future.
 Verification will happen whenever footage is exported by Control Center as part of an Incident and the result of the verification will be written into the Incident. This provides an extra level of security: the Incident itself is protected by a watermark proving that the Incident has not been tampered with and the NVR digital signatures prove that the footage on the NVR had not been tampered with at the point of export. Tamper Protection is not compatible with video thinning. You cannot enable Tamper Protection if video thinning is already enabled.
- **Video thinning** – This removes the intermediate P-frames, leaving only independent I-frames. This leads to a reduction in storage requirements at the expense of full motion video. Video thinning is performed on footage only when it becomes older than the specified age.
 For effective use of video thinning, it is important to configure the maximum I-frame interval on the transmitter such that the frame rate of thinned footage is acceptable. Video thinning is most effective on footage with significant amounts of motion. Video thinning is not compatible with Tamper Protection. You cannot enable video thinning if Tamper Protection is already enabled.

- **Automatic Unprotect of Video** – This automatically unprotects footage after a certain time period. Footage will be unprotected only when it becomes older than the specified age.



Enabling Automatic Unprotect in conjunction with Reaping can result in the loss of video data that has been protected to provide evidence relating to an incident.



Recordings which are marked as “protected” are never automatically deleted (unless automatic unprotect of video is configured).

- **Maximum Recording Streams** - This setting specifies the maximum number of streams that the NVR can record. Use this setting to prevent overloading the NVR based on the expected stream bit rates. For example, this NVR could be used as a failover for multiple primary NVRs. In the event of the failure of multiple primary NVRs, this NVR could become overloaded. Set the maximum number of streams to avoid overload.

Alarms

Use the following parameters to configure the Alarm Server.



In order to configure the Alarm Server, your Control Center license must include the Alarm Management feature.

- **Zone alarm reaping** – This automatically deletes zone alarms based on their age. Select the check box and enter the time after which zone alarms will be deleted.

Notice

When zone alarms are reaped, any activations that contributed to those alarms are also reaped.

- **Activation reaping** – This automatically deletes activations that are not part of an alarm based on their age. Select the check box and enter the time after which activations with no associated alarm will be deleted.
- **Data record reaping:** This automatically deletes data records based on their age. Select the check box and enter the time after which data records will be deleted.



In order to configure data record reaping, your Control Center license must include the Alarm Management and Integrated Data features.

Status Monitoring

This page shows the current state of the monitored hardware diagnostics as well as options for configuring the generated alerts.

Notice *To effectively monitor the health of an Enterprise NVR-AS 4000 unit, IndigoVision recommend that you create a Device Fault Detector for the NVR.*

► For more information, refer to the Control Center help.

- **Network Redundancy** – Displays the state of the network ports that have been configured for monitoring.
 - **Generate Alerts** – Configure alerts for the following faults:
 - **Network Link Failure** – If checked, the Compact NVR-AS 4000 generates an alert when one of the Ethernet ports is not connected to the network.
-



Alerts will always be generated in Control Center for complete network failure (device unavailable).

Network Security

This page allows you to restrict access to the NVR.

Appliance Administrator Password

Specify an appliance administrator password to restrict access to the Web Configuration pages. This appliance administrator password can also be used to access the device using SSH or SFTP, when logging in as **root**.

- **Change Password** – Enter a password for the unit. This must contain between 8 and 32 printable ASCII (7-bit US-ASCII) characters. Enter the password again to confirm it.

Passwords are automatically verified for security strength, and a warning will be provided if the submitted password is not believed to be secure or could be improved.

Notice *If you forget the password, you will need to log in on the serial console or via a monitor and keyboard connected directly to the device and reset the device's security settings*

► For more information, see "Configuration" on page 10

NVR-AS Authentication

Configure the credentials required for Control Center to authenticate with the NVR-AS.



If you change the credentials, Control Center must also be updated to allow administrators and operators to continue using the NVR-AS.

- **Allow Unauthenticated Access**: Select this option to allow the NVR-AS to be used by Control Center without a username or password. This is useful to allow older workstations to be upgraded before enabling authentication.
 - For more information, see the Control Center Installation Guide.



Once all Control Center workstations are upgraded to 17.1 or later, IndigoVision recommends that unauthenticated access is disabled.

- **Username:** Enter the username to be used by Control Center to authenticate with the NVR-AS.
- **Password:** Enter the password to be used by Control Center to authenticate with the NVR-AS.
Passwords must have 8 or more characters.
- **Confirm password:** Re-enter the password to confirm you have entered it correctly.

IP Access Restrictions

- **Enable** – Check this box to restrict NVR access to the allowed addresses.

Notice

Before enabling the IP Access Restrictions, please make sure that a management PC is included in the Addresses Allowed list. Failure to do so may result in a loss of connectivity, and require physical access to the unit to disable the restrictions.

- For more information, see "Reset network security – Enter Y to reset all passwords used to access device, disable IP Access Restrictions, and reset the device to HTTP use only by deleting any HTTPS certificate or certificate request." on page 10.

- **Addresses Allowed** – Enter the IP addresses of cameras that will be used for recording, and Control Center PCs that will be used to administer and play back video from this NVR-AS.
To remove an address, select the address and click **Remove**. Shift-click or Control-click to select more than one address.
- **Add Address** – Enter an IP address and click **Add**.
You can also enter an address range, for example 10.5.1.12-20, or a CIDR address including a netmask, for example 192.168.123.0/24.

Remote Secure Shell Access

Use these settings to control remote access to the unit using a secure shell (SSH). It is possible to create a separate account with a different password to the unit for diagnostic purposes. This support account has more restricted and secure access to the unit.

Enable - Use this to enable or disable remote access to the unit.

Support User - Use this to enable or disable a remote access account with the user name "support". If enabled, remote access users will be able to login using this user name.

Support Password - Enter a password for the "support" user account. This must contain between 8 and 32 printable ASCII (7-bit US-ASCII) characters. Enter the password again to confirm it.

Passwords are automatically verified for security strength, and a warning will be provided if the submitted password is not believed to be secure or could be improved.

Root Access - Use this option to enable or disable full administrative direct remote access to the unit with the user name "root".



For best security it is recommended to ensure that remote access is disabled after unit configuration. If remote access is required for diagnostic purposes it is recommended to enable a support user account with a different password to the device password and disable root access.

HTTPS Configuration

Use these settings to configure the HTTPS settings.



*You can only install Signed Certificates when HTTPS is disabled.
Disable HTTPS before changing these settings.*

- **Mode**
Select to enable device configuration using HTTP and HTTPS. You must select at least one option.
You must have a valid HTTPS certificate to enable HTTPS. Use the options in this section to create and apply a certificate.
- **Private Key (Regenerate)**
Use this option to regenerate your private key. Using this option invalidates and deletes any certificate or certificate request that is stored on the device.
- **Self Signed Certificate**
Use this option to create and install a self-signed certificate.
To create a self-signed certificate, click **Create**. A new page opens. Enter your details and click **OK**. A self-signed certificate is generated and installed.
This option is unavailable if a certificate is already installed.
- **Certificate Authority**
Use this option to create a certificate request to submit to a Certification Authority for signing. Certificate Authority Certificates created this way are specific to this device.
To create a certificate request, click **Create**. A new page opens. Enter your details and click **OK**. A certificate request is generated and displayed in your browser. Copy the certificate request and submit it to the Certification Authority for signing.
After the certificate request has been signed and returned, **Browse** to the location of the saved certificate, then **Upload** it to the device.
You can **View** and **Delete** a certificate request if one is available.
- **Installed Certificate**
You can **View** and **Delete** the installed certificate.

Email

Use these pages to configure the email parameters.

- **Email Configuration**
 - **SMTP Server Address** – The address of your email server. You can enter an IP address, or a name such as **server.example.com** (if you have specified a name server).
 - **SMTP Server Port** – The port number used to connect to the email server. This is usually 25 or 587.

- **SMTP Server Username** – This is the username used to log into your SMTP email account (if required).
- **SMTP Server Password** – This is the password for the email account.
- **SMTP From: Address** – All emails sent by the NVR are sent from this email address. The address must be in standard email address format.

The Compact NVR-AS 4000 automatically uses secure TLS encryption for email servers that support STARTTLS. This allows emails to be sent using many corporate or Internet mail providers.

Bandwidth Management

- **Bandwidth Manager**

None – Select if no bandwidth manager is used. Playback speeds will be unconstrained.

Run Local Server – Select to run the bandwidth manager on this unit. This can be used to limit access to cameras and NVRs on the same network.

Enter the maximum uplink bandwidth available. This is the maximum network speed at which cameras and NVRs can be accessed from remote locations. Access from the local network is unrestricted.

Use Remote Server – Select to use a remote bandwidth manager. Enter the IP address of the machine hosting the bandwidth manager.

- **NVR Bandwidth Limit** – If a bandwidth manager is enabled, enter the maximum bandwidth available to a playback session for this unit. The bandwidth is shared between all playback streams in a session.



Changing the Bandwidth Manager configuration will cause a momentary interruption in recording.

License

Use these pages to view or change the License Server used by the Compact NVR-AS 4000.

License Server – A valid License Server must be configured to allow the Compact NVR-AS 4000 to record.

- For more information, refer to the Control Center Installation Guide.

The Compact NVR-AS 4000 can access an IndigoVision License Server in the following ways:

- The Compact NVR-AS 4000 can use an existing License Server running on a separate device specified using the License Server's IP address
- The Compact NVR-AS 4000 can act as a License Server for the Control Center site

Notice

Each IndigoVision site should only have a single License Server. If you configure the Compact NVR-AS 4000 to act as a License Server, make sure that there are no other License Servers active in your site.

Notice *If the Compact NVR-AS 4000 is configured to act as a License Server, you must manually configure all instances of Control Center and the other NVR-AS devices in your site to use this Compact NVR-AS 4000 as a License Server.*

License Management

The installed Control Center license can be updated here when the Compact NVR-AS 4000 is acting as a License Server.

- For more information, see *"Install a new license or update an existing license"* on page 18

License Information

This section shows information about the configured License Server.

- **License Server Status** – This shows the status of the configured License Server. This can be one of the following:
 - *Unconfigured*
 - *Offline*
 - *Unlicensed*
 - *Licensed*
- **License ID** – The unique id of the installed license. This is only shown if the License Server is licensed.
- **Trial Expiry** – The date which the trial license expires. This is only shown if the License Server is using a trial license.
- **License Tier** – The tier of the installed License. This is only shown if the License Server is licensed.
- **Device Connections** – The total number of Device Connections the installed license supports and the number that are currently unused. This is only shown if the License Server is licensed.
- **Third Party Windows NVR-AS Connections** – The total number of third-party Windows NVR-AS Connections the installed license supports and the number that are currently unused. This is only shown if the License Server is licensed.

Firmware Upgrade

Browse to the vex file you require to upgrade your unit, then click **Perform Upgrade**. Uploading the vex file may take a few minutes. After the file has been uploaded, follow the on-screen instructions to start the upgrade process. The upgrade itself will take several minutes. It is important not to power off the unit or disconnect it from the network during this process.

Diagnostics

These pages provide support information which may be requested by your IndigoVision supplier.

- **Support Information** - This button downloads a zip archive containing diagnostic information. Provide this file to Technical Support when reporting any issues with the unit.

- **Maintenance:**
 - **Reset** - Click to reset all NVR-AS settings configured from the web pages including the appliance administrator password, and reboot the unit.
The NVR-AS device retains its IP address, subnet mask, gateway and DNS servers, and HTTPS configuration.
 - **Reboot** - Click to reboot the device.
 - **Power Off** - Click to power off the device.



If the device is powered off using this option, the device will only power on again when the physical power button on the front panel is pressed.

7 TROUBLESHOOTING

This chapter provides troubleshooting information to resolve common issues.

Monitor recordings

To monitor jobs that are currently recording, use IndigoVision's Control Center application.

Control Center allows you to monitor all jobs on your NVR-AS. It allows you to set up recording jobs on NVRs on a visible network. You can also use it to view any existing jobs and their current state (enabled, disabled, recording, etc).

If a transmitter shows *Trying to record* in Control Center's recording schedule this indicates a problem with the transmitter. You should check the network connections and that the device is switched on. You should then try to access the device's Web Configuration pages.

NVR Alerts

You should pay particular attention to the following alerts in Control Center:

- **Disk Full**

Disk full alerts indicate that the NVR-AS disk is full, and that the NVR-AS cannot delete any recordings, for example, because they are protected. Use Control Center to check for recordings marked as Protected and unprotect these recordings.

- **Maximum Recordings**

These indicate that the maximum number of recordings has been exceeded. This may be because there are too many short recordings.

Recording failure alerts

Recording failure alerts indicate that one or more transmitters are not recording correctly.

- Check the network connectivity between the transmitter and the NVR-AS.
- Ensure that the maximum number of licensed streams has not been exceeded.

Network failure alerts

If there are network redundancy failures, then configured alerts are seen in Control Center and any configured device fault detectors are activated.

- For more information, see *"Status Monitoring" on page 25*

8

HARDWARE SPECIFICATION

This chapter details the hardware specifications for the Compact NVR-AS 4000 device.

Video

- Simultaneously record and playback full frame rate
- Full resolution video streams from any IndigoVision IP Camera or Encoder
- Record and playback from other devices
- Digital signing at point of recording and at export

Audio

- Recording and playback of AAC and G.711 audio

Network

- Dual redundant 100/1000 BaseT RJ-45
- Protocols - TCP, UDP, ICMP, IGMP, HTTP, NTP, SSH, SFTP

Storage

Standard variant:

- 3.5" SATA Seagate SkyHawk Surveillance Hard Drive optimised for 24x7 video storage
- 12000GB (12TB variant) / 4000GB (4TB variant) / 1000GB (1TB Extended Temperature variant)

Slimline variant:

- Disk - 1 x 2.5" Western Digital SATA AV series optimized for 24x7 video storage
- 1000 GB

Performance

- 40 Recording plus simultaneous playback of 20 streams
- 40 Mbps in
- 40 Mbps out
- 80 Mbps total

Environment

Operating temperature:

- 0°C (32°F) to +50°C (122°F)
- 0°C (32°F) to +60°C (140°F) (1TB Extended Temperature variant)

Regulatory

- | | |
|-------------------------|-----------------|
| • EN 55032 | • EN 60068-2-6 |
| • EN 55035 | • EN 60068-2-30 |
| • EN 55024 | • EN 60068-2-1 |
| • FCC Part 15 Subpart B | • EN 60068-2-2 |
| • EN 60068-2-29 | • UL |
| • EN 60068-2-64 | |



In accordance with the EC Waste Electrical and Electronic Equipment (WEEE) directive 2002/96/EC this product must be sent to a recycling plant for proper disposal at the end of its use.

A

GENERAL PUBLIC LICENSE

IndigoVision's NVR-AS products use code that is freely available under the General Public License (GPL).

This license makes it a requirement to release changes made to the source code. In compliance, the GPL source code and any changes made by IndigoVision are available on request through IndigoVision Customer Support.

