IndigoVision

Enterprise NVR-AS 4000 2U Linux Appliances

User Guide

IndigoVision®
a Motorola Solutions Company

This manual was created on Monday, August 23, 2021.

Document ID: IU-NVR-MAN036-6

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

Contact address

IndigoVision

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

Dell Software License Agreement

Before using your system, read the Dell Software License Agreement that came with your system. You must consider any media of Dell-installed software as BACKUP copies of the software installed on your system's hard drive. If you do not accept the terms of the agreement, call the customer assistance telephone number.

For customers in the United States, call 800-WWW-DELL (800-999-3355).

For customers outside the United States, visit **SUPPORT.DELL.COM** and select your country or region from the top of the page.

NVR-AS License Terms

The operating system on the device is not licensed as general purpose server software. As such, you are prohibited from installing and using any other software on that server (unless supplied by IndigoVision); and accessing or using desktop functions on the server other than as necessary for operating the NVR-AS software.

TABLE OF CONTENTS

1 ABOUT THIS GUIDE

This guide is written for users of all IndigoVision's Enterprise NVR-AS 4000 2U Linux Appliances. It provides an overview of the systems as well as installation and configuration information.

Safety notices

This guide uses the following formats for safety notices:


Warning

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


Caution

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

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

Additional information relating to the current section.

2 Overview

IndigoVision's Enterprise NVR-AS 4000 2U Linux Appliances are part of IndigoVision's Control Center suite. They provide a powerful and integrated recording and playback system for video and audio from IP cameras and encoders, to suit all your requirements.

The Enterprise NVR-AS 4000 2U Linux Appliances can be located at any point on the network and operation can continue without the need for management software providing a truly scalable and reliable system.

The Enterprise NVR-AS 4000 2U Linux Appliances provide the following features:

- Record and playback MJPEG, JPEG 2000, MPEG-4, H.264 and H.265 video and audio streams
- Full frame rate recording of up to 200 streams with simultaneous playback of up to 100 streams
- Third party camera support
- RAID storage resilience and redundant network connections
- Powerful and distributed alarm management
- Digital Signatures and Tamper Protection of recordings
- Integrated hardware fault monitoring

Hardware

Enterprise NVR-AS 4000 G2 2U

The Enterprise NVR-AS 4000 G2 2U has 12 hot-swappable hard-disk bays, accessible from the front of the device. The disks in these bays are configured as a RAID6 array. This array is used for video storage.

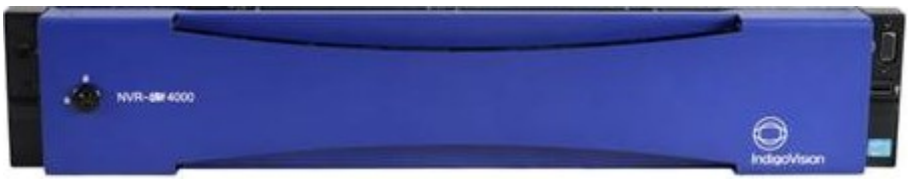

Figure 1: Enterprise NVR-AS 4000 G2 2U

The 16 disk variant has an additional four hard-disk bays, accessible internally. These are not hot-swappable.

These four bays and the 12 front-accessible bays are configured as a single RAID6 array for video storage.

In addition there are also two hot-swappable disks, accessible from the rear of the device. These disks are configured as a RAID1 array. This array is used for the operating system and configuration information.

This platform has two 10Gbps Ethernet ports and two 1Gbps Ethernet ports. These are configured as separate aggregated pairs for greater throughput and redundancy.

In order to use the 10Gbps Ethernet ports, you must also purchase Direct Attach twinax cables or 10GBASE-SR fibre optic SFP+ transceiver modules from IndigoVision.

Notice *The Enterprise NVR-AS 4000 G2 2U only supports either the 1Gbps Ethernet pair or the 10Gbps Ethernet pair to be connected at any given time, not both.*

Enterprise NVR-AS 4000 G3 2U

The Enterprise NVR-AS 4000 G3 2U has three configurations, defined by base video storage capacity. In all three configurations, storage is divided between a RAID1 array which is used to store OS and configuration data and a RAID6 array which is used to store recorded video. Each configuration only differs by the location and type of the physical disks included in these arrays.

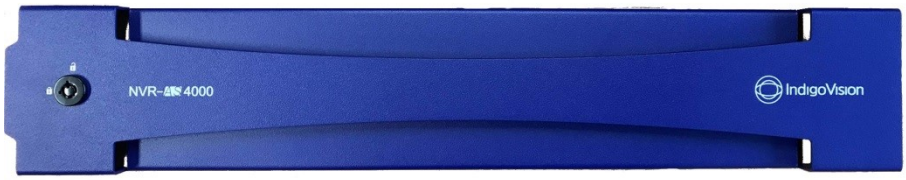

Figure 2: Enterprise NVR-AS 4000 G3 2U

The disk configurations are as follows:

- 48TB
  - RAID1: Two hot-swappable solid-state disks, accessible from the rear of the device
  - RAID6: 12 hot-swappable hard-disk bays, accessible from the front of the device
- 100TB
  - RAID1: Two hot-swappable solid-state disks, accessible from the rear of the device
  - RAID6: Four internal (i.e. non-hot-swappable) hard-disk drives and 12 hot-swappable hard-disk bays, accessible from the front of the device
- 140TB
  - RAID1: Two internal (non-hot-swappable) solid-state disks
  - RAID6: Four internal (non-hot-swappable) hard-disk drives, 12 hot-swappable hard-disk bays, accessible from the front of the device and two hot-swappable hard-disk bays, accessible from the rear of the device

All three configurations have two 10Gbps Ethernet ports and two 1Gbps Ethernet ports. These are configured as an aggregated group.

In order to use the 10Gbps Ethernet ports, you must also purchase Direct Attach twinax cables or 10GBASE-SR fibre optic SFP+ transceiver modules from IndigoVision.

Notice *The Enterprise NVR-AS 4000 G3 2U only supports either the 1Gbps Ethernet pair or the 10Gbps Ethernet pair to be connected at any given time, not both.*

Fault monitoring

The Enterprise NVR-AS 4000 2U platforms provide hardware fault monitoring integrated with IndigoVision Control Center.

The following hardware is monitored:

- RAID arrays for video storage and the Operating System
- System fans
- Redundant power supplies (if installed)
- Network interfaces

The RAID arrays and fans are always monitored. The redundant power supplies and network interface fault monitoring must be configured before these components are monitored.

► For more information, *see "Status Monitoring" on page 34*

Notice *To effectively monitor the health of the IndigoVision unit, IndigoVision recommends that you create a Device Fault Detector for the NVR.*

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

iDRAC

The iDRAC (Integrated Dell Remote Access Controller) is embedded within every Enterprise NVR-AS 4000 and provides functionality that helps IT administrators deploy, update, monitor, and maintain servers with no need for any additional software to be installed. iDRAC functions regardless of operating system or hypervisor presence because it is embedded within each server from the factory, allowing it to be ready to work from a pre-OS or bare-metal state.

The iDRAC interface uses its own network interface which is located on the rear of the Enterprise NVR-AS 4000. This allows iDRAC to be accessed when the main OS is not responding or even when the host Operating System is powered down. This interface is not required in order for iDRAC to monitor the server hardware – it has internal connectivity that allows it to achieve this – however in order to access iDRAC regardless of the state of the host Operating System this interface must be connected to your network. By default the iDRAC interface will be configured via DHCP. The IP address it is using is shown on the BIOS screen when the system is powered on.

Notice *In order to access iDRAC when the host Operating System is powered down it requires that the Enterprise NVR-AS-4000 still has power going to it. If the power cables are unplugged or have no power iDRAC will not be accessible.*

► For more information, consult www.dell.com for documentation covering the version of iDRAC used by your system.

3 GETTING STARTED

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

Server installation

Follow the instructions provided in the Quick Start Guide to safely install the server.

Warning *Before installing the Enterprise NVR-AS 4000, review the safety instructions and guides provided with the system.*

Notice *Before installing a redundant PSU into the system, perform the initial configuration process.*

► For more information, *see "Install, replace or remove a redundant PSU" on page 20*

Installing additional disks (Enterprise NVR-AS 4000 G3 2U only)

To expand the disk capacity of a standard Enterprise NVR-AS 4000 G3 2U before commissioning it, delete the existing RAID6 virtual disk and recreate it.

► For more information, *see "Recreating RAID configuration using the BIOS" on page 26*

Notice *This operation must be completed before the Enterprise NVR-AS 4000 Operating System is booted for the first time. The Enterprise NVR-AS 4000 performs a self-test at first boot, as part of this process the storage array is formatted. If you have already completed the first boot you are required to manually format it.*

► For more information, *see "Formatting a storage array after rebuild" on page 28*

The following table outlines the options for expanding the capacity of the Enterprise NVR-AS 4000 G3 2U variants:

Table 1Expansion capacity and options

Variant	Initial disk count	Supported expansion options
48TB	8 x 8TB (48TB total when in RAID6 array)	9 (56TB), 10 (64TB), 11 (72TB), 12 (80TB)
100TB	12 x 10TB (100TB total when in RAID6 array)	13 (110TB), 14 (120TB)
140TB	16 x 10TB (140TB total when in RAID6 array)	17 (150TB), 18 (160TB)

Complete the initial system setup

Before you can configure the rest of the Enterprise 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 Enterprise 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 13*

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

Configuration

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

- Monitor and keyboard connected directly to the device

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

► For more information, *see "Configuration" on page 29*

DHCP

If your network supports DHCP connections, attach the device to the network and a valid IP address is automatically assigned. The Enterprise 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 the monitor and keyboard instructions.

Notice *The Enterprise NVR-AS 4000 2U platforms only support either the 1Gbps ethernet pair or the 10Gbps ethernet pair to be connected at any given time, not both.*

Using a monitor and keyboard

The Enterprise NVR-AS 4000 device can be configured by connecting a monitor to the VGA 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 Enterprise 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 chose 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 Enterprise 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 37*

Edge Storage Retrieval

The Enterprise NVR-AS 4000 2U Linux Appliances 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 30*.

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 Enterprise NVR-AS 4000 2U Linux Appliances 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.*

Caution *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 OPERATIONS

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

Disk management

Raid status monitoring and disk replacement uses the Dell™ OpenManage™ Server Administrator (OMSA). The OMSA can be started from the Enterprise NVR-AS 4000 Disk configuration page.

► For more information, *see "Disk" on page 31*

- When accessing the OMSA, Internet Explorer indicates that there is a problem with the website's security certificate unless the procedure in OMSA X.509 Certificate Management is followed. Click ***Continue to this website*** to open the OMSA.
  ► For more information, *see "OMSA X.509 Certificate Management" on page 23*
- The OMSA then requests credentials. Enter the user name `root` and the password currently set for the Web Configuration pages.

RAID redundancy

The Enterprise NVR- AS 4000 2U platforms use RAID1 for operating system and configuration information, and RAID6 for video storage.

A RAID1 array can tolerate a single disk failure. A RAID6 array can tolerate up to two disks failing.

If a disk fails, it must receive attention at the earliest opportunity to maintain maximum array redundancy.

Notice *IndigoVision recommend you create a Device Fault Detector for the NVR in order to receive alarms if the video storage array is degraded.*

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

Replacing a faulty disk

Caution ***Do not remove disks unnecessarily while the device is in operation. This causes the system to consider the disk as failed.***

Caution

Power off the NVR before attempting to examine or replace any internal disks.

Caution

Always use ESD protection when examining or replacing the components inside the NVR.

When the Dell OpenManage Server Administrator (OMSA) reports that a disk is faulty, it must be replaced as soon as possible. Contact IndigoVision Technical Support to arrange for a replacement to be supplied.

Notice

The disks installed in the Enterprise NVR-AS 4000 2U variants have different part numbers dependent on where they are located and whether they are video storage disks or not. Before ordering replacements, be sure to obtain the part number of the actual disk that is malfunctioning.

- **Use the OMSA to put the faulty disk offline.**
  ► **For more information,** ***see "Taking a disk offline" on page 18***
- **Remove the faulty disk and replace it with a disk of the same capacity.**
- **The RAID controller automatically incorporates the replacement disk and starts rebuilding the array.**
- **Confirm that the disk is incorporated into the array and has started rebuilding using the OMSA.**
- **In some cases the disk may need to be manually added as a hot spare. Shortly after adding a new disk, the controller starts rebuilding the new disk.**

If two disks fail at the same time, do the following:

- **Replace one disk and allow it to completely rebuild.**
- **After the first disk has completely rebuilt and the array has redundancy, replace the second disk**

Taking a disk offline

Caution

Before a disk is physically removed from an Enterprise NVR-AS 4000 it must first be taken offline using the OMSA.

To take a disk offline, do the following:

1. **Open the OMSA**
2. **Expand the** *Storage node* in the right hand pane
3. Expand the *PERC H730* node
4. Expand the *Connector 0* node
5. Expand the *Enclosure* node
6. Select the *Physical Disks* node
7. Select *Offline...* from the Tasks drop down that corresponds to the disk you want to take offline
8. Click *Execute* that corresponds to the disk you want to put offline

9. Use the displayed confirmation page to confirm you are taking the correct disk offline
10. When you are confident you are taking the correct disk offline click ***Offline***
11. Click ***OK***

Whole storage array replacement

Whole storage array replacement allows a running storage array to be archived.

Archiving a storage array

You can archive the storage array by removing the disk array.

1. Press the front panel button on the Enterprise NVR-AS 4000 or use the shutdown button on the Diagnostics Web Configuration page to safely shut down the unit.
2. Remove the entire storage disk array.

Caution

Label the disks appropriately to ensure you can identify them at a later date.

After you have removed the disk array, you can replace them with one of the following:

- An archived disk array,
- A new set of disks that can be configured as a blank storage array.

Restoring an archived storage array

You can restore an archive storage array by replacing the archived disk array in an Enterprise NVR-AS 4000 that contains no storage disks.

Before starting this procedure, ensure the Enterprise NVR-AS 4000 is powered off and has no storage disks.

Notice

When restoring an archived storage array, all disks from the archived array must be inserted into the NVR.

1. Insert the complete archived video storage disk array that is to be restored.
2. Power on the device.
3. Within the BIOS or using the OMSA, import the foreign disk array configuration.
   - For more information, *see "Importing or clearing a foreign array configuration" on page 28*
4. Reboot the Enterprise NVR-AS 4000.

The Enterprise NVR-AS 4000 is now running with the restored storage array.

Inserting new disks to create a new storage array

You can add new disks to create a blank storage array.

Before starting this procedure, ensure the Enterprise NVR-AS 4000 is powered off and has no storage disks.

1. Insert an array of at least 8 disks that are either blank or can be erased.

Notice *The Enterprise NVR-AS 4000 G3 2U supports a storage array containing any number of disks between 8 and 18.*

2. Power on the device.
3. Within the BIOS or using the OMSA, clear any foreign storage disk array configuration.
   - ► For more information, *see "Importing or clearing a foreign array configuration" on page 28*
4. Within the BIOS or using the OMSA, configure the new disks.
   - ► For more information on the settings to use, *see "RAID configuration" on page 26*
   - ► For more information on setting up the disk from the BIOS, *see "Recreating RAID configuration using the BIOS" on page 26*
5. Format the storage array.
   - ► For more information on the settings to use, *see "Formatting a storage array after rebuild" on page 28*

The Enterprise NVR-AS 4000 is now running with a newly created storage array.

Install, replace or remove a redundant PSU

Redundant PSUs are manually installed, replaced and removed from the Enterprise NVR-AS 4000.

Install a redundant PSU

Notice ***Before installing a redundant PSU, perform the initial configuration for the Enterprise NVR-AS 4000.***

► **For more information, *see "Getting Started" on page 11***

To add a second PSU to the unit, do the following:

1. **If installed, remove the power supply unit blank plate.**
2. **Slide the new PSU into the chassis until the power supply unit is fully seated and the release latch snaps into place.**
3. **Attach the AC power cable to the new PSU.**
4. **Wait for 15 seconds for the system to recognize the power supply unit and determine its status.**

   The power supply redundancy may not occur until discovery is complete.

   The power supply unit status indicator turns green to signify that the power supply unit is functioning correctly.

Notice ***The next time the unit reboots, it may go through an automatic configuration stage including a two-minute power-off period. At the end of this process, the unit automatically reboots and starts normally.***

Redundant power can be monitored through Control Center by using an NVR Fault Detector.

Replace a redundant PSU

Caution

When replacing a redundant PSU, ensure that the other PSU is fully operational. Loss of power may lead to corrupt or lost data.

To replace a PSU in the unit:

1. **Remove the faulty PSU from the unit.**
2. **Slide the new PSU into the chassis until the power supply unit is fully seated and the release latch snaps into place.**
3. **Attach the AC power cable to the new PSU.**
4. **Wait for 15 seconds for the system to recognize the power supply unit and determine its status.**

   The power supply redundancy may not occur until discovery is complete.

   The power supply unit status indicator turns green to signify that the power supply unit is functioning correctly.

Notice

It can take up to a minute for any configured NVR Fault Detectors monitoring this NVR-AS to deactivate after redundant power is restored.

Remove a redundant PSU

Caution

When removing a redundant PSU, ensure that the other PSU is fully operational. Loss of power may lead to corrupt or lost data.

To remove a secondary PSU from the unit:

1. **Disconnect AC power from the PSU to be removed.**
2. **Remove the PSU.**

The removed PSU remains in the system inventory until the following steps are carried out:

1. **Power down the unit using the web configuration Diagnostics page**
   ► **For more information, *see "Diagnostics" on page 39***
2. **Remove AC power from the remaining PSU for at least 15 seconds.**
3. **Re-attach AC power to the remaining PSU and start the unit normally.**

Notice

Any configured NVR Fault Detectors monitoring this NVR-AS remain activated until the 'Redundant PSU failure' alert is unchecked on the Status Monitoring *page.*

► For more information, *see "Status Monitoring" on page 34*

Install a new license or update an existing license

You can configure the Enterprise 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 Enterprise NVR-AS 4000 to act as a License Server, make sure that there are no other License Servers active in your site.*

Notice *The Enterprise NVR-AS 4000 may 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 Enterprise 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 instance of the IndigoVision NVR-AS application running on third-party hardware in your site.

The trial period starts when you first configure the Enterprise 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 Enterprise NVR-AS 4000.

Create and send a fingerprint file

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

1. Access the Enterprise 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 Enterprise NVR-AS 4000.

1. Access the Enterprise 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.

OMSA X.509 Certificate Management

This section describes how to manage X.509 certificates with the Dell™ OpenManage™ Server Administrator (OMSA).

► For more information about how to access OMSA, *see "Disk management" on page 17*

Web certificates are necessary to ensure the identity of a remote system and ensure that information exchanged with the remote system are not viewed or changed by others.

To ensure system security, IndigoVision recommends that you do the following:

- Generate a new X.509 certificate, reuse an existing X.509 certificate or import a certificate chain from a Certification Authority (CA).
- Ensure that all systems that have Server Administrator installed have unique host names.

To manage X.509 certificates through the Preferences home page, click ***General Settings > Web Server > X.509 Certificate***.

The following options are displayed:

- **Generate a new certificate** – Generates a new self-signed certificate used for SSL communication between the server running Server Administrator and the browser.

Notice *When you are using a self-signed certificate, most web browsers display an untrusted warning, because the self-signed certificate is not signed by a Certificate Authority (CA) trusted by the operating system. Some secure browser settings can also block the self-signed SSL certificates. The Server Administrator web GUI requires a CA-signed certificate for such secure browsers.*

- **Certificate Maintenance** – Allows you to generate a Certificate Signing Request (CSR) containing all the certificate information about the host required by the CA to automate the creation of a trusted SSL web certificate. You can retrieve the necessary CSR file either from the instructions on the

  Certificate Signing Request (CSR) page or by copying the entire text in the text box on the CSR page and pasting it in the CA submit form. The text must be in the Base64-encoded format.

Notice *You also have an option to view the certificate information and export the certificate that is being used in the Base64-encoded format, which can be imported by other web services.*

- **Import certificate chain** – Allows you to import the certificate chain (in PKCS#7 format) signed by a trusted CA. The certificate can be in DER or Base64-encoded format.
- **Import a PKCS12 Keystore** – Allows you to import a PKCS#12 keystore that replaces the private key and certificate used in Server Administrator web server.

  PKCS#12 is a public keystore that contains a private key and the certificate for a web server. Server Administrator uses the Java KeyStore (JKS) format to store the SSL certificates and its private key.

  Importing a PKCS#12 keystore to Server Administrator deletes the keystore entries, and imports a private key and certificate entries to the Server Administrator JKS.

Notice ***An error message is displayed if you select an invalid PKCS file or type an incorrect password.***

SSL Server Certificates

Server Administrator Web server is configured to use the industry-standard SSL security protocol to transfer encrypted data over a network. The SSL security protocol is built on an asymmetric encryption technology. SSL is widely accepted for providing authenticated and encrypted communication between clients and servers, to prevent eavesdropping across a network.

An SSL-enabled system can perform the following tasks:

- Authenticate itself to an SSL-enabled client
- Allow the two systems to establish an encrypted connection

The encryption process provides a high level of data protection. Server Administrator uses the most secure form of encryption generally available for Internet browsers in North America.

Server Administrator Web server has a Dell self-signed unique SSL digital certificate by default. You can replace the default SSL certificate with a certificate signed by a well-known Certificate Authority (CA).

A Certificate Authority is a business entity that is recognized in the Information Technology industry for meeting high standards of reliable screening, identification, and other important security criteria. Examples of CAs include Thawte and VeriSign.

To obtain and install a CA-signed certificate, do the following:

1. Use the Server Administrator Web interface to generate a Certificate Signing Request (CSR) with your company's information.
2. Submit the generated CSR to a CA such as VeriSign or Thawte. The CA can be a root CA or an intermediate CA.

   The CA will return a signed SSL certificate.
3. Upload the certificate to Server Administrator.

   In the certificate store of the management station, install the SSL certificates of each Server Administrator which you want to be trusted by the management station.

After the SSL certificate is installed in the management stations, supported browsers can access Server Administrator without certificate warnings.

5 MAINTENANCE

This chapter describes procedures and information required for the maintenance of the Enterprise NVR-AS 4000.

Recover system using USB Restore Media

If the Enterprise NVR-AS 4000 becomes inoperable the USB Restore Media can be used to restore the unit to its original system software.

Caution

This procedure deletes all data on the OS Virtual Disk. You will lose all configuration and alarms. You will lose all video footage if you also delete the video Virtual Disk.

Before restoring the system software, replace any faulty hardware and recreate the RAID arrays.

- For more information about faulty disk replacement, *see "Replacing a faulty disk" on page 17*
- For more information about RAID configuration, *see "RAID configuration" on page 26*

After the hardware is installed and configured, use the following procedure to recover the system software:

1. Shut down the unit so that it is powered off.
   Ensure the keyboard, mouse and monitor are attached.
2. Remove any other USB devices.

Caution

Ensure you use the USB Restore Media supplied with the specific Enterprise NVR-AS 4000 system you are recovering.

3. Insert the USB Restore Media.
4. Power on the Enterprise NVR-AS 4000.
   Wait for the keyboard shortcuts to be displayed at the top of the screen.
5. When the keyboard shortcuts appear, press ***F11***.
6. Select ***One-shot BIOS Boot Menu***.
7. Select the entry corresponding to the USB Restore Media.
   The Enterprise NVR-AS 4000 boots from the USB Restore Media and displays the restore instructions.
8. Select ***Restore***. A confirmation dialog opens.
9. Select ***Continue***. The restore process starts.
   The re-imaging process takes 5 to 10 minutes.

10. Select ***Reboot*** when the restore has completed.
11. Remove the USB Restore Media as soon as the reboot process starts.

The Enterprise NVR-AS 4000 re-starts with its factory system software.

RAID configuration

The configuration of the disks on the Enterprise NVR-AS 4000 2U is as follows:

- The two internal system disks are configured as a RAID1 mirror, using all of the available capacity, and with the following options:
  - Read Ahead
  - Write Back caching
  - 64KB Stripe Element Size
  - Disk cache disabled
- The disks used for video storage are configured as a RAID6 array, using all of the available capacity, and with the following options:
  - Read Ahead
  - Write Back caching
  - 128KB Stripe Element Size
  - Disk cache disabled

Notice

The Enterprise NVR-AS 4000 G3 2U (140TB) shows two RAID controllers:

- *BOSS-S1 controller: this should contain two physical disks with which to create the RAID1 array*
- *PERC H730 controller: this should contain the physical disks with which to create the RAID6 array*

The configuration settings to apply to each array are unchanged, with the exception of 'Read Ahead', which is not applicable to the BOSS-S1 controller.

Recreating RAID configuration using the BIOS

Caution

The following instructions for deleting a Virtual Disk will destroy all data on that disk. If the OS Virtual Disk is deleted, the operating system will be destroyed and the system will need to be recovered from the USB Restore Media, after which you will lose all configuration and alarms. If the video Virtual Disk is deleted, you will lose all video footage.

► **For more information, *see "Recover system using USB Restore Media" on page 25***

To reconfigure the RAID array in the BIOS:

1. **Ensure that a keyboard and monitor are connected to the unit.**
2. **Power up the unit, or reboot it if it is already powered on.**
3. **Early in the boot process, press F2 to enter System Setup.**
4. **Select** *Device Settings*.
5. Select the entry for the RAID Controller Configuration Utility:

a. ***BOSS-S1*** for OS Virtual Disk on the 140TB variant of the Enterprise NVR-AS 4000 G3 2U.
b. ***PERC H730P*** for anything else.

6. Select ***Virtual Disk Management***.

Notice *There may be existing foreign configurations that need to be imported or cleared.*

► For more information, *see "Importing or clearing a foreign array configuration" on page 28*

Delete any existing broken virtual disks as necessary:

1. Select the Virtual Disk you want to delete.
2. Change the operation to ***Delete Virtual Disk***.
3. Click ***Go***.

   When you finish deleting the required virtual disks, click ***Back*** to return to the **Main Menu** of the RAID Controller Configuration Utility.

Recreate any virtual disks as necessary by following this procedure:

1. Select ***Configuration Management***.
2. Select ***Create Virtual Disk***.

   If this option is disabled, press ***Escape*** to leave the ***Virtual Disk Operations*** menu and select ***Virtual Disk Operations*** again.
3. Select the desired RAID level.
   ► For more information, See "RAID configuration" on page 26
4. Select ***Unconfigured Capacity*** for the Virtual Disk allocation.
5. Click ***Select Physical Disks***.
   - If required, change ***Select Media Type*** to `Both`.
   - If required, change ***Select Interface Type*** to `Both`.
6. Select the check box beside all of the disks on which Virtual Disks should be created.
7. Make sure that the expected number of disks are selected.
8. Click ***Apply Changes***.
9. Select the settings for the new Virtual Disk as previously specified.
   ► For more information, *see "RAID configuration" on page 26*
10. Set the ***Default Initialization*** option to ***Fast***.
11. Click ***Create Virtual Disk***.
12. Repeat for the remaining Virtual Disks as necessary.

When completed, your system should have two Virtual Disks configured:

- Virtual Disk for the OS
- Virtual Disk for the Storage

Notice *If the operating system is not being recovered using a USB Restore Media, prepare the video storage with `diskprep -s` after the system is running again. This command attempts to reuse any existing filesystems, but will reformat them when necessary.*

Importing or clearing a foreign array configuration

Using the BIOS:

1. Press ***F2*** during boot to get into BIOS configuration
2. Select ***Device Settings***
3. Select the entry for the RAID Controller Configuration Utility:
   a. ***BOSS-S1*** for OS Virtual Disk on the 140TB variant of the Enterprise NVR-AS 4000 G3 2U.
   b. ***PERC H730P*** for anything else.
4. Select ***Configuration Management > Manage Foreign Configuration > Preview Foreign Configuration***
5. Select ***Import Foreign Configuration*** or ***Clear Foreign Configuration***
6. Follow the instructions

Using the OMSA:

1. Open the OMSA
2. Select the ***Storage*** node in the OMSA explorer
3. The RAID controller has an Available Tasks drop-down in the main window: select ***Foreign Configuration Operations...***
4. On the Foreign Configuration Preview page, click either ***Clear*** or ***Import/Recover***
5. Follow the instructions

   After the import has completed, the browser returns to the main page for the Storage node and the imported Virtual Disk is visible under the RAID controller in the main window.

Formatting a storage array after rebuild

If you have rebuilt or replaced the video storage virtual disk array, it will need to be formatted ready for use. This is typically done by the self-test on initial power-on, but if you need to repeat the process manually, use the following steps:

1. Log in to the system's Web Configuration pages
2. Select ***Disk*** in the left hand pane
3. Click ***Format***
4. Wait for the Enterprise NVR-AS 4000 to complete the operation

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.

Caution

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 Enterprise NVR-AS 4000 device and its operational status.

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

  If the label is set to ***Licensed***, then the Enterprise 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 Enterprise 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.
- **NVR 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 12*.

- **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 13*.

- **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.
- **Master Time Server** – Check this option if the NVR-AS device is expected to serve as a master 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 array status and update its configuration.

- **Array Status** – This indicates the overall status of the video storage array. The status can be as follows:
  - **Array OK** – The video storage is functioning normally.

- **Array Blank** – The video storage array has not been formatted with a filesystem. This status may be seen if you are in the process of replacing the array. Press ***Format*** to format the array and the status should change to ***OK***.
- **Array Degraded** – The video storage array redundancy is degraded. Check OMSA for details of the disks involved.

Notice *When the storage array is first built, it will need to spend a considerable amount of time performing background initialisation. During this time, the disk will be usable, but will show as 'Array Degraded'*

- **Array Rebuilding** – The video storage array is rebuilding. Check OMSA for progress of this operation.
- **Array Error** – There is a fault with the video storage array, such that the NVR-AS cannot function. Contact Technical Support.

- **Storage Space** – This figure indicates the total storage space on the disk array.
- **Used Space** – Shows the percentage of disk space currently used.
- **Array Maintenance:**
  - **Open Window** – Click ***Open Window*** to open the Open Manage Server Administrator (OMSA) interface for this unit. OMSA can be used to monitor the state of the video storage array and other hardware components on the unit.

Caution *Note that using OMSA to delete or create the video storage array when the NVR is running is not supported, and could lead to system instability and data loss.*

  - **Format Array** – Reformats the disk array.
- **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.

Caution

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.

Caution

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.

  Changing this setting also affects the amount of free disk space that the NVR maintains. To maximize the retention of footage on your NVR, set the Maximum Recording Streams to the maximum number of simultaneous recording jobs that you intend to configure through Control Center.

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.

- **PSU Redundancy** – Displays whether the unit currently has redundant power through it's power supplies.
- **Network Redundancy** – Displays the state of the network ports that have been configured for monitoring.
- **Fan Status** – Displays any fan failures on the unit. For additional information on any indicated failures, open OMSA from the ***Disk*** page.
  ► For more information, *see "Disk" on page 31*.
- **Generate Alerts** – Configure alerts for the following faults:
  - **Redundant PSU Failure** – If checked, the Enterprise NVR-AS 4000 generates an alert when it does not have redundant power through its power supplies. If the unit has been intentionally installed without redundant power, this can be unchecked to avoid unnecessary alerts.
  - **Network Link Failure** – If checked, the Enterprise NVR-AS 4000 generates an alert when any of the selected Ethernet ports are not connected to a network switch.

Alerts will always be generated in Control Center for video storage array faults, complete network failure (device unavailable) or fan failures.

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 12*

NVR-AS Authentication

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

Caution *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.

Caution *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 13*****.**

- **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`.

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 Enterprise 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 Enterprise NVR-AS 4000.

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

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

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

- The Enterprise NVR-AS 4000 can use an existing License Server running on a separate device specified using the License Server's IP address

- The Enterprise 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 Enterprise 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 Enterprise 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 Enterprise NVR-AS 4000 as a License Server.*

License Management

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

► For more information, *see "Install a new license or update an existing license" on page 22*

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.

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.