IndigoVision

Enterprise NVR-AS 4000 Windows Appliance

User Guide

IndigoVision

THIS MANUAL WAS CREATED ON MONDAY, NOVEMBER 12, 2018.

DOCUMENT ID: IU-NVR-MAN011-18

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 Limited

Charles Darwin House,
The Edinburgh Technopole,
Edinburgh,
EH26 0PY

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 IndigoVision's Enterprise NVR-AS 4000 and provides an overview of the Enterprise NVR- AS 4000 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 - Windows Appliance is part of IndigoVision's Control Center suite. It provides 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 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 provides the following features:

- Record and playback MJPEG, JPEG 2000, MPEG-4, and H.264 video and audio streams
- Full frame rate recording of up to 200 streams (2U/G3 2U variants) with simultaneous playback of up to 25 streams (up to 100 streams on Enterprise NVR-AS 4000 G3 2U)
- Third party camera support
- RAID storage resilience and redundant power and network connections
- Powerful and distributed alarm management
- Digital Signatures and Tamper Protection of recordings
- Integrated hardware fault monitoring

Additionally the Enterprise NVR-AS 4000 includes the IndigoVision Video Stream Manager (VSM) which enables cameras from a range of other manufacturers to be seamlessly integrated with the IndigoVision Control Center suite by using the industry standard RTSP protocol.

The VSM also provides powerful and integrated enterprise management of ultra-high resolution JPEG2000 video from Ultra 5K Fixed Cameras.

- Support for up to 1000 RTSP cameras.
- Support for up to 10 Ultra 5K Fixed cameras on the Enterprise NVR-AS 4000 2U/G3 2U and 2 Ultra 5K Fixed cameras on the Enterprise NVR-AS 4000 1U.

Hardware

The Enterprise NVR-AS 4000 is available as a 1U or 2U rack mounted chassis. Two generations of 2U platforms are supported - the 2U and G3 2U.

Enterprise NVR-AS 4000 1U variant

The Enterprise NVR-AS 4000 1U variant has four hot-swappable hard-disk bays, accessible from the front of the device. The disks in these bays are configured as a RAID5 array. This array is used for the operating system, configuration information and for video storage.

Figure 1: Enterprise NVR-AS 40001U

This variant has two 1Gbps Ethernet ports which are aggregated for greater throughput and redundancy.

Enterprise NVR-AS 4000 2U variant

The Enterprise NVR-AS 4000 2U variant 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 2: Enterprise NVR-AS 4000 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 variant 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 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 variant

The Enterprise NVR-AS 4000 G3 2U variant 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 3: Enterprise NVR-AS 4000 2U/G3

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 separate redundant pairs.

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.*

Notice *The Enterprise NVR-AS 4000G3 2U has its Ethernet ports configured to work with a network switch with no LACP aggregation configured. If LACP aggregation is configured on the switch, the NVR will need to be reconfigured to match.*

Fault monitoring

The Enterprise NVR-AS 4000 provides 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 redundant power supply and network interface monitoring must be configured before it is enabled.

► For more information, refer to the NVR Admin Guide.

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.

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 from the Enterprise NVR-AS 4000 2U/G3 2U variant" on page 23*

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

If you intend 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 31*

Notice *This operation must be completed before the NVR is powered up for the first time. On first-time boot, the NVR should complete the job of configuring the modified RAID6 array as part of running First Boot Wizard. If you have already run the First Boot Wizard, format the storage array.*

► For more information, *see "Formatting Storage Array after Rebuild" on page 33*

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

Table 1: Expansion 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 operating system setup

When you power up the Enterprise NVR-AS 4000 for the first time, Windows performs initial configuration. During the initial configuration:

- Specify the location settings
- Read and accept the Windows license agreement
- Define the administrator password.
  The password must meet the following criteria.
  - Be at least six characters in length
  - Contain characters from three of the following four categories:
    English uppercase characters (A through Z)
    English lowercase characters (a through z)
    Base 10 digits (0 through 9)
    Non-alphabetic characters (for example, !, $, #, %)

During this process, Windows may reboot a number of times.

On delivery, the Enterprise NVR-AS 4000 RAID arrays commence a background initialization process. During this operation the RAID array is fully operational but does not have full redundancy until it completes.

After Windows configuration is complete and you login for the first time, the Enterprise NVR-AS 4000 Installation Wizard opens. There are currently two versions of installation wizard supported, with slightly different functionality. The version of the Installation Wizard can be found in the wizard's title bar.

If no version number is present, the wizard can be assumed to be pre-15.3.

Installation wizards before version 15.3

The installation wizard will present a series of pages allowing the following tasks to be performed:

- Read and accept the IndigoVision license agreement.
- Specify a Name and Location for the device.
- Specify the IndigoVision License Server for the device.

Notice *If you do not already have a compatible deployed IndigoVision License Server, a local License Server should be set up via the installation wizard in order to allow the wizard to complete successfully.*

On completing the wizard, it performs device configuration and prepares the video storage. If you don't complete the wizard, you are prompted to do so again the next time Windows starts up.


Warning

Do not interrupt device configuration and storage preparation after it has started.

When the configuration process has finished, Windows reboots. After the reboot, the Enterprise NVR-AS 4000 is fully operational.

You can now configure the rest of the Enterprise NVR-AS 4000 settings. By default the network interfaces are configured to use DHCP.

Installation wizards from version 15.3 onwards

The installation wizard will present a series of pages allowing the following tasks to be performed:

- Read and accept the IndigoVision license agreement.
- Install a local IndigoVision License Server for the device

On completing the wizard, it launches the NVR Administrator tool in order to complete NVR setup. If you don't complete the wizard, you are prompted to do so again the next time Windows starts up. Once the NVR Administrator tool has completed, the Enterprise NVR-AS 4000 is fully operational.

Notice *If you do not install a local License Server and do not have an existing compatible deployed IndigoVision License Server available, it is possible to complete initial setup by simply leaving the License Server field in the NVR-AS Administrator tool blank. While this will allow setup to complete, the NVR will not be able to record/playback video until it has been configured to use a compatible License Server.*

► For more information, *see "IndigoVision License Server configuration" on page 13*

You can now configure the rest of the Enterprise NVR-AS 4000 settings. By default the network interfaces are configured to use DHCP.

IndigoVision License Server configuration

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.

For existing Control Center sites the IP address of the License Server should be entered during first boot configuration.

The Enterprise NVR-AS 4000 Installation Wizard offers the ability to configure this Enterprise NVR-AS 4000 to act as a License Server for a Control Center site. When this option is selected a time-limited trial of Control Center is started. To continue to use Control Center an appropriate license should be purchased.

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.*

Caution *Configuring the Enterprise NVR-AS 4000 device to act as a License Server will start the time limited trial license.*

Configuration

You must configure the following settings to complete the Enterprise NVR-AS 4000 setup.

- Date and time settings
- Network settings
- Network teaming
- Remote desktop configuration

Date and time settings

Caution *All devices in the IndigoVision system, including the Enterprise NVR-AS 4000, must be time synchronized using the same NTP hierachy. If they are not, warnings are issued, and certain functionality may not behave correctly, including aspects of video playback.*

Adding upstream time servers

1. Open the file ***C:\Program Files (x86)\NTP\etc\ntp.conf*** in a text editor. See **Figure 4:** on page 15 for an example configuration file.
2. Add the upstream NTP server following the format in the configuration file.
   For example to add an NTP server with IP address 192.168.1.1, add the following line:
   ```
   server 192.168.1.1 iburst
   ```
3. Add further server configuration lines for any additional upstream NTP servers.
4. Save and close the configuration file.
5. Restart the NTP service by selecting ***Restart NTP Service*** from the Start screen.

```
# NTP Network Time Protocol configuration
#
# You have to restart the NTP service when you change this file to apply the
# changes.
#
# Please refer to the Enterprise NVR-AS 4000 User Guide for more information.
```

```
#
# The NTP server is configured to allow client synchronization but access to
# service monitoring is restricted to the local machine only.
#
restrict default limited kod nomodify notrap noquery
restrict 127.0.0.1
restrict -6 default limited kod nomodify notrap noquery
restrict -6 ::1
# The driftfile is stored in the following location. There should be no need
# to modify this line.
driftfile "C:\Program Files (x86)\NTP\etc\ntp.drift"
#
# The following enables the local system clock as a time source.
# If this NVR-AS 4000 will act as a master time server on a local area network
# when the configured NTP servers are not available, the stratum value should
# be changed. Refer to the Enterprise NVR-AS 4000 User Guide for more
# information.
#
server 127.127.1.0
fudge 127.127.1.0 stratum 12
# Add upstream NTP servers below. For example:
# server 192.168.1.1 iburst
```

Figure 4: Example configuration file

Removing upstream time servers

1. Open the file ***C:\Program Files (x86)\NTP\etc\ntp.conf*** in a text editor. See **Figure 4:** on page 15 for an example configuration file.
2. Remove the line beginning with the IP address of the server you wish to remove.
3. Save and close the configuration file.
4. Restart the NTP service by selecting ***Restart NTP Service*** from the Start screen.

Master time server

If this Enterprise NVR-AS 4000 will act as a master time source for a local area network when the configured NTP servers are not available, then the stratum value for the local clock should be changed in the configuration file.

For other NVR-AS 4000 units, this setting should be left at the default of a stratum value of 12.

1. Open the file ***C:\Program Files (x86)\NTP\etc\ntp.conf*** in a text editor. See **Figure 4:** on page 15 for an example configuration file.
2. Find the following line in the configuration file:
   ```
   fudge 127.127.1.0 stratum 12
   ```
3. Change this line to the following:
   ```
   fudge 127.127.1.0 stratum 5
   ```
4. Save and close the configuration file.
5. Restart the NTP service by selecting ***Restart NTP Service*** from the Start screen.

For full documentation on the NTP configuration file format refer to www.ntp.org.

Time zone

Review the time zone setting of the device and change it if necessary.

1. Open the Control Panel.
2. Select ***Set the time and date***.
3. Adjust the time zone setting as required.

Network settings

The 1U and 2U/G3 2U Enterprise NVR-AS 4000 variants have different networking hardware options. All variants are configured to use DHCP by default and obtain network settings from the local DHCP server.

Change the network settings for the 1U variant

The 1U variant has four 1Gbps Ethernet ports configured as a single team.

1. Open the ***Network and Sharing Center > Adapter Settings***.
2. Right-click ***BASP Virtual Adapter*** and select ***Properties***.
3. Select ***Internet Protocol Version 4 (TCP/IPv4)*** and click ***Properties***.
4. Review and modify the settings as required.

Change the network settings for the 2U/G3 2U variants

The 2U/G3 2U variants have two 1Gbps Ethernet ports and two 10Gbps Ethernet ports configured as separate aggregated pairs.

Choose between these two connection options when installing the NVR-AS 4000.

To avoid confusion, IndigoVision recommend disabling the interface team that is not in use.

1. Open the ***Network and Sharing Center > Adapter Settings***.
2. Open the Properties dialog for the network ports.
   - For the 1Gbps network ports right-click ***1 Gbps Team*** and select ***Properties***.
   - For the 10Gbps network ports right-click ***10 Gbps Team*** and select ***Properties***.
3. Select ***Internet Protocol Version 4 (TCP/IPv4)*** and click ***Properties***.
4. Review and modify the settings as required.

Network teaming

Teaming behaviour varies between the 1U/2U variants and the G3 2U variant.

Enterprise NVR-AS 4000 1U and 2U variant

The network interfaces are configured to use 802.3ad Link Aggregation Control Protocol (LACP). LACP balances the network traffic across all of the interfaces and provides redundancy.

The ports on the network switch that are connected to the Enterprise NVR-AS 4000 should be configured for 802.3ad LACP to maximize performance. If the ports on the switch are not correctly configured for LACP, the Enterprise NVR-AS 4000 is still accessible from the network, but only a single link is used.

Enterprise NVR-AS 4000 G3 2U variant

For this variant, the network interfaces are configured as Switch Independent. This enables them to inter-operate with switches that do not have LACP configured. In this mode, outgoing traffic will be distributed over multiple links to maximize performance, but incoming traffic cannot be guaranteed to do so.

If the ports on the switch are configured for LACP, the Enterprise NVR-AS 4000 will also need to be reconfigured to use LACP.

Remote desktop configuration

Remote desktop is disabled by default. Enabling remote desktop updates the firewall rules to allow remote desktop connections.

1. Open the Control Panel.
2. Select ***System and Security > System > Remote settings***. The **System Properties** dialog opens.
3. Select the required **Remote Desktop** option.

   If ***Remote Desktop*** connections are allowed, a dialog opens to warn you of the firewall implications.
4. Click ***OK*** to confirm the additional firewall exception.
5. Click ***OK*** to close the **System Properties** dialog.

Windows Update

IndigoVision recommends that all Enterprise NVR-AS 4000 devices have Windows Update enabled and that updates are applied as soon as practicable after release.

The operating system must be regularly updated to ensure optimal security and performance level.

4 OPERATIONS

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

Disk management

Disk and array management uses the Dell™ OpenManage™ Server Administrator (OMSA). The OMSA can be started from the desktop shortcut or from the Start screen. These shortcuts open Internet Explorer with the correct URL to allow maintenance of the server.

- 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 26*
- The first time Internet Explorer is started on the Enterprise NVR-AS 4000, you will be asked to configure the security and compatibility settings. Either setting can be chosen without any affect on the OMSA.
- If the OMSA requests credentials, enter the user name `Administrator` and the administrator password currently set for the operating system.

RAID redundancy

The Enterprise NVR-AS 4000 1U variant uses RAID5 for all of the storage in the system: operating system, configuration and video footage.

The Enterprise NVR-AS 4000 2U/G3 2U variants use RAID1 for operating system and configuration information, and RAID6 for video storage.

A RAID1 or RAID5 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.*

- 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 in the Enterprise NVR-AS 4000 2U/G3 2U variant, 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

Whole storage array replacement

Whole storage array replacement is only possible on the 2U variants. This allows a running storage array to be archived.

Archiving a running storage array

You can archive the storage array from a 2U variant by removing the disk array.

1. Navigate to the **Services Panel** on the Enterprise NVR-AS 4000.
2. Stop the ***IndigoVision NVR-AS*** service.
3. Disable the ***IndigoVision NVR-AS*** service.
4. Shut down the device so that it powers off.
5. 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 either:

- An archived disk array, or
- 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 to a 2U variant 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 32*
4. From the operating system, ensure that the storage volume is present and that it has been assigned drive letter D.
5. In the **Services Panel**, enable but do not start the ***IndigoVision NVR-AS*** service.
6. Start the ***NVR-AS Administrator***, and complete the following checks:
   - Verify the video storage location is set correctly
   - Verify all other settings
   - Complete the Administrator wizard

   Confirm that you want the NVR-AS Administrator to restart the service when prompted. The NVR-AS Administrator restarts the service.

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 a 2U variant 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.
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 32*
4. Within the BIOS or from the OMSA, configure the new disks as a ***RAID6 Virtual Disk*** with ***128KB stripe size*** and enable ***write-back cache***.

5. From the operating system, format the volume as ***NTFS*** with ***64KB cluster size*** and assign it the drive letter ***D***.
6. In the **Services Panel**, enable but do not start the ***IndigoVision NVR-AS*** service.
7. Start the ***NVR-AS Administrator***, and complete the following checks:
   - Verify the video storage location is set correctly
   - Verify all other settings
   - Complete the Administrator wizard

   Confirm that you want the NVR-AS Administrator to restart the service when prompted. The NVR-AS Administrator restarts the service.

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

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 integrated RAID controller
4. Select ***Controller 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.

Expanding capacity

You can expand the video storage capacity of some configurations of NVR-AS 4000 in the field by populating the empty hot-swappable drive bays.

Notice *This operation may take several days to complete, depending on the nature of the change.*

Notice *Care must be taken when ordering new disks. Part numbers vary between disks stored in each of the different possible locations in the device. When adding drives to an existing RAID array, the new disks must have the same individual capacity as the existing ones.*

Caution

Due to the demanding nature of this operation, the device will not be able to reliably record video or provide alarm functionality for the initial stage of the expansion.

Caution

Ensure that the Enterprise NVR-AS 4000 is powered on for the entire duration of the operation.

Caution

Before starting the expansion procedure, ensure that the array is fully redundant.

1. Navigate to the **Services Panel**.
2. Stop the ***IndigoVision NVR-AS*** service.
3. Insert the additional disks.
4. Verify that all the physical disks are recognized using the OMSA.

   If the disks have been used previously in another RAID set, they may need their foreign configuration to be cleared.
5. Initiate a ***Reconfigure*** operation for the virtual disk using the OMSA.
6. Select the check boxes for all the new disks in the **Reconfiguration** wizard.
7. Select ***RAID6*** as the new RAID level.

   The RAID controller incorporates the disks into the array and starts performing the initial relocation of data.

   This may take a considerable amount of time to complete, depending on the extent of the relocation.

   Monitor the progress of the Reconfiguration in OMSA.

   After the OMSA indicates that the storage array is no longer performing a Reconfiguration and is performing a Background Initialization, go to the next step.
8. Expand the file system on the array to take up the new full capacity of the virtual disk.
   a. Navigate to the **Windows Server Manager**.
   b. Right-click ***Disk Management*** entry in the menu on the left, and select ***Rescan Disks***.

      The video storage volume should now have new unclaimed space next to it.
   c. Right-click the video storage volume and instruct the operating system to expand the video storage volume to fill the increased storage space.
9. In the **Services Panel**, start the ***IndigoVision NVR-AS*** service.

   The Background Initialization continues and takes approximately 25 hours to complete.

   The Enterprise NVR-AS 4000 is able to record video and provide alarm functionality while the Background Initialization completes.

Install, replace or remove a redundant PSU from the Enterprise NVR-AS 4000 2U/G3 2U variant

Redundant PSUs are manually installed, replaced and removed from the Enterprise NVR-AS 4000 2U/G3 2U variant.

Install a redundant PSU in the Enterprise NVR-AS 4000

Notice *Before installing a redundant PSU, perform the initial configuration for the Enterprise NVR-AS 4000 2U/G3 2U variant.*

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

To add a second PSU to the unit:

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 2 minute power-off period. At the end of this process, the unit automatically reboots and starts normally.*

Replace a redundant PSU in the Enterprise NVR-AS 4000

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 from the Enterprise NVR-AS 4000 2U/G3 2U variant

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.
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.

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.*

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 third-party Windows NVR-AS in your site.

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

For both of these steps, use the License Manager tool, which comes with the License Server standard installation.

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

Create a fingerprint file using the ***License Manager*** tool.

1. In the **License Manager**, select ***Request a new or updated IndigoVision license*** and click ***Next***.
2. Select where you want the **License Manager** to save a fingerprint file, and click ***Next***.

   The **License Manager** displays the following:
   - The location of the new fingerprint file
   - The contact details for IndigoVision Sales Orders

3. Send the fingerprint file to IndigoVision Sales Order with your IndigoVision order acknowledgment number.

IndigoVision then provides a license file.

Apply a license file

Use the ***License Manager*** tool to apply your IndigoVision license file to the License Server.

1. In the **License Manager**, select ***Apply a new or updated IndigoVision license*** and click ***Next***.
2. Select the IndigoVision license file, and click ***Next***.
   The **License Manager** displays a confirmation notification.
3. Click ***Finish***.
   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).

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 operating system disks.

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 20*
- For more information about RAID configuration for an Enterprise NVR-AS 4000 1U, *see "RAID configuration for an Enterprise NVR-AS 4000 1U " on page 30*
- For more information about RAID configuration for an Enterprise NVR-AS 4000 2U/G3 2U, *see "RAID configuration for an Enterprise NVR-AS 4000 2U/G3 2U" on page 30*

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. Press ***F2***.
   Wait for the system setup screen to appear.
6. Select ***System BIOS > Boot Settings***.
7. Change ***Boot Mode*** from `UEFI` to `BIOS`.
8. Save the changes and exit the system setup.
   The server reboots.

9. When the keyboard shortcuts appear, press ***F11***.
10. Select ***One-shot BIOS Boot Menu***.
11. 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.
12. Select ***Restore***. A confirmation dialog opens.
13. Select ***Continue***. The restore process starts.

    The re-imaging process takes 5 to 10 minutes.
14. Select ***Reboot*** when the restore has completed.
15. Remove the USB Restore Media as soon as the reboot process starts.
16. Press ***F2***.

    Wait for the system setup screen to appear.
17. Select ***System BIOS > Boot Settings***.
18. Change ***Boot Mode*** from `BIOS` to `UEFI`.
19. Save the changes and exit the system setup.

    The server reboots.

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

RAID configuration for an Enterprise NVR-AS 4000 1U

The four front-panel disks are configured as a virtual disk in a single RAID5 array.

Use the following options:

- No read ahead
- Write through caching
- 64KB Stripe element size
- Disk cache enabled

RAID configuration for an Enterprise NVR-AS 4000 2U/G3 2U

The configuration of the disks on the Enterprise NVR-AS 4000 2U/G3 2U is:

- The two internal system disks are configured as a RAID1 mirror, with options:
  - Read Ahead
  - Write Back caching
  - 64KB Stripe Element Size
  - Disk cache enabled
- The disks used for video storage are configured as a RAID6 array, with options:
  - Read Ahead
  - Write Back caching
  - 128KB Stripe Element Size
  - Disk cache enabled

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

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

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 > Integrated RAID Controller 1.
5. Select Virtual Disk Management.

Notice *On an Enterprise NVR-AS 4000 G3 2U, there are potentially multiple controllers in use.*

*To recreate the OS/config RAID array on the 140TB version, select **Device Settings> AHCI Controller** in **Slot 1: BOSS-S1 Configuration Utility**.*

*Otherwise select **Device Settings > Integrated RAID Controller 1: Dell PERC <PERC H730P Mini> Configuration Utility**.*

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 32*

Delete any existing broken virtual disks as necessary:

Caution *The following instructions for deleting a Virtual Disk will destroy all data on that disk. If the OS Virtual Disk is deleted, you will lose all configuration and alarms. If the video Virtual Disk is deleted, you will lose all video footage.*

Notice *Deleting and recreating the Virtual Disk containing the operating system requires the USB Restore Media to be used.*

► For more information, *see "Recover system using USB Restore Media" on page 29*

1. Select ***Virtual Disk Operations***.
2. Select the Virtual Disk to be deleted.

3. Click ***Delete Virtual Disk*** and confirm the action.
4. Repeat for the remaining Virtual Disks as necessary.

Recreate any virtual disks as necessary by following this procedure:

1. Select ***Create Virtual Disk***.

   If this option is disabled, press ***Escape*** to leave the Virtual Disk Operations menu and select ***Virtual Disk Operations*** again.
2. Select the desired RAID level.
   - If creating a Virtual Disk on a set of physical disks that are currently unused, select ***Unconfigured Capacity***.
   - If creating a Virtual Disk on a set of physical disks that already have some space allocated to a Virtual Disk, select ***Free Capacity***.
3. Click ***Select Physical Disks***.
   - If necessary, change ***Select Media Type*** to `Both`.
   - If necessary, change ***Select Interface Type*** to `Both`.
4. Select the check box beside all of the disks on which Virtual Disks should be created.
5. Make sure that the expected number of disks are selected.
6. Click ***Apply Changes***.
7. Select the settings for the new Virtual Disk as previously specified.
8. Set the ***Default Initialization*** option to ***Fast***.
9. Click ***Create Virtual Disk***.
10. Repeat for the remaining Virtual Disks as 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 integrated RAID controller
4. Select ***Controller 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 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 First Boot Wizard on initial power-on, but if you need to repeat the process manually, follow these steps on the Windows desktop:

1. Navigate to the Services Panel on the Enterprise NVR-AS 4000.
2. Ensure the IndigoVision NVR-AS service is enabled but stopped.
3. From the operating system, format the volume as NTFS with 64KB cluster size and assign it the drive letter D.
4. Start the NVR-AS Administrator, and complete the following checks:
   - Verify the video storage location is set correctly
   - Verify all other settings

   Complete the Administrator wizard

   Confirm that you want the NVR-AS Administrator to restart the service when prompted.

   The NVR-AS Administrator restarts the service.

6 SOFTWARE DESCRIPTION

This chapter provides a description of the configuration dialogs for the Enterprise NVR-AS 4000.

The Enterprise NVR-AS 4000 is configured using the NVR-AS Administrator. You can access this tool via the Start screen:

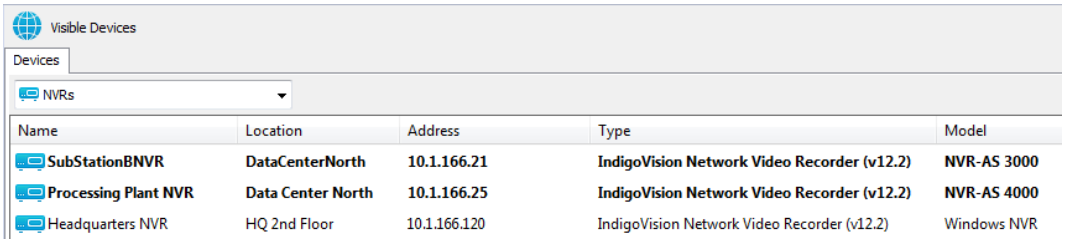
Start > IndigoVision > NVR-AS Administrator

Caution

It is not possible to use the NVR-AS Administrator until you have completed the initial installation of your Enterprise NVR-AS 4000.

Identification dialog

Enter the server (NVR-AS) name and location as required. These are the name and location that are used by IndigoVision Control Center and other client applications.



License Server Details dialog

Use this dialog to configure the License Server which the NVR-AS uses.

- **License Server Address**: The IP address of the machine hosting the License Server software.

Storage Locations dialog

Use this dialog to specify the locations where data is stored.

- **Video**: Specify the path to the video library (where recordings are stored)
- **Configuration**: Specify the path to the folder containing configuration information

  Click ... to browse to the required locations.
- **Advanced Configuration**: Select ***Override Database Paths*** if you wish to store the Alarm and/or Bookmark databases in a location other than the default. This can

improve performance when configuring an NVR-AS to review archived footage, alarms, and bookmarks.

Network Settings dialog

Use this dialog to configure the NVR-AS network settings.

- **Recording Stream Limit**: This setting specifies a limit for the number of recording streams (1-200) on the NVR-AS. Use this setting to avoid exceeding the NVR-AS recording capability (typically limited by storage bandwidth).
- **Playback Bandwidth Management**: Select ***Enable*** to manage the playback bandwidth.
  - **Bandwidth Management Address**: This is the IP address of the machine hosting the bandwidth manager.
  - **Bandwidth Limit**: This is the maximum bandwidth available to a playback session. The bandwidth is shared between all playback streams in a session.
- **NVR-AS IP Address**: This is the IP address on the local machine that the NVR-AS uses to communicate with Control Center and IndigoVision transmitters. This option is only available on systems that have multiple IP addresses. Defining the IP address is useful when the NVR-AS uses IP based storage, such as an iSCSI SAN.

Status Monitoring Settings dialog

Use this dialog to configure the alerts generated by the hardware diagnostics on the NVR-AS 4000.

Notice *Status monitoring of network interfaces and redundant power is only available on NVR-AS 4000 products. This dialog does not appear on third party Enterprise NVR-AS 4000s.*

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 Monitoring** — When selected, the NVR-AS 4000 generates an alert when the Ethernet ports are not correctly connected to the network.

  On units with more than 2 Ethernet ports, the number of connected network interfaces can be specified. The NVR-AS 4000 only generates alerts when it cannot find the specified number of connected network interfaces.

  On the Enterprise NVR-AS 4000 2U variants with both 10Gbps and 1Gbps network interfaces, all 4 Ethernet ports count towards the number of connected network interfaces.
- **PSU Monitoring (supported devices only)** — When selected, the NVR-AS 4000 generates an alert if it does not have redundant power through its power supplies.

  If the unit has been intentionally installed without redundant power, clear this option to avoid unnecessary alerts. If the unit is not capable of providing redundant power, the PSU Monitoring option does not appear.

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

Disk Space Management dialog

Use this dialog to configure the disk space management settings.

- **Maximum Chunk Size**: This is the largest size that a recording chunk can be before a new chunk is automatically begun. If you are recording at a high bit rate, you may want to set this at a higher value to limit the number of recordings that the NVR-AS and Control Center have to manage.

  Smaller chunk sizes are useful when using the protect on alarm feature to minimize the amount of disk space used. Care should be taken when selecting the chunk size to limit the total number of recordings to be under 100,000 otherwise system performance may be compromised.

Notice *The maximum length of a chunk is four hours of footage.*

- **Video Volume Minimum Free Disk**: This displays the minimum amount of space that should be left free on the NVR-AS. The value is calculated from the maximum number of streams the NVR-AS can record and the maximum chunk size.

Notice *If the value is > 5% of the total disk volume the system displays a warning. If the amount of free disk space does not leave enough space for recordings, reduce the* ***Recording Stream Limit*** *or the* ***Maximum Chunk Size****.*

- **Reaping**
  - **Space**: Recordings are only deleted when the NVR-AS disk is becoming full.
  - **Time and Space**: Recordings are deleted either when the NVR-AS disk is becoming full, or when recordings reach a specified age (max age).

Notice *Do not select the Time and Space option on an NVR-AS which you use to play back archived recordings.*

- **Maximum Chunk Age**: This specifies the length of time that recordings are stored on the NVR-AS before they are automatically deleted.

Notice *Recordings which are marked as* **protected** *are never automatically deleted.*

- **Enable Tamper Protection on recordings**: The NVR-AS 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.

In order to configure Tamper Protection, your Control Center license must include the NVR Tamper Protection feature.

- **Enable video thinning**: Video thinning removes the intermediate P-frames leaving only independent I-frames. This leads to a dramatic reduction in the storage requirements but at the expense of full motion video.

  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. MJPEG and JPEG 2000 streams only contain I-frames, so thinning does not have any effect on footage in these formats.

  Video thinning is not compatible with Tamper Protection. You cannot enable video thinning if Tamper Protection is already enabled.
- **Reduce storage to I-frames only after**: Video thinning is performed on footage once the time entered here has elapsed.
- **Enable automatic unprotect of video**: Select this checkbox to automatically unprotect video older than the age specified in ***Unprotect video after***.

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

- **Unprotect video after**: Video will be unprotected only when it becomes older than the age specified here.

Alarm and Data Record Management dialog

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.

Email Settings dialog

Use this dialog to configure the email alert settings. Select ***Enable email actions*** to configure the NVR-AS to send an email when an alarm occurs.

- **SMTP Server**: This is the IP address of your email server. This may be any SMTP-compliant server, for example UNIX sendmail or Microsoft Exchange Server.
- **Port**: This is the port number on your email server. This is usually 25 or 587.
- **SMTP Username**: This is the username used to log into your SMTP email account (if required).
- **SMTP Password**: This is the password for the email account.
- **Sender email address**: This is the email address that will be used when an email is sent.

The NVR will automatically use secure TLS encryption for email servers that support STARTTLS. This allows emails to be sent using many corporate or internet mail providers.

Finish dialog

You have now completed NVR-AS configuration. You must restart the NVR-AS service for your changes to take effect. Please note that this will temporarily interrupt any active recordings.

- Select ***Yes*** to restart the NVR-AS service now, and click ***Finish***.
- Select ***No*** to restart the service later, and click ***Finish*** to save your settings.
  You must manually restart the NVR-AS service later.

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.