IndigoVision

Enterprise NVR-AS 4000 G3 1U Windows Appliance

User Guide

This manual was created on Tuesday, January 7, 2020.

Document ID: IU-NVR-MAN037-2

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

Save as otherwise agreed with IndigoVision Limited and/or IndigoVision, Inc., this manual is provided without express representation and/or warranty of any kind. To the fullest extent permitted by applicable laws, IndigoVision Limited and IndigoVision, Inc. disclaim all implied representations, warranties, conditions and/or obligations of every kind in respect of this manual. Accordingly, save as otherwise agreed with IndigoVision Limited and/or IndigoVision, Inc., this manual is provided on an “as is”, “with all faults” and “as available” basis. Please contact IndigoVision Limited (either by post or by e-mail at technical.support@indigovision.com) with any suggested corrections and/or improvements to this manual.

Save as otherwise agreed with IndigoVision Limited and/or IndigoVision, Inc., the liability of IndigoVision Limited and IndigoVision, Inc. for any loss (other than death or personal injury) arising as a result of any negligent act or omission by IndigoVision Limited and/or IndigoVision, Inc. in connection with this manual and/or as a result of any use of or reliance on this manual is excluded to the fullest extent permitted by applicable laws.

Contact address

IndigoVision 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 all IndigoVision's Enterprise NVR-AS 4000 G3 1U Windows Appliance. 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 G3 1U 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 G3 1U provides 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 50 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

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 two Ultra 5K Fixed cameras

Hardware

The Enterprise NVR-AS 4000 G3 1U 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.

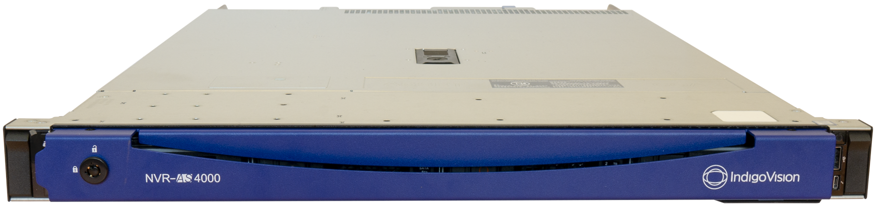


Figure 1: Enterprise NVR-AS 4000 G3 1U

The Enterprise NVR-AS 4000 G3 1U has two 1Gbps Ethernet ports configured as a redundant pair.

Fault monitoring

The Enterprise NVR-AS 4000 1U 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
- Network interfaces

The redundant 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.

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.

iSM

The iSM (iDRAC Service Module) is a small OS-resident process that expands iDRAC management into supported host operating systems. The primary use of the iSM is to make OS information available from iDRAC. This allows iDRAC to give a more complete overview of the system and is used when generating diagnostic reports for hardware related support cases. In addition, iSM provides direct access from the host OS to the iDRAC web UI without requiring the dedicated iDRAC network interface to be connected. By default this access is restricted to read-only.

► For more information, consult www.dell.com for documentation covering the version of iSM 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.*

⚠ **Caution** *Using a UPS with redundant system power supplies is highly recommended. If deployed without a UPS, it is advisable to use the RAID controller section of the BIOS to disable the Disk Cache Policy on each of the Virtual Disks in order to reduce the risk of data loss in the event of power loss. Note that this may reduce the NVR-AS system performance.*

► For more information, *see "Recreating RAID configuration using the BIOS" on page 24*

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.

Notice *While the Enterprise NVR-AS 4000 is preparing Windows for the first time, the screen may go black for several minutes. Do not power-off the device during this time as it may result in an incomplete initialization.*

After Windows configuration is complete and you log in for the first time, the Enterprise NVR-AS 4000 Installation Wizard opens.

Installation wizard

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 12*

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 Control Center trial is started. To continue using Control Center an appropriate license must 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 hierarchy. 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 2:** on page 14 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 2: 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 2:** on page 14 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 2:** on page 14 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 Enterprise NVR-AS 4000 G3 1U has two 1Gbps Ethernet ports configured as a single team. By default this team is configured to use DHCP. To change the network settings, do the following:

1. Open the ***Network and Sharing Center > Adapter Settings***.
2. Right-click ***1 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

The network interfaces on the Enterprise NVR- AS 4000 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 19*
- 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 G3 1U uses RAID5 for all of the storage in the system: operating system, configuration and video footage.

A RAID5 array can tolerate a single disk failure.

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.

- 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.

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 H330*** 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***

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 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.

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).

► 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.

Secure Boot

Secure Boot is a security feature of modern computers which ensures that only authorised and trusted firmware and software can be used to boot a system. It uses digital signatures on all core parts of the firmware and operating system to prevent malware, such as rootkits, from running when the computer boots. No performance penalty is incurred when using Secure Boot.

Secure Boot is an opt-in feature on the Enterprise NVR-AS 4000 G3 1U. It is disabled by default but can be enabled using the following procedure:

1. Ensure the keyboard, mouse and monitor are attached to the Enterprise NVR-AS 4000 G3 1U and reboot the unit.

   Wait for the keyboard shortcuts to be displayed at the top of the screen.
2. When the keyboard shortcuts appear, press ***F2*** to enter System Setup.
3. Select ***System BIOS***.
4. Select ***System Security***.
5. Change the state of ***Secure Boot*** to ***Enabled***.
   - A warning popup will be displayed if a Setup password has not been configured.

Notice *IndigoVision recommends that you create a Setup password to secure the Enterprise NVR-AS 4000 G3 1U against unauthorised access.*

6. Click ***Back***.
7. Click ***Finish***.
   - A warning popup will be displayed asking if changed settings should be saved. Click ***Yes***.
   - Another popup will be displayed when the settings have been saved successfully. Click ***OK***.
8. Click ***Finish***.
   - A warning popup will be displayed asking if you want to exit and reboot. Click ***OK***.
9. The unit will reboot with Secure Boot enabled.

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 17*
- ► For more information about RAID configuration, *see "RAID configuration" on page 24*

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 UEFI 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.

    Wait for the keyboard shortcuts to be displayed at the top of the screen.

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 G3 1U is as follows:

- The four front panel disks are configured as a single RAID 5 array which is then split into two Virtual Disks.
- The first Virtual Disk contains the operating system and NVR-AS configuration, and must be 64GB in size.
- The second Virtual Disk is reserved for video footage.

The following options should be used for both Virtual Disks:

- No Read Ahead
- Write Through caching
- 64KB Stripe Element Size
- Disk cache enabled

⚠ **Caution** *Using a UPS with redundant system power supplies is highly recommended. If deployed without a UPS, it is advisable to use the RAID controller section of the BIOS to disable the Disk Cache Policy on each of the Virtual Disks in order to reduce the risk of data loss in the event of power loss. Note that this may reduce the NVR-AS system performance.*

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 23*

To reconfigure the RAID array in the BIOS, do the following:

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.
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 26*

Delete any existing broken virtual disks as necessary by following this procedure:

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

Notice *If recreating the Virtual Disks for both OS and Storage, you must recreate the OS Virtual Disk first.*

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 24
4. From the following options, choose where space for the Virtual Disk should be allocated:
   - Create a new RAID array for the Virtual Disk to use (step 5).
   - Allocate the Virtual Disk from unused space on an existing RAID array (step 6).
5. If creating a new RAID array, do the following:
   a. Select ***Unconfigured Space***.
   b. Select ***Select Physical Disks***.
   c. If necessary, change ***Select Media Type*** to `Both`.
   d. If necessary, change ***Select Interface Type*** to `Both`.
   e. Select the check boxes next to all of the disks where Virtual Disks should be created.
   f. Ensure you select the expected number of disks.
   g. Select ***Apply Changes***.
6. If using unallocated space from an existing RAID array, do the following:
   a. Select ***Free Capacity***.
   b. Select ***Select Disk Groups***.
   c. Select the check box beside all of the disks on which Virtual Disks should be created.
   d. Select ***Apply Changes***.
7. Set the size of the Virtual Disk.
   - If recreating the OS Virtual Disk, change the size to exactly 64GB.
   - If recreating the Storage Virtual Disk, leave it as the default to use all remaining space.
8. Select the settings for the new Virtual Disk as previously specified.

   ► For more information, *see "RAID configuration" on page 24*
9. Set the ***Default Initialization*** option to ***Fast***.
10. Click ***Create Virtual Disk***.
11. 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

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
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 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 from the Start screen:

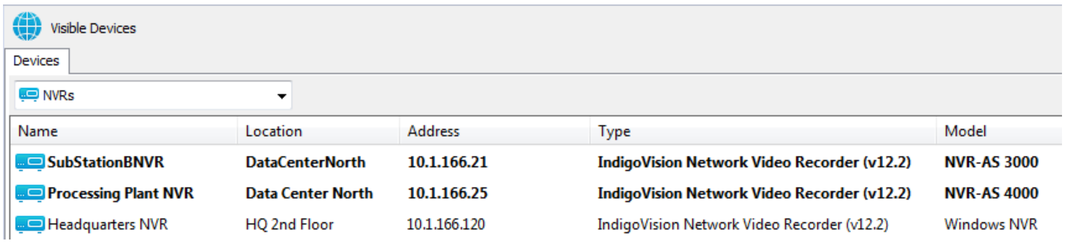
Start > IndigoVision > NVR-AS Administrator

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.



Name	Location	Address	Type	Model
SubStationBNVR	**DataCenterNorth**	**10.1.166.21**	**IndigoVision Network Video Recorder (v12.2)**	**NVR-AS 3000**
Processing Plant NVR	**Data Center North**	**10.1.166.25**	**IndigoVision Network Video Recorder (v12.2)**	**NVR-AS 4000**
Headquarters NVR	HQ 2nd Floor	10.1.166.120	IndigoVision Network Video Recorder (v12.2)	Windows NVR

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 Enterprise NVR-AS 4000.

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

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 Enterprise NVR-AS 4000 generates an alert when the Ethernet ports are not correctly connected to the network.

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.