

IndigoVision

**Large Enterprise Network
Video Recorder
(NVR-AS) 4000 G3**

User Guide



IndigoVision

THIS MANUAL WAS CREATED ON WEDNESDAY, MAY 29, 2019.

DOCUMENT ID: IU-NVR-MAN032-1

Legal Considerations

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

Copyright

COPYRIGHT © INDIGOVISION LIMITED. ALL RIGHTS RESERVED.

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

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

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

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

Contact address



IndigoVision 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

	Legal Considerations	2
	Copyright	2
	Contact address	2
	Dell Software License Agreement	2
	NVR-AS License Terms	2
1	About This Guide	5
	Safety notices	5
2	Overview	7
	Hardware	7
	NVR-AS 4000 G3 Storage Array Server (SAS)	8
	NVR-AS 4000 G3 Storage Array	8
	NVR-AS 4000 G3 Storage Array Expansion	8
	Configuration	8
	Fault monitoring	9
3	Getting Started	11
	Overview	11
	Install the rack mounted equipment	11
	Additional guidelines	12
	Configure the Storage Array Server	12
	Power up the Storage Array Server	12
	Complete the operating system setup	12
	Configure the Storage Array Server	13
	Connect the NVR-AS 4000 G3 Storage Array Server to other equipment	17
	Configure the video storage	18
	Configure Storage Array System Settings	18
	Set up storage	19
	Map host	20
	Initialize the disks	21
	Enable Storage Array Fault Monitoring on the Storage Array Server	22
	Configure NVR-AS instances on the Storage Array Server	22
	Configure the NVR-AS Instance using the NVR-AS Administrator	23
	Install the NVR-AS instance	23
	Create the remaining instances	23
4	Operations	25
	Identifying and replacing a faulty disk in a storage array enclosure	25
	Identifying and replacing other faulty hardware in a storage array enclosure	26
	Operating System Disk management	26
	Operating System RAID redundancy	26

	Replacing a faulty disk	26
	Adding storage capacity to an existing system	27
	Connect the additional Storage Array Expansion unit	27
	Setup storage	27
	Expand Volumes	28
	Extend Filesystem Partitions	28
	Add further Expansions	28
	Upgrading NVR-AS software	28
	Install a new license or update an existing license	29
	Create and send a fingerprint file	29
	Apply a license file	29
	OMSA X.509 Certificate Management	30
	SSL Server Certificates	31
5	Maintenance	33
	Recover system using USB Restore Media	33
	Operating system installation wizard process	34
6	Software Description	35
	Identification dialog	35
	License Server Details dialog	35
	Storage Locations dialog	35
	Network Settings dialog	36
	Status Monitoring Settings dialog	36
	Disk Space Management dialog	37
	Alarm and Data Record Management dialog	38
	Email Settings dialog	39
	Finish dialog	39
A	Troubleshooting	41
	Monitor recordings	41
	NVR Alerts	41
	Recording failure alerts	41
B	Physical configuration	43
	750TB variant	43
	1.5PB variant	44
	2.25PB variant	45
	3.0PB variant	46

1 ABOUT THIS GUIDE

This guide is written for users of the IndigoVision Large Enterprise NVR-AS 4000 G3 System. It provides installation and configuration information for the system variants, as well as a description of the hardware and specifications.

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

Safety notices

This guide uses the following formats for safety notices:



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



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

Notice

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



Additional information relating to the current section.

2 OVERVIEW

IndigoVision's Large Enterprise NVR-AS 4000 G3 System is part of IndigoVision's Control Center.

The system provides powerful and integrated recording and playback of video and audio from IP cameras and encoders. The system is designed to suit the requirements of larger centralized installations.

The Large Enterprise NVR-AS 4000 G3 System 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 4Gbps with simultaneous playback.
- Third party camera support.
- ADAPT/RAID storage resilience, redundant RAID controllers, redundant power supplies, and redundant network connections.
- Powerful and distributed alarm management.
- Digital Signatures and Tamper Protection of recordings.



ADAPT is a RAID-based data protection technology that provides a number of advantages compared to standard RAID. There is no need for idle hot spare drives, in an ADAPT configuration there is built-in spare capacity and all drives contribute to performance. Rebuilds are fast and performance degradation when drives fail is less.

Hardware

The Large Enterprise NVR-AS 4000 G3 System is available as the following variants:

- 750TB - 800 streams - 4000Mbps
- 1.5PB - 800 streams - 4000Mbps
- 2.25PB - 800 streams - 4000Mbps
- 3.0PB - 800 streams - 4000Mbps

These variants are made up from one or more of the following components:

- NVR-AS 4000 G3 Storage Array Server
- NVR-AS 4000 G3 Storage Array
- NVR-AS 4000 G3 Storage Array Expansion

The following figure illustrates the key components of each variant:

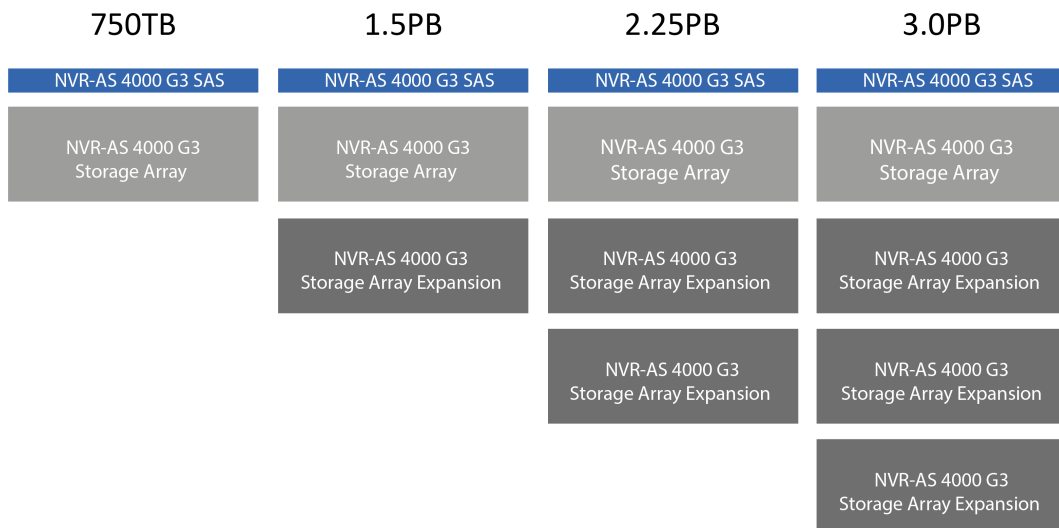


Figure 1: Large Enterprise NVR-AS 4000 G3 System variant components

NVR-AS 4000 G3 Storage Array Server (SAS)

The NVR-AS 4000 G3 Storage Array server has the following features:

- Video optimized Windows Server 2016 with pre-installed NVR-AS application software
- Dual port 10GbE SFP+ network adapter
- 12Gbps SAS Host Bus Adapter
- 32GB RAM
- 2U

NVR-AS 4000 G3 Storage Array

- Dual redundant RAID controllers
- 84 x 12TB Nearline SAS disks
- 5U

NVR-AS 4000 G3 Storage Array Expansion

- Needs an NVR-AS 4000 G3 Storage Array for ADAPT/RAID Support
- 84 x 12TB Nearline SAS disks
- 5U

Configuration

To ensure reliability and performance of each variant the storage capacity is divided into a number of separate logical NVR-AS instances. Each NVR-AS instance has the following features:

- A Windows service that has its own configuration directory.
- An instance name and registry entries for further configuration.
- A single Virtual Disk assigned to it for video storage and used solely by this instance.
- Is visible in the Control Center suite as an independent NVR.

Fault monitoring

The Large Enterprise NVR-AS 4000 G3 System 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
- Network interfaces
- Enclosure sub-components (controllers, drawers, side-planes and expanders)
- Enclosure temperature

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 Large Enterprise NVR-AS 4000 G3 System device.

Overview

Setting up a Large Enterprise NVR-AS 4000 G3 System involves the following steps:

1. Install the rack mounted equipment into suitable cabinets.
2. Configure the Storage Array Server.
3. Connect the Storage Array Server to the NVR-AS 4000 G3 Storage Array(s).
4. Configure the video storage.
5. Configure NVR-AS instances on the Storage Array Server.

Install the rack mounted equipment



Proper care must be taken that the floor support and cabinets are designed for the amount of equipment to be installed.

The Large Enterprise NVR-AS 4000 G3 System weighs between 168kg and 428kg (370lb and 943lb) depending on the variant being installed.



Proper care must be taken when lifting the equipment and installing it in cabinets.



Proper care must be taken to ensure that all safety guidelines are followed and all necessary fixtures are used during installation.



The storage array enclosures require 200-240V AC power circuits. The design of the server room needs to take this into account. Both power supply units for each storage array enclosure must be connected to a power supply using IEC 60320 C19 to C20 cables.

Take care to plan out the location of each of the components of the Large Enterprise NVR-AS 4000 G3 System for cabling and ease of maintenance.

Additional guidelines

- It should be possible to cable redundant 200-240V AC power connections for each storage array enclosure to separate power circuits.
- It should be possible to cable redundant AC power connections for the Storage Array Servers to separate power circuits.
- Care should be taken to observe maximum cable reach.
- The individual components for the Large Enterprise NVR-AS 4000 G3 System should be located close to one another, all in the same cabinet.
- Careful layout and labeling is advised to keep each Large Enterprise NVR-AS 4000 G3 System clearly separated.

The physical layout and connections of each system are shown in the appendix.

► For more information, see *"Physical configuration" on page 43*

Configure the Storage Array Server

After the equipment has been installed into the cabinets, the next step is to configure the Storage Array Server.

The Storage Array Server needs to go through an initial configuration process.

Power up the Storage Array Server

The Storage Array Server needs to be connected to a suitable power supply.

1. Connect a monitor, mouse, and keyboard to the Storage Array Server.
2. Ensure the SAS cables are NOT connected to the Storage Array Server.



If the SAS cables are connected to the Storage Array Server, the operating system configuration will fail. If this happens you will need to use the Recovery Media.

► For more information, see *"Recover system using USB Restore Media" on page 33*

3. Connect the redundant power supplies on the Storage Array Server to an AC power supply.
4. Power up the Storage Array Server.
5. Allow the operating system setup to proceed.

Complete the operating system setup

When you power up the NVR-AS 4000 G3 Storage Array Server for the first time, Windows performs an 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.

Notice *While the NVR-AS 4000 G3 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 G3 Installation Wizard opens.

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 G3 Storage Array Server 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 14

You can now configure the rest of the Enterprise NVR-AS 4000 G3 settings. By default, the network interfaces are configured to use DHCP.

Configure the Storage Array Server

After the Storage Array Server has been installed it can be configured.

1. Allocate a number of static IP addresses on the 10GbE network team.
There should be one IP address per NVR-AS instance on the Storage Array Server.
For all Large Enterprise NVR-AS 4000 G3 variants, it is recommended that 4 NVR-AS instances are created.
2. Change the network settings:
 - a. Open the **Network and Sharing Center > Change Adapter Settings**.
 - b. Right-click the adapter identified as 10Gbps Team and select **Properties**.
 - c. Select **Internet Protocol Version 4 (TCP/IPv4) > Properties**.
 - d. Select **Use the following IP address** to enable manual IP address assignment.
 - e. Open **Advanced** settings.
 - f. Add the IP addresses (and the corresponding subnet masks) allocated in step 1.
 - g. Click **OK**. The **Advanced TCP/IP Settings** dialog closes.
 - h. If required, provide the preferred and alternate DNS server addresses.
 - i. Click **OK**. The **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog closes.
 - j. Click **Close**. The 10Gbps Team properties are saved.

Leave the Network Connections interface open for the next step.

3. Configure the 1Gbps NIC for the storage array management network.
4. Configure the date and time on the Storage Array Server.
 - ▶ For more information, see *"Date and time settings"* on page 15
5. If required, configure the Remote Desktop settings.
 - ▶ For more information, see *"Remote desktop configuration"* on page 17
6. Ensure the NVR-AS and (if required) License Server applications are at their latest versions – version numbers can be verified from **Programs and Features**. Latest software is available through the Partner Portal.

IndigoVision License Server configuration


To complete the NVR-AS setup and allow it to record, you must configure the NVR-AS 4000 G3 Storage Array Server 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 Large Enterprise NVR-AS 4000 G3 Installation Wizard offers the ability to configure this NVR-AS 4000 G3 Storage Array Server 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 NVR-AS 4000 G3 Storage Array Server to act as a License Server, make sure that there are no other License Servers active in your site.*

Notice *If the Network Video Recorder (NVR-AS) 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 Network Video Recorder (NVR-AS) as a License Server.*

 *If the NVR-AS 4000 G3 is required to act as a License Server but no license server software has been installed, the License Server installer can be obtained from the Partner Portal and installed manually.*



Configuring the NVR-AS 4000 G3 Storage Array Server device to act as a License Server will start the time limited trial license.

Date and time settings



All devices in the IndigoVision system, including the Large Enterprise NVR-AS 4000 G3 System, 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 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 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 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 Large Enterprise NVR-AS 4000 G3 System 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 G3 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 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 teaming

The network interfaces should be 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 Network Video Recorder (NVR-AS) will also need to be reconfigured to use LACP.

1. Open **Server Manager**.
The **Local Server** tab contains a panel containing general server properties, including **NIC Teaming**.
2. Click on the associated link and verify that the teaming settings are as expected.

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 NVR-AS 4000 G3 Storage Array Server 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.

Connect the NVR-AS 4000 G3 Storage Array Server to other equipment

After the NVR-AS 4000 G3 Storage Array Server has been initialized, they need to be connected to the Large Enterprise NVR-AS 4000 G3 System components.

- ▶ For more information, see *"Physical configuration" on page 43*
 1. Connect SAS cables between the Storage Array Server and the primary storage array enclosure.
 2. Connect the storage array expansion.
 - a. If you are connecting one storage array expansion, connect SAS cables between the primary storage array enclosure and the first storage array expansion.
 - Ensure that each RAID controller on the primary enclosure is connected to the corresponding management module on the expansion enclosure.
 - Ensure that the SAS connections going into each management module are connected to SAS port 1 and not SAS port 2.
 - b. If you are connecting two or more storage array expansions, connect SAS cables between the primary storage array enclosure and the first storage array expansion, then between each storage array expansion and its subsequent storage array expansion.
 - Ensure that the SAS connections going into each management module are connected to SAS port 1 and not SAS port 2.
 - Do not create symmetrical connections from the two management controllers as this reduces fault-tolerance. Instead, stagger the connections.
- ▶ For more information, see *"Physical configuration" on page 43*
 3. Connect the network cables.
 - a. Connect one 10GbE network port on each NVR-AS 4000 G3 Storage Array Server to each of the video network switches.
 - b. Connect the GbE network ports on each NVR-AS 4000 G3 Storage Array Server to the management network switches.

- c. Connect the GbE network ports on each primary enclosure RAID controller to the management network switches.
4. Power on all core network switches and array management switches.
Ensure that all disks are correctly installed.
5. Connect a 200-240V AC supply to both power supply units on each storage array enclosure.
6. Switch on both power supply units on each storage array enclosure.

All of the components of the Large Enterprise NVR-AS 4000 G3 System should now be powered on and connected with the required 10GbE, GbE, or SAS cables.



Both redundant PSU connections must be used otherwise the storage array will not function correctly.

Configure the video storage

Configure the video storage using the following steps:

1. Configure Storage Array System Settings.
2. Set up storage.
3. Map host.
4. Initialize the disks.

Configure Storage Array System Settings

The first step in configuring the NVR-AS 4000 G3 Storage Array is to configure its general system settings. Until all mandatory system settings have been modified, the **Welcome** page will block access to storage configuration.

1. Connect a PC directly to Controller A's management port and set the PC's network interface to be on a 10.0.0.* network. Ensure that TLS 1.2 is enabled in the PC's Internet settings.

Notice

Your browser may display a warning indicating a certificate error when you try to browse to either network controller. This error is shown because the storage array management interface has temporary HTTPS certificates.

Typically most browsers let you continue to the web interface despite showing this error.

You can suppress the warning by adding the network controller IP address to the PC's list of trusted sites and setting the browser's local-intranet security option to medium or medium-low.

2. In a web browser, navigate to `https://10.0.0.2` and enter the admin login details in the login page:
 - user: manage
 - password: !manageA welcome panel opens to guide you through the initial setup steps.
3. From the **Welcome** panel, select **System Settings > Manage Users**.
4. Modify the password for each of the users with red asterisks against them.
5. Select the **Network** tab.

6. Set the IP address details on each controller to values suitable for your network.
7. On submission of the results, connectivity to the storage array will be lost.
The browser will be redirected to the new address specified for Controller A, but will fail if the new address is on a different subnet to the PC.
8. Reconfigure the PC to be on the same network as the storage array and reconnect the browser to its web interface.



When logging back into the web interface, the new `manage` user password supplied at step 4 will now be in effect.

9. When you log back into the web interface, the welcome page is displayed.
Select **System Settings > Notifications**.
10. If you require direct notifications to be sent from the storage array, configure as appropriate.



The NVR-AS 4000 G3 fault monitoring functionality is configured independently and will feed selected notifications into Control Center regardless of the configuration options chosen here. This tab represents mandatory config – to make storage configuration available, you must either configure notification details, or explicitly disable notifications.

11. Click on the **Date and Time** tab.
 - a. Make sure the **Network Time Protocol (NTP)** checkbox is selected
 - b. Enter the IP address of the master NTP server and required time-zone offset
 - c. Click **Apply and Close**



The IP address provided for the Master NTP server should match the one set on the NVR-AS 4000 Storage Array Server - see "Date and time settings" on page 15

12. Click the **SupportAssist** tab.
You have two options:
 - **I acknowledge that I do not want to set up SupportAssist at this point in time.** - Select this option if you do not want any information sent to Dell and you want to disable the SupportAssist feature.
 - **SupportAssist** - Select this option to enable SupportAssist feature. After selecting this feature you need to provide accurate contact information. This information is provided to Dell when your system encounters an error or system failure.
13. After all configuration tasks have been completed, click **Close** in the main **System Settings** pane to return to the welcome page.

Set up storage

In a web browser, navigate to Controller A's web interface and enter the admin login details. A welcome panel opens to guide you through the initial setup steps.

1. Click **Storage Setup**.
A **Storage Setup** wizard opens and prompts for the type of storage to use.
2. Select **Virtual**.

The storage setup wizard scans all available disks and suggests an optimal storage configuration. Configuration should consist of 2 pools of 42 disks each.

3. Click **Create Pools**.

Map host

Set up Multi-path IO on the NVR-AS 4000 G3 Storage Array Server.

1. Open **Server Manager**.
2. Choose **Add Roles and Features**, then click **Next** until the **Features** page is displayed.
3. Verify that Multi-path IO is installed. If not, do the following:
 - a. Check the feature
 - b. Click **Next > Install > Close**
 - c. Reboot the system
4. Open **Server Manager** again and select **Tools > MPIO**.
5. Click on the **Discover Multi-paths** tab.
6. Select the **Add support for SAS devices** checkbox then click **Add**.
A dialog opens prompting to restart the server.
7. To restart the server, click **Yes**.

In a web browser, navigate to Controller A's web interface and enter the `manage` login details. A welcome panel opens to guide you through the initial setup steps.

1. Select **Host Setup**.
A host setup wizard opens, showing a list of pre-requisites for host setup.
2. Click **Next**.
Wizard displays a list of all detected initiators
3. Select both initiators for the NVR-AS-4000 G3 Storage Array Server



IDs can be verified as correct by running

Get-InitiatorPort

in a PowerShell console on the NVR-AS 4000 G3 Storage Array Server.

4. Enter a meaningful host name in the **Host Name** text box.
This is only a label – it does not need to be an actual network hostname.
5. Assign meaningful nicknames to each initiator. Click **Next**.
Wizard opens a page allowing clustering of hosts.
6. If the NVR-AS 4000 G3 Storage Array Server is intended to operate as a stand-alone host, select **Do not group this host**. Click **Next**.
Wizard opens a page allowing volumes to be created. Initially, it shows a default configuration with two 100GB volumes, one in pool A and one in pool B.
7. Click in each **Volume Size** text box and modify the volume size to half of the maximum permitted.
Unallocated space is displayed at the top of the table and it is generally ~127.8TB.
When updating the value, you must modify the units as well as the numeric value.
8. Click the **Add Row** button to create a second volume in pool A.
9. Click in the **Volume Size** textbox to set the size to the remaining unallocated space in pool A. Ensure the **Pool** drop-down is set to **A**.
10. Repeat the two previous steps to create a second volume in pool B. Click **Next**.

- Wizard opens a page showing a summary of the configuration.
11. Check values are all as expected and click **Configure Host**
A dialog opens stating that configuration is in progress.
 12. Once configuration is complete, it shows a success message and allows you to configure another host. Click **No**.
The web UI shows all three sections as completed.
 13. Click **Go To Home Page**.
 14. The web UI now shows the standard homepage rather than the welcome page. The three menu options previously selected from the **Welcome** page are now available from **Home** tab of the homepage, under the **Actions** button.

Initialize the disks

1. On the NVR-AS 4000 G3 Storage Array Server, open **Disk Management (Control Panel > System and Security > Administrative Tools > Create and Format Disk Partitions)**.
2. On startup, **Disk Management** shows an **Initialize Disk** dialog including a table with four uninitialized disks.
Ensure **GPT** partition style is selected and click **OK**.

Notice *Depending on the state of the newly-created disks, Disk Management may not show the Initialize Disk dialog on startup. If the dialog does not appear:*

a. Select **Rescan Disks** from the **Action** menu.

This causes the new disks to be displayed in the list of disks in the bottom panel.

b. Right-click any that are offline and select **Online**.

c. When all disks are online, right-click one of them and select **Initialize** to open the **Initialize Disk** dialog.

3. The dialog closes to show the **Disk Management** screen, with the four disks shown as online, but unallocated.
4. Right-click in the unallocated space of the first disk and select **New Simple Volume...**
A **New Simple Volume Wizard** opens.
5. Click **Next**.
6. A page opens allowing to specify the volume size. Set size to the maximum available.
7. A page opens allowing to specify a drive letter/mount point. Note the drive letter for use in subsequent configuration. Click **Next**.
8. A page opens allowing to format the volume. Set file system to **NTFS** and allocation unit size to **64K**. Enter a meaningful label to the volume (for example, `instance 1`) and click **Next**.

Notice *Specifying anything other than 64KB for allocation units will prevent the NVR-AS instances from being configured and will require a rescan and reformatting of the volumes.*

9. A page opens showing a summary of the selected options. Check if the options are correct and click **Finish**.
10. Repeat steps 4-9 for the other three disks.

Enable Storage Array Fault Monitoring on the Storage Array Server

In order for the NVR-AS 4000 G3 Storage Array Server to detect and report faults on behalf of the NVR-AS 4000 G3 Storage Array, a Fault Monitoring Client is required.

The Fault Monitoring Client installer is included on the IndigoVision Partner Portal. You must install it to complete the NVR-AS 4000 G3 Storage Array Server configuration and configure to point to an ME Storage Manager (MESM) interface on the NVR-AS 4000 G3 Storage Array.

To install and configure the Fault Monitoring Client:

1. Download the installer from the IndigoVision Partner Portal.
2. Double-click the installer.
The installation wizard opens.
3. Accept the End-User License Agreement.
4. Select the default location for the client.
5. Click **Install**.
6. If the wizard pops up a second installer asking you to install .NET Framework 4.7.2, accept the EULA for this and proceed with the installation (this will require a restart).
7. If the device was restarted, select Fault Monitoring Admin tool from the start menu to configure the Fault Monitoring client
If no restart was required during installation, the Admin tool will start automatically on completion of the install.
8. Enter the IP address of at least one of the controllers on the storage array.

Notice *While you can configure the Fault Monitoring Client to query only one controller, it is strongly recommended to configure connections to both controllers, in order to provide redundancy between the management interfaces.*

9. Enter the password for the `monitor` account on the storage array (`monitor` user name should already be populated). Click **Next**.
10. The tool will display a page allowing root certificate automatic updates to be disabled. This is necessary when running on isolated networks, as HTTPS connections may fail if automatic updates are enabled. Click **Next**.
11. The tool will test each configured connection – if any fail, it will report an error in the configuration but allow configuration to proceed.
12. Finish admin tool.

Configure NVR-AS instances on the Storage Array Server

After the video storage has been configured for each NVR-AS 4000 G3 Storage Array Server, it is now ready for NVR-AS instances to be created and configured.

The Storage Array Server must be set up to have multiple NVR-AS instances – this is necessary because each individual NVR service has a hard limit of 200 streams. To achieve the stream count limit supported by the platform, 4 instances should be created. Each instance requires its own storage partition to record to, corresponding to the 4 volumes created in the previous section.

Follow these steps to configure each instance on each Storage Array Server:

1. Configure the NVR-AS instance using the NVR-AS Administrator.
2. Install the NVR-AS instance and create a Windows Service for the instance.

Configure the NVR-AS Instance using the NVR-AS Administrator

A shortcut to the NVR-AS Administrator must be created for each NVR-AS instance in the system.

1. Create a shortcut to the NVR-AS Administrator on the desktop for the instance that is being configured.
 - a. Navigate to **C:\Program Files (x86)\IndigoVision\NVR-AS**
 - b. Right click **NvrAdmin.exe** and select **Send to > Desktop (create shortcut)**
 - c. Amend the shortcut **Target** to:


```
"C:\Program Files (x86)\IndigoVision\NVR-AS\NvrAdmin.exe"
nostart norestart instance=instancename
```

Replace `instancename` with the correct name of the instance, for example `instance1`.
2. Rename the shortcut to include the name of the instance that it configures.
3. Double-click the shortcut.

The NVR Administrator starts and permits configuration of the instance.
4. Enter the required settings for the instance into the NVR-AS Administrator.

On completion, the NVR-AS Administrator does not ask if you wish to restart the service.

Install the NVR-AS instance

Before the NVR-AS instance can be used it must be installed as a Windows Service.

1. Open a command prompt.
2. Enter the following command to navigate to the NVR-AS folder.


```
CD "C:\Program Files (x86)\IndigoVision\NVR-AS"
```
3. Enter the following command to start the installation.


```
NvrServer --install instance1
```

This installs an instance with the instance name `instance1`.
4. Select **Start > Administrative Tools > Services** and locate the new service.

The name of the service is of the form: **IndigoVision NVR-AS instancename**.
5. Right-click the service and select **Start**.

If an NVR-AS instance fails to start:

- Check the Application log in the Windows Event Viewer for detailed error information.
- Check that the Configuration and Video Library directories have valid paths and that the target directories exist. The directories should be empty and no two instances should be sharing the same Config directory.
- Check that the IP address configured for the instance is valid for the machine and that it is not in use by another NVR-AS instance. The IP addresses were created during initial setup of the Storage Array Server and can be verified by clicking the relevant NVR-Admin shortcut setup previously.

Create the remaining instances

Repeat the previous tasks for the remaining instances for the Storage Array Server.

After the NVR-AS service for each instance is running, the NVR-AS instance can be incorporated into the Control Center suite.

4 OPERATIONS

This chapter describes common tasks required for the operation of the Large Enterprise NVR-AS 4000 G3 System device.

Identifying and replacing a faulty disk in a storage array enclosure

ADAPT immediately rebalances data in the event of a disk failure. It has sufficient redundancy to cope with up to two faulty disks per pool at any given time.



After the ADAPT array has completed the rebalancing operation, it is then tolerant of at least one further disk failure per pool.

Failed disks should be identified and replaced at the earliest opportunity to maintain system redundancy. Use the web UI hosted by either storage array controller to identify a failed disk.

To remove a faulty disk:

1. Remove the bezel from the correct storage array enclosure.
2. Slide out the drawer containing the failed disk.

Notice *The enclosure fans run at full speed until the drawer is replaced.*

3. Replace the disk.
4. Slide the drawer shut and replace the bezel.
5. Check the faulty disk in the storage array web UI System tab to confirm that it is detected by the system and reconstruction of the disk has started.

If the disk does not automatically start reconstruction, it may already contain metadata. If necessary, follow these steps to clear metadata:

1. On the **System** tab, click **Action**, then select **Clear Metadata**.
This option is only available if at least one disk has this problem. After selecting it, a list of applicable disks is displayed.
2. Highlight the disks you require cleared, then click **Ok**.
A confirmation dialog opens.
3. Click **Ok** to perform the operation.

Identifying and replacing other faulty hardware in a storage array enclosure

Failed components should be identified and replaced at the earliest opportunity in order to maintain system redundancy.

Use the web UI hosted by either storage array controller to identify the failed component and its location.

Operating System Disk management

NVR-AS 4000 G3 Storage Array Server operating system disk management uses the Dell™ OpenManage™ Server Administrator (OMSA). The OMSA can be started from the desktop shortcut or from the Start menu. 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. Click **Continue to this website** to open the OMSA.
- Internet Explorer then opens a **Windows Security** dialog requesting credentials. Click **Cancel** to close the dialog.
- If the OMSA requests credentials, enter the user name `Administrator` and the administrator password currently set for the operating system.

Alternatively, you can configure Internet Explorer to avoid the requests for credentials:

1. Select **Tools > Internet Options** in Internet Explorer. The **Internet Options** dialog opens.
2. Click **Local internet** from the **Security** tab.
3. Click **Sites**.
4. Clear the check box **Automatically detect intranet network**.
5. Select the check box **Include all local (internet) sites not listed in other zones**.
6. Click **OK**. The **Local internet** dialog closes.
7. Click **OK**. The **Internet Options** dialog closes.

The next time you start OMSA from the desktop shortcut or the Start screen, click **Continue** to access OMSA, without having to enter the credential checks.

Operating System RAID redundancy

The NVR-AS 4000 G3 Storage Array Server uses two disks in a RAID1 mirror for operating system and configuration information.

The RAID1 mirror can tolerate a single disk failure.

If a disk fails, it must receive attention at the earliest opportunity to maintain maximum array redundancy. The disks can be found in the two hot-swappable bays at the rear of the Storage Array Server.

Replacing a faulty disk



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.

- 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.

Adding storage capacity to an existing system

Existing Large Enterprise NVR-AS 4000 G3 systems can be expanded by adding Storage Array Expansion units using the following steps:

1. Connect the additional Storage Array Expansion unit.
2. Setup storage.
3. Expand Volumes.
4. Extend Filesystem Partitions.
5. Add further Expansions.

Connect the additional Storage Array Expansion unit

To start connecting the additional Storage Array Expansion unit, connect correctly the SAS controllers across the devices using the provided cabling. Once the expansion unit is correctly connected, the NVR-AS 4000 G3 Storage Array should automatically detect it and make it instantly available for use.

► For more information, see *"Physical configuration"* on page 43

Setup storage

To set up the newly attached Storage Array Expansion unit, it is necessary to log in to the management interface. The unit will be automatically detected and installed in the existing system.

1. In a web browser, navigate to the `https://<IP address of the Storage Array management interface>` and enter the admin login details in the login page. Home page loads.
2. From the side panel, select **Pools**.
3. On the **Pools** page select **Actions > Add Disk Group**.
4. In the **Add Disk Group** wizard leave the **Name** unchanged and modify the following:
 - a. Click on **Type** drop box and select **Virtual**.

- b. Click on **Pool** drop box and select **A**.
 - c. Click on **Data Protection** drop box and select **ADAPT**.
5. From the disk table, select 42 disks and click **Add**.



You can either select the disks by entering the range of disks or you can select the disks with the cursor while holding the Shift button pressed.

6. Wait for the Disk Group creation process to finish. Once the operation has completed successfully, select **OK**.
7. Repeat steps 3-6. In step 4, modify the **Pool** drop box value and select **B**.

Expand Volumes

After expanding the pools, it is required to expand the existing virtual volumes.

1. From the side panel select **Volumes**.
2. On the **Volumes** page, select the volume you want to expand, then select **Actions > Modify Volume**.
3. **Modify Volume** wizard page opens. Click on **Expand By** text box and modify the volume size to match the half of the single disk group capacity. Click **OK**.



You can expand any amount of volumes to the desired value as long as you do not oversubscribe it.

4. Wait for the volume creation process to finish. Once the wizard operation completed successfully, select **OK**.

Extend Filesystem Partitions

To extend the instances of the NVR, go to the NVR-AS 4000 G3 Storage Array Server.

1. Open **Disk Management**.
2. Locate the disks with unallocated space.
3. Select the partition on this disk, right click on it and select **Extend Volume**.
4. In the **Extend Volume** wizard, expand the volume to use all available space. To do it, select **Next > Next > Finish**.
5. Repeat steps 2-4 for all expanded disks.

Add further Expansions

In case you would like to add additional Storage Array Expansion units, repeat the steps from sections one to four. The maximum number of Storage Array Expansion units in a single system is three.

Upgrading NVR-AS software

When upgrading NVR-AS software on a Large Enterprise system, all Storage Array Servers need to be upgraded.

As the Storage Array Servers are running multiple instances of the NVR-AS service, upgrading to a newer version requires additional steps from upgrading a single instance.

1. Stop all running NVR-AS instances using the Windows Services Control Panel.
2. Upgrade the NVR-AS software.
 - ▶ For more information, refer to the IndigoVision Applications Installation Guide.
3. Stop the upgraded primary IndigoVision NVR-AS service if it is running and set it to Manual start.
4. Restart all of the previously stopped instances.

Install a new license or update an existing license

You can configure the NVR-AS 4000 G3 Storage Array Server to act as a License Server for IndigoVision products.

Notice *Each IndigoVision site should only have a single License Server. If you configure the NVR-AS 4000 G3 Storage Array Server to act as a License Server, make sure that there are no other License Servers active in your site.*

The NVR-AS 4000 G3 Storage Array Server 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 NVR-AS 4000 G3 Storage Array Server to act as a License Server.

Use the following steps to upgrade to a full license:

1. Create a fingerprint file and send it to IndigoVision with your IndigoVision order acknowledgment number.
2. Apply the license file from IndigoVision to the NVR-AS 4000 G3 Storage Array Server.

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 Certification 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 PKCS#12 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 Large Enterprise NVR-AS 4000 G3 System.

Recover system using USB Restore Media

If the Large Enterprise NVR-AS 4000 G3 System becomes inoperable the USB Restore Media can be used to restore the unit to its original system software.

In this case the alarm and configuration data will be lost, but the video footage will still be available on the storage array. After system recovery, follow the normal Storage Array Server configuration procedure.

However, you do not need to recreate and reformat the Disk Groups and Virtual Disks for the recovered Storage Array Server.



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 26
- ▶ For more information about RAID configuration for an NVR-AS 4000 G3 Storage Array Server, see *"Operating system installation wizard process"* on page 34

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.
3. Remove both SAS cables from the rear of the Storage Array Server.



Ensure you use the USB Restore Media supplied with the specific Large Enterprise NVR-AS 4000 G3 System you are recovering.

4. Insert the USB Restore Media.
5. Power on the Large Enterprise NVR-AS 4000 G3 System.
Wait for the keyboard shortcuts to be displayed at the top of the screen.
6. Press **F2**.
Wait for the system setup screen to appear.

7. Select **System BIOS > Boot Settings**.
8. Change **Boot Mode** from UEFI to BIOS.
9. Save the changes and exit the system setup.
The server reboots.
10. When the keyboard shortcuts appear, press **F11**.
11. Select **One-shot BIOS Boot Menu**.
12. Select the entry corresponding to the USB Restore Media.
The Large Enterprise NVR-AS 4000 G3 System boots from the USB Restore Media and displays the restore instructions.
13. Select **Restore**. A confirmation dialog opens.
14. Select **Continue**. The restore process starts.
The re-imaging process takes 5 to 10 minutes.
15. Select **Reboot** when the restore has completed.
16. Remove the USB Restore Media as soon as the reboot process starts.
17. Press **F2**.
Wait for the system setup screen to appear.
18. Select **System BIOS > Boot Settings**.
19. Change **Boot Mode** from BIOS to UEFI.
20. Save the changes and exit the system setup.
The server reboots.

The Large Enterprise NVR-AS 4000 G3 System re-starts with its factory system software.

Operating system installation wizard process

The operating system installation wizard follows this process:

1. Configure the Storage Array Server.
 - ▶ For more information, see *"Configure the Storage Array Server" on page 12*
2. Reconnect both SAS cables to the rear of the Storage Array Server.
3. Ensure the other equipment is connected.
4. Confirm the video storage is correctly provisioned.
 - Ensure that the video storage for each instance is accessible from the Storage Array Server. If the disks are not visible, then rescan for them but do not re-initialise the disks.
 - Ensure that each volume is assigned an appropriate drive letter. If they do not have a drive letter assigned, then assign an appropriate drive letter to each volume.
5. Reconfigure the NVR-AS instances on this restored Storage Array Server.
 - ▶ For more information, see *"Configure NVR-AS instances on the Storage Array Server" on page 22*

6

SOFTWARE DESCRIPTION

This chapter provides a description of the configuration dialogs for the NVR-AS 4000 G3 Storage Array Server.

The Large Enterprise NVR-AS 4000 G3 System is configured using the NVR-AS Administrator. You can access this tool via the Start screen:

Start > IndigoVision > NVR-AS Administrator



It is not possible to use the NVR-AS Administrator until you have completed the initial installation of your Large Enterprise NVR-AS 4000 G3 System.

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 NVR-AS 4000 G3.

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 NVR-AS 4000 G3 unit, IndigoVision recommends 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 Large Enterprise NVR-AS 4000 G3 units, the number of connected network interfaces can be specified. The NVR-AS 4000 G3 only generates alerts when it cannot find the specified number of connected network interfaces.
On Large Enterprise NVR-AS 4000 G3 units, all 4 Ethernet ports count towards the number of connected network interfaces.
- **PSU Monitoring** — When selected, the NVR-AS 4000 G3 generates an alert if it does not have redundant power through its power supplies.
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**.



*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.

A 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.

B PHYSICAL CONFIGURATION

This appendix details the cable connections required for the Large Enterprise NVR-AS 4000 G3 System variants.

750TB variant

The diagrams below shows the cable connections for this variant.

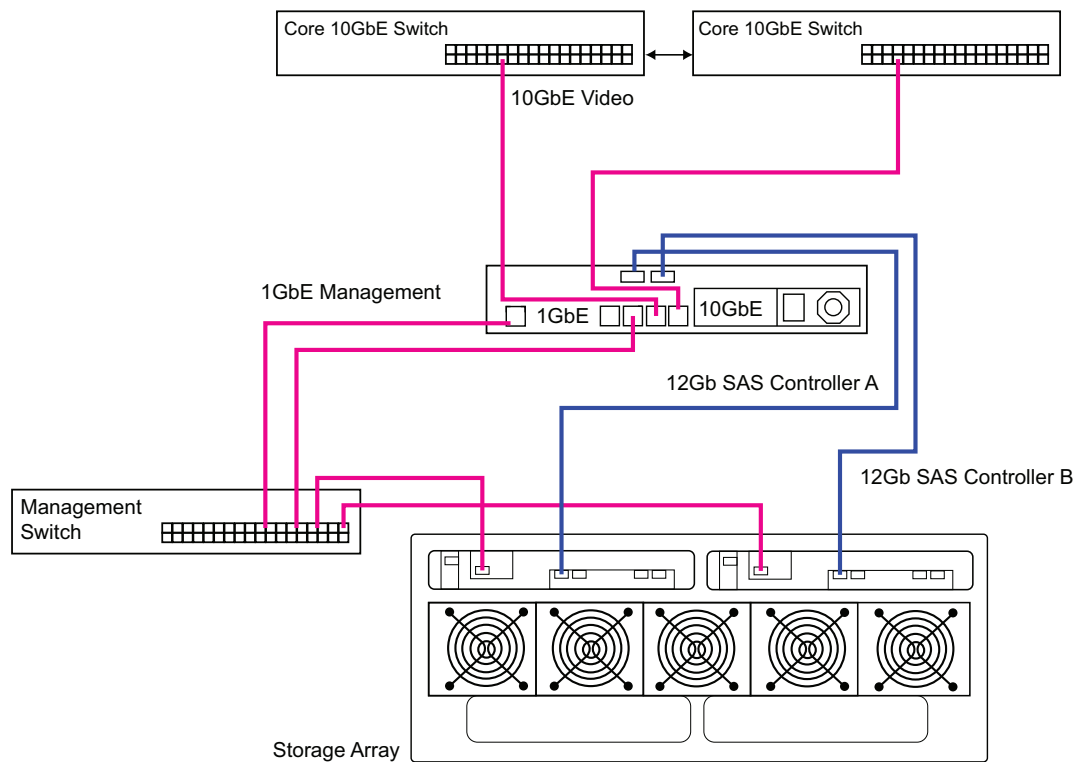


Figure 3: Large Enterprise NVR-AS 4000 G3 System 750TB variant - 10GbE and GbE connections

1.5PB variant

The diagrams below shows the cable connections for this variant.

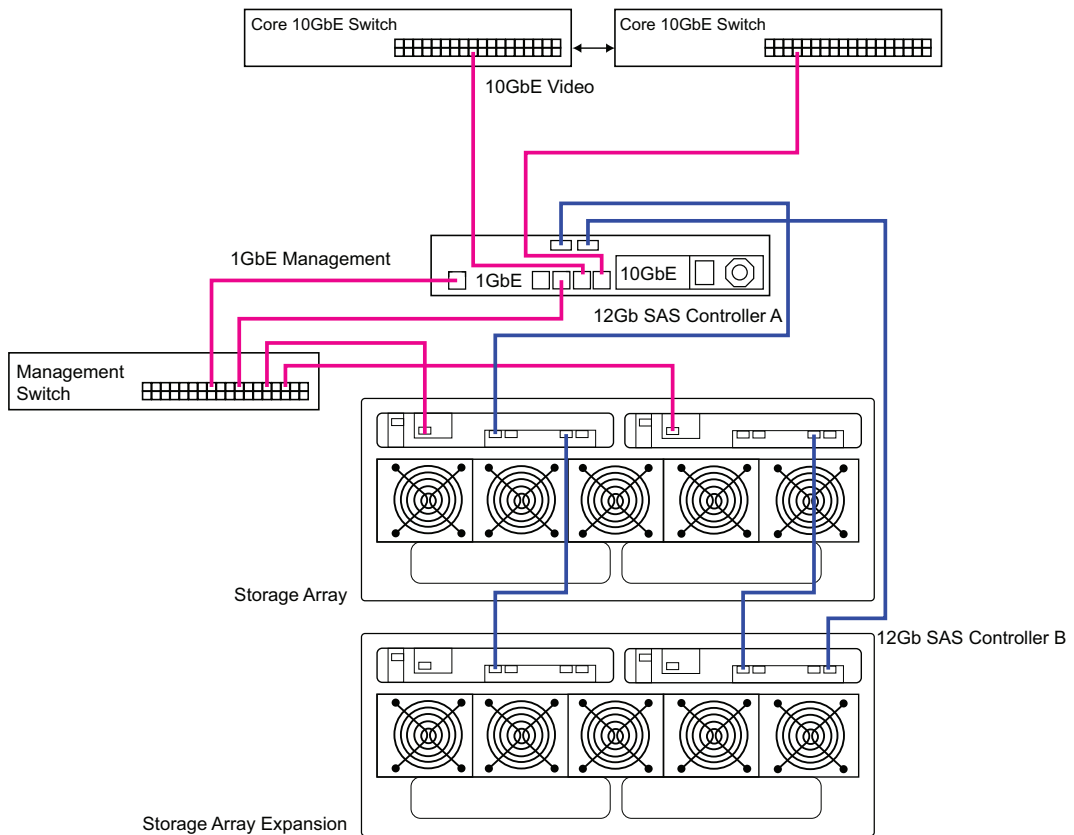


Figure 4: Large Enterprise NVR-AS 4000 G3 System 1.5PB variant - 10GbE and GbE connections

2.25PB variant

The diagrams below shows the cable connections for this variant.

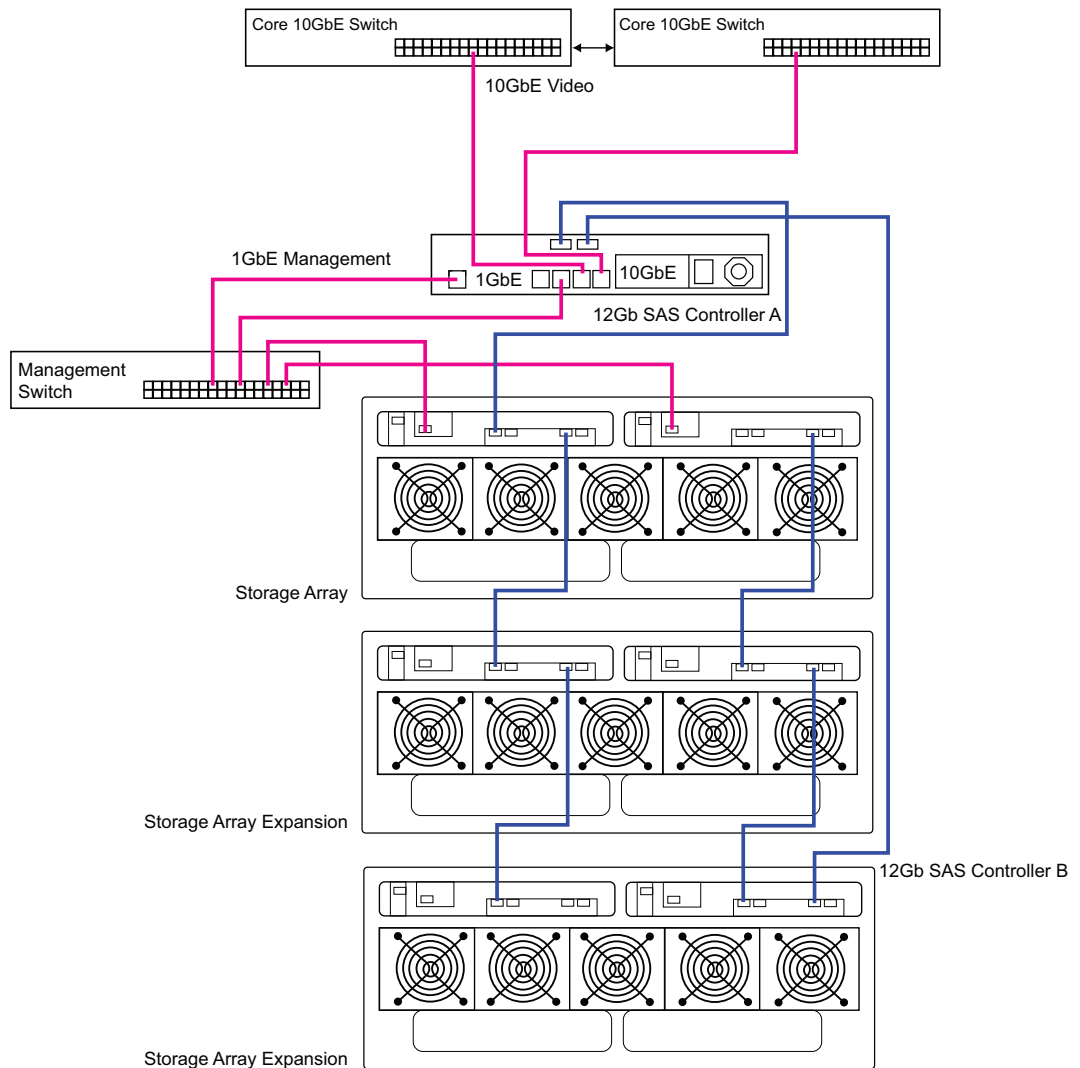


Figure 5: Large Enterprise NVR-AS 4000 G3 System 2.25PB variant - 10GbE and GbE connections

3.0PB variant

The diagrams below shows the cable connections for this variant.

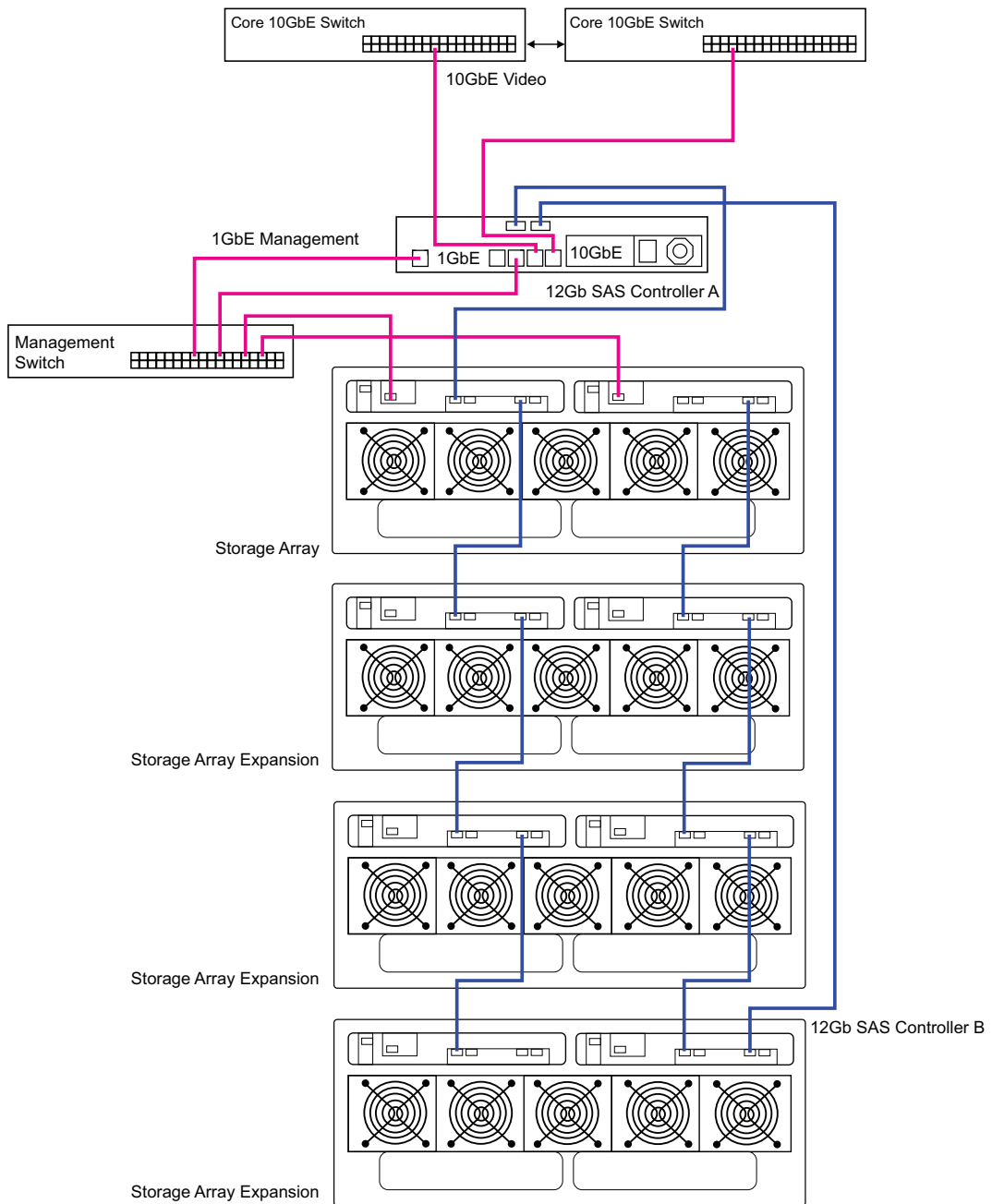


Figure 6: Large Enterprise NVR-AS 4000 G3 System 3PB variant - 10GbE and GbE connections