

IndigoVision

**Network Video Recorder
(NVR-AS)**

4000 Large Enterprise

User Guide



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

DOCUMENT ID: IU-NVR-MAN015-9

Legal Considerations

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

Copyright

COPYRIGHT © INDIGOVISION LIMITED. ALL RIGHTS RESERVED.

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

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

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

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

Contact address

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

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](https://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	7
	Safety notices	7
2	Overview	9
	Hardware	9
	NVR-AS 4000 Storage Array Server (SAS)	10
	NVR-AS 4000 Storage Array	10
	NVR-AS 4000 Storage Array Expansion	10
	Configuration	10
	Fault monitoring	11
3	Getting Started	13
	Overview	13
	Install the rack mounted equipment	13
	Additional guidelines	14
	Configure each Storage Array Server	14
	Power up the Storage Array Server	14
	Complete the operating system setup	14
	Configure the Storage Array Server	16
	Connect the Storage Array Server to other equipment	20
	Configure the video storage	21
	RAID controller configuration	21
	Create a disk group	22
	Create a virtual disk	23
	Assign physical disks as hot spares	23
	Rescan and initialize the disks	23
	Configure NVR-AS instances on each Storage Array Server	24
	Configure the NVR-AS Instance using the NVR-AS Administrator	24
	Install the NVR-AS instance	24
	Create the remaining instances	25

4	Operations	27
	Identifying and replacing a faulty disk in a storage array enclosure	27
	Identifying and replacing other faulty hardware in a storage array enclosure	27
	Operating System Disk management	27
	Operating System RAID redundancy	28
	Replacing a faulty disk	28
	Upgrading NVR-AS software	29
	Install, replace or remove a redundant PSU from the NVR-AS 4000 Large Enterprise System	29
	Install a redundant PSU in the NVR-AS 4000 Large Enterprise System	29
	Replace a redundant PSU in the NVR-AS 4000 Large Enterprise System	30
	Remove a redundant PSU from the NVR-AS 4000 Large Enterprise System	30
	Install a new license or update an existing license	30
	Create and send a fingerprint file	31
	Apply a license file	31
	OMSA X.509 Certificate Management	31
	SSL Server Certificates	32
5	Maintenance	35
	Recover system using USB Restore Media	35
	Operating system installation wizard process	36
6	Software Description	37
	Identification dialog	37
	License Server Details dialog	37
	Storage Locations dialog	37
	Network Settings dialog	38
	Status Monitoring Settings dialog	38
	Disk Space Management dialog	39
	Alarm and Data Record Management dialog	40
	Email Settings dialog	41
	Finish dialog	41
7	Troubleshooting	43
	Monitor recordings	43
	NVR Alerts	43
	Recording failure alerts	43
A	Physical configuration	45
	200/500TB - 350/600 streams - 2400/3000Mbps variant	45
	Video and management network connections	45
	Storage connections	46
	1000TB - 600 streams - 3000Mbps variant	47
	Video and management network connections	47

	Storage connections	48
	1.5PB - 600 streams - 3000Mbps variant	49
	Video and management network connections	49
	Storage connections	50
B	Logical configuration	51
	200/500TB - 350/600 streams - 2400/3000Mbps variant	51
	1.0PB - 600 streams - 3000Mbps variant	51
	1.5PB - 600 streams - 3000Mbps variant	52

1 ABOUT THIS GUIDE

This guide is written for users of the IndigoVision NVR-AS 4000 Large Enterprise 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.



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



Additional information relating to the current section.

2

OVERVIEW

IndigoVision's NVR-AS 4000 Large Enterprise 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 NVR-AS 4000 Large Enterprise 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 3Gbps with simultaneous playback.
- Third party camera support.
- 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.

Hardware

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

- 200TB - 350 streams - 2400Mbps
- 500TB - 600 streams - 3000Mbps
- 1.0PB - 600 streams - 3000Mbps
- 1.5PB - 600 streams - 3000Mbps

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

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

The following figure illustrates the key components of each variant:

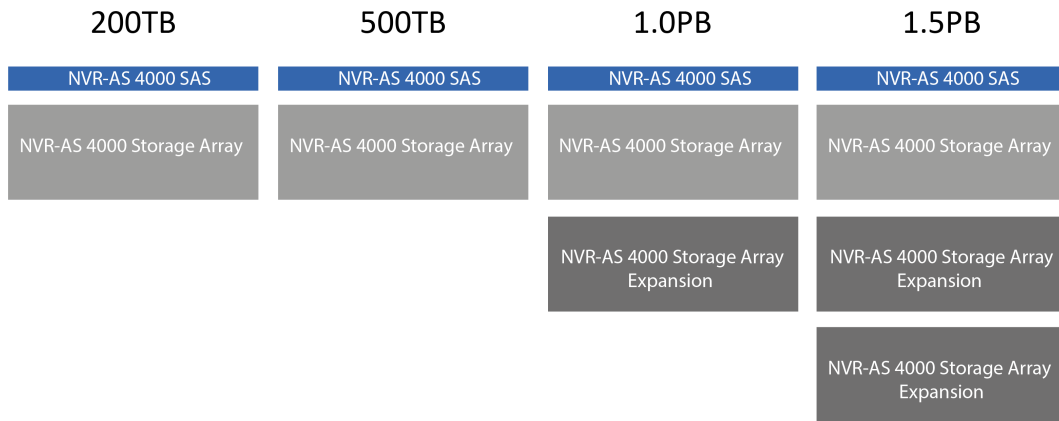


Figure 1: NVR-AS 4000 Large Enterprise System variant components

NVR-AS 4000 Storage Array Server (SAS)

There are two supported generations of NVR-AS 4000 Storage Array server.

G2 Variant

- Video optimized Windows Server 2012 R2 with pre-installed NVR-AS application software
- Dual port 10GbE SFP+ network adapter
- 12Gbps SAS Host Bus Adapter
- 1U

G3 Variant

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

NVR-AS 4000 Storage Array

- Dual redundant RAID controller
- 60 x 4TB or 10TB Nearline SAS disks
- 4U

NVR-AS 4000 Storage Array Expansion

- Needs an NVR-AS 4000 Storage Array for RAID Support
- 60 x 10TB Nearline SAS disks
- 4U

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 NVR-AS 4000 Large Enterprise 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 (if installed)
- Network interfaces

The redundant power supply and network interface monitoring must be configured before it is enabled.

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

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

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

3

GETTING STARTED

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

Overview

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

1. Install the rack mounted equipment into suitable cabinets.
2. Configure each Storage Array Server.
3. Connect the Storage Array Server to the NVR-AS 4000 Large Enterprise System.
4. Configure the video storage.
5. Configure NVR-AS instances on each Storage Array Server.

Repeat the configuration steps 2 to 5 for each 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 NVR-AS 4000 Large Enterprise System weighs between 125kg and 350kg (276lb and 772lb) 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 NVR-AS 4000 Large Enterprise 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 NVR-AS 4000 Large Enterprise System should be located close to one another, all in the same cabinet.
- Careful layout and labeling is advised to keep each NVR-AS 4000 Large Enterprise System clearly separated.
- When there are multiple Storage Array Servers for one NVR-AS 4000 Large Enterprise System, locate them next to each other.

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

- For more information, see *"Physical configuration" on page 45*

Configure each Storage Array Server

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

Each 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 35*
-

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 Enterprise NVR-AS 4000 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.



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

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

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

Installation wizards before version 15.3

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

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

Notice

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

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



Warning

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

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

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

Installation wizards from version 15.3 onwards

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

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

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

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

► For more information, see *"IndigoVision License Server configuration" on page 16*

You can now configure the rest of the Enterprise NVR-AS 4000 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 more information, see *"Logical configuration" on page 51*
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 17*
5. If required, configure the Remote Desktop settings.
► For more information, see *"Remote desktop configuration" on page 19*
6. Install the Modular Disk Storage Manager.
► For more information, see *"Install the Modular Disk Storage Manager" on page 20*

IndigoVision License Server configuration

To complete the NVR-AS setup and allow it to record, you must configure the NVR-AS 4000 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 NVR-AS 4000 Large Enterprise Installation Wizard offers the ability to configure this NVR-AS 4000 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 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.*



Configuring the NVR-AS 4000 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 NVR-AS 4000 Large Enterprise 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: 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 primary 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: 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.

Primary time server

If this NVR-AS 4000 Large Enterprise System will act as a primary 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: 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

Teaming behaviour varies between the G2 and G3 variants.

NVR-AS 4000 Large Enterprise G2

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

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

NVR-AS 4000 Large Enterprise G3

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

If the ports on the switch are configured for LACP, the Network Video Recorder (NVR-AS) 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 NVR-AS 4000 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.

Install the Modular Disk Storage Manager

The Modular Disk Storage Manager (MDSM) installer is included on the storage array server. It must be installed to complete the Storage Array Server configuration.

To install the MDSM follow these steps:

1. Locate the MDSM directory on the C: drive.
C:\MDSM_<version>
2. Double-click **md_launcher.exe** from the root of the resources. The storage array resource DVD menu opens.
3. Select **Install MD Storage Software**.
4. Choose a locale and select **OK**.
5. At the Welcome screen select **Next**.
6. Read the license agreement carefully, select **I accept the terms of the License Agreement**, then select **Next**.
7. At the first **Feature Selection** screen, ensure that all of the features are enabled, then select **Next**.
8. At the **Automatically Start the Event Monitor** screen, select the **No, I will manually start the event monitor service** option, then select **Next**.

Notice *If the Event Fault Monitoring service (included with the Modular Disk Storage Manager) is manually configured, ensure that it is enabled on only one host. Configuration on more than one host will impact the performance of the storage array.*

This service is not required for integrated fault monitoring within IndigoVision Control Center.

9. On the **Configuration** utility screen, ensure that **No** is selected for **Automatic Modular Disk Configuration Utility** start-up at first reboot.
10. Click **Next**. Ensure you have not modified the default installation directory.
11. A dialog is displayed with details of driver installation. Accept all requests.
12. Review the installation summary then select **Install**.
13. At the end of the installation restart your system. Allow the Storage Array Server to reboot.

Connect the Storage Array Server to other equipment

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

- For more information, see *"Physical configuration" on page 45*
 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 storage array expansions, connect SAS cables between the first and second storage array expansions.
 - Ensure that the SAS connections going into each management module are connected to SAS port 1 and not SAS port 2.
- 3. Connect the network cables.
 - a. Connect one 10GbE network port on each Storage Array Server to each of the video network switches.
 - b. Connect the GbE network ports on each 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 NVR-AS 4000 Large Enterprise 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. RAID Controller configuration.
2. Create a disk group.
3. Create a virtual disk.
4. Assign physical disks as hot spares.
5. Rescan and initialize the disks.

The details of each disk group and hot spares for each variant are provided in the Appendix.

- For more information, see *"Logical configuration" on page 51*

RAID controller configuration

1. Note the name of the Storage Array Server.
 - a. Right-click the **Start** screen icon.
 - b. Select **System**.
The name of the Storage Array Server is shown in the **Computer name** field.
2. Open the Modular Disk Storage Manager (MDSM) using the desktop shortcut and accept the automatic scan.
3. The array should be available in MDSM. If it is not, then rescan for it.
 - a. Right-click the node for the current host in the **Devices** tab.

- b. Click **Automatic Discovery**.
4. If required, rename the storage array.
 - a. Right-click the node.
 - b. Click **Rename**.
5. Double-click the storage array node.
6. The MDSM application displays dialogs with automatic configuration suggestions. Reject these and continue with manual configuration.
7. If the system has three enclosures, then the Premium Feature needs to be enabled.
 - a. In the **Summary** tab, click **Manage Premium Features**.
 - b. Select **Use Key File...**
 - c. Locate the **Feature Key** file.
8. Configure the network interfaces on the RAID controllers so that they are appropriate for the management network.
 - a. In the Array Management interface, select the **Hardware** tab, then scroll down to the image of the two RAID controllers in Enclosure 0 (back).
 - b. Right-click on the first RAID controller and select **Configure > Management Ports...**
 - c. Select the **IPv4 Settings** tab and modify the IP address, subnet mask, and gateway for the first RAID controller (by default this should be set to DHCP).
 - d. Click **OK** to update the configuration for the first RAID controller.
 - e. Right-click on the second controller and select **Configure > Management Ports...**
 - f. Modify the IPv4 address, subnet mask, and gateway for the second RAID controller (by default this should be set to DHCP).
 - g. Click **OK** to update the configuration for the second RAID controller.

Create a disk group

On the **Storage & Copy Services** tab, create a **Disk Group** on the array.

1. Right-click **Total Unconfigured Capacity**.
2. Select **Create Disk Group**.
3. Name the **Disk Group**.
4. In the **Physical Disk** section, select **Manual**.

Notice

Do not create Disk Pools as storage capacity will not be optimal and performance may be impacted.

5. From the Disk Group, select **RAID6** for the **RAID level**.



Only create RAID6 groups. Using other RAID levels is not supported and increases the potential for data loss.

6. Select the physical disks to be used for the disk group.
 - For more information, see "Logical configuration" on page 51
7. Select **Calculate Capacity**.
8. Verify that the capacity and number of disks are as expected.
9. Click **Finish**.

Create a virtual disk

After you have created a disk group create a virtual disk.

1. Confirm that you wish to create **Virtual Disks**.
2. Select **TB** for the **Units**.
3. Type the required capacity.
4. Type a **Virtual Disk name**.
5. Select the Storage Array Server that the Virtual Disk host should be mapped to, or select **Map Now to Default Group**.
6. Click **Finish** to create the Virtual Disk.

Assign physical disks as hot spares

After the virtual disks have been created, assign physical disks as hot spares for the group.

1. Select the **Hardware** tab.
2. Right-click any disk and select **Hot Spare Coverage**.
3. Click **View/change current hot spare coverage**.
4. Click **Assign**.
5. Choose the physical disks to be assigned.
 - For more information, see "Logical configuration" on page 51
6. Click **Close**.

Rescan and initialize the disks

After you have created the virtual disks and assigned physical disks as hot spares, you need to initialize the disks from each of the Storage Array Servers. The virtual disks will be mapped to their corresponding Storage Array Server. For each Storage Array Server, rescan for the virtual disks mapped to that server and initialize the partition tables.

1. Open the Disk Management panel for the Storage Array Server.
 - a. Right-click the **Start** screen icon and select **Computer Management**.
This opens the **Computer Management** dialog.
2. Select the os (C:) drive.
3. Right-click the Disk Management node and click **Rescan Disks**.
If **Rescan Disks** is unavailable, click any of the existing disks and try again.
The Virtual Disks that were defined and mapped will then be visible.
4. Right-click one of the new disks (not its partitions).
5. Click **Online**.
6. Click **Initialize Disk**.
7. Select all the new disks.
8. Click **GPT (GUID Partition Table)**.
9. Click **OK**.
10. Create a **New Simple Volume** and format a single NTFS file system within each mapped disk.
11. Specify 64KB allocation units, and a volume drive letter as required.

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.

Configure NVR-AS instances on each Storage Array Server

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

Each Storage Array Server must be set up to have multiple NVR-AS instances.

► For more information, see *"Logical configuration" on page 51*

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.

The expected IP address, video storage location, and configuration storage location for each instance are detailed in the Appendix.

► For more information, see *"Logical configuration" on page 51*

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.
- Check that the IP address configured for the instance is valid for the machine and that is not in use by another NVR-AS instance. The IP addresses were created during initial setup of the Storage Array Server.

Create the remaining instances

Repeat the previous tasks for the remaining instances for each 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 NVR-AS 4000 Large Enterprise System device.

Identifying and replacing a faulty disk in a storage array enclosure

Available hot spares are used immediately to rebuild a disk group if it is degraded.

► For more information, see *"Assign physical disks as hot spares" on page 23*

Failed disks should be identified and replaced at the earliest opportunity in order to maintain system redundancy. Use the Modular Disk Storage Manager 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.
3. Replace the disk.
4. Slide the drawer shut and replace the bezel.

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

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 Modular Disk Storage Manager to identify the failed component and its location.

Operating System Disk management

NVR-AS 4000 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 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. 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 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. Depending on the variant, the disks can either be found in the two hotswappable bays at the rear of the Storage Array Server, or behind the bezel on the front.

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.

- 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.

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, replace or remove a redundant PSU from the NVR-AS 4000 Large Enterprise System

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

Install a redundant PSU in the NVR-AS 4000 Large Enterprise System

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

- For more information, see "Getting Started" on page 13
-

To add a second PSU to the unit:

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

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

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

Notice *The next time the unit reboots, it may go through an automatic configuration stage including a 2 minute power-off period. At the end of this process, the unit automatically reboots and starts normally.*

Replace a redundant PSU in the NVR-AS 4000 Large Enterprise System



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

To replace a PSU in the unit:

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

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

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

Notice

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

Remove a redundant PSU from the NVR-AS 4000 Large Enterprise System



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

To remove a secondary PSU from the unit:

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

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

1. Power down the unit.
2. Remove AC power from the remaining PSU for at least 15 seconds.
3. Re-attach AC power to the remaining PSU and start the unit normally.

Install a new license or update an existing license

You can configure the NVR-AS 4000 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 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 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 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 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 Certificate Authority (CA) trusted by the operating system. Some secure browser settings can also block the self-signed SSL certificates. The Server Administrator web GUI requires a CA-signed certificate for such secure browsers.*

- **Certificate Maintenance** – Allows you to generate a Certificate Signing Request (CSR) containing all the certificate information about the host required by the CA to automate the creation of a trusted SSL web certificate. You can retrieve the necessary CSR file either from the instructions on the Certificate Signing Request (CSR) page or by copying the entire text in the text box on the CSR page and pasting it in the CA submit form. The text must be in the Base64-encoded format.

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

- **Import certificate chain** – Allows you to import the certificate chain (in PKCS#7 format) signed by a trusted CA. The certificate can be in DER or Base64-encoded format.
- **Import a PKCS12 Keystore** – Allows you to import a PKCS#12 keystore that replaces the private key and certificate used in Server Administrator web server. PKCS#12 is a public keystore that contains a private key and the certificate for a web server. Server Administrator uses the Java KeyStore (JKS) format to store the SSL certificates and its private key. Importing a PKCS#12 keystore to Server Administrator deletes the keystore entries, and imports a private key and certificate entries to the Server Administrator JKS.

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

SSL Server Certificates

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

An SSL-enabled system can perform the following tasks:

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

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

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

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

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

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

The CA will return a signed SSL certificate.

3. Upload the certificate to Server Administrator.

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

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

5

MAINTENANCE

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

Recover system using USB Restore Media

If the NVR-AS 4000 Large Enterprise 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 28
- For more information about RAID configuration for an NVR-AS 4000 Storage Array Server, see *"Operating system installation wizard process"* on page 36

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 NVR-AS 4000 Large Enterprise System you are recovering.

4. Insert the USB Restore Media.
5. Power on the NVR-AS 4000 Large Enterprise 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 NVR-AS 4000 Large Enterprise 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 NVR-AS 4000 Large Enterprise 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 each Storage Array Server" on page 14*
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 each Storage Array Server" on page 24*

6

SOFTWARE DESCRIPTION

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

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

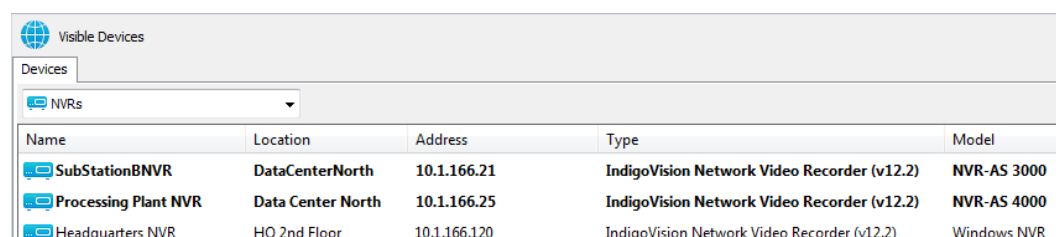
Start > IndigoVision > NVR-AS Administrator



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

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 unit, IndigoVision recommend that you create a Device Fault Detector for the NVR.*

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

- **Network Monitoring** – When selected, the NVR-AS 4000 generates an alert when the Ethernet ports are not correctly connected to the network.
On NVR-AS 4000 Large Enterprise units, the number of connected network interfaces can be specified. The NVR-AS 4000 only generates alerts when it cannot find the specified number of connected network interfaces.
On NVR-AS 4000 Large Enterprise units, all 4 Ethernet ports count towards the number of connected network interfaces.
- **PSU Monitoring (supported devices only)** – When selected, the NVR-AS 4000 generates an alert if it does not have redundant power through its power supplies.
If the unit has been intentionally installed without redundant power, clear this option to avoid unnecessary alerts. If the unit is not capable of providing redundant power, the PSU Monitoring option does not appear.
Alerts are always generated in Control Center for video storage array faults, complete network failure (device unavailable) or fan failures.

Disk Space Management dialog

Use this dialog to configure the disk space management settings.

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

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

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

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

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

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

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

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

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

- **Enable Tamper Protection on recordings:** The NVR-AS will embed digital signatures in every recording file allowing the authenticity and integrity of that footage to be verified at any point in the future.
Verification will happen whenever footage is exported by Control Center as part of an Incident and the result of the verification will be written into the Incident. This provides an extra level of security: the Incident itself is protected by a watermark proving that the Incident has not been tampered with, and the NVR digital signatures prove that the footage on the NVR had not been tampered with at the point of export. Tamper Protection is not compatible with video thinning. You cannot enable Tamper Protection if video thinning is already enabled.



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

- **Enable video thinning:** Video thinning removes the intermediate P-frames leaving only independent I-frames. This leads to a dramatic reduction in the storage requirements but at the expense of full motion video.
For effective use of video thinning, it is important to configure the maximum I-frame interval on the transmitter such that the frame rate of thinned footage is acceptable. Video thinning is most effective on footage with significant amounts of motion. MJPEG and JPEG 2000 streams only contain I-frames, so thinning does not have any effect on footage in these formats.
Video thinning is not compatible with Tamper Protection. You cannot enable video thinning if Tamper Protection is already enabled.
- **Reduce storage to I-frames only after:** Video thinning is performed on footage once the time entered here has elapsed.
- **Enable automatic unprotect of video:** Select this checkbox to automatically unprotect video older than the age specified in **Unprotect video after**.



*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.

Some email providers support setting up a secondary email password, sometimes referred to as an app password, to be used when email clients connect.

If the NVR reports an authentication problem when trying to connect to the email server with the normal password, and all details have been verified as correct, it is possible that a secondary password will need to be set up and used in this dialog in place of the standard one.

- For more information, refer to the email client setup instructions from the email provider.

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.

A PHYSICAL CONFIGURATION

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

200/500TB - 350/600 streams - 2400/3000Mbps variant

The diagrams below shows the cable connections for this variant.

Video and management network connections

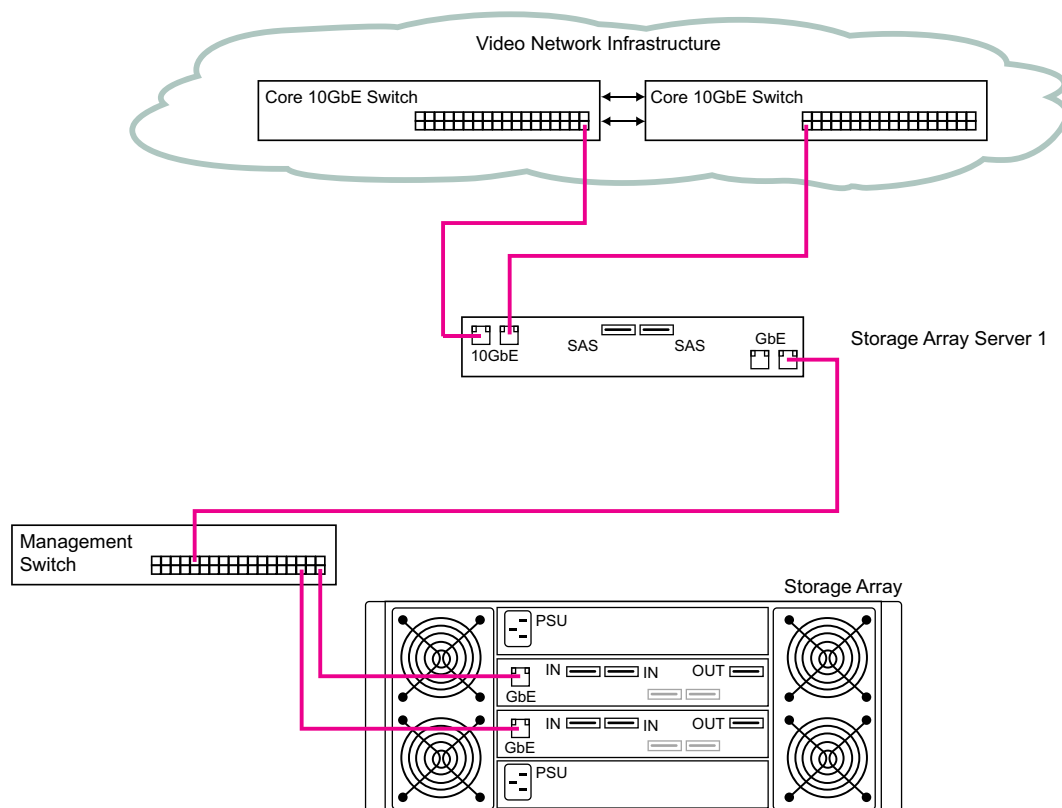


Figure 3: NVR-AS 4000 Large Enterprise System 200/500TB - 350/600 streams - 2400/3000Mbps variant - 10GbE and GbE connections

Storage connections

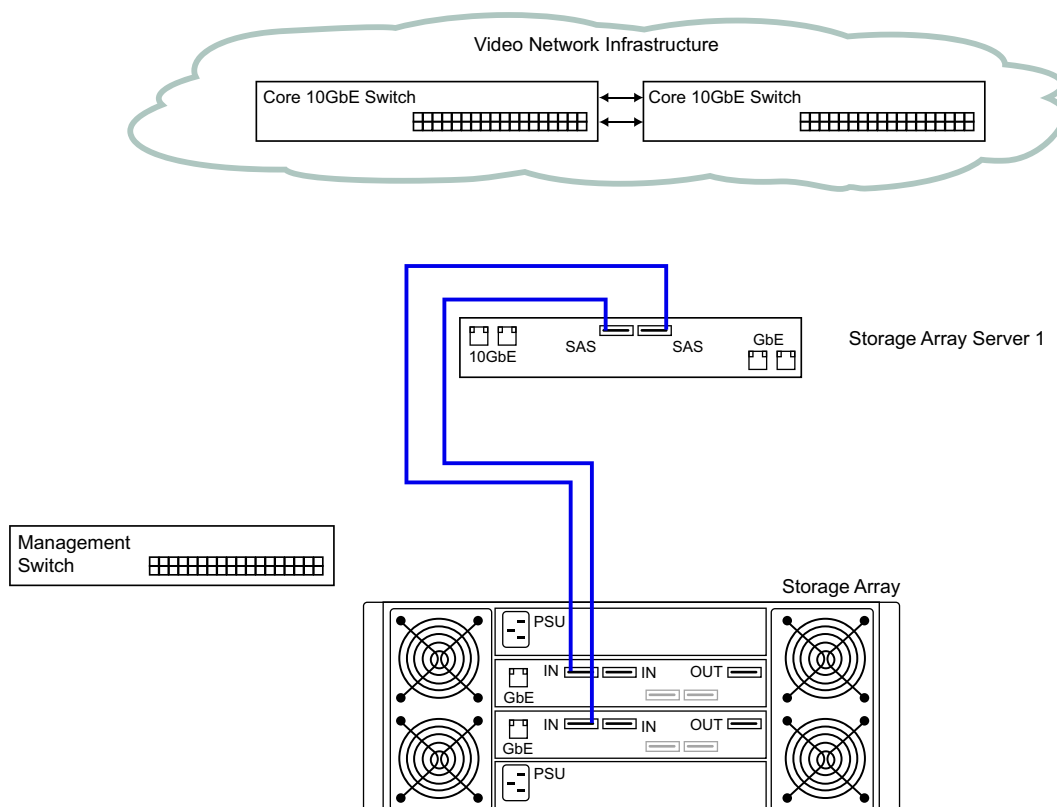


Figure 4: NVR-AS 4000 Large Enterprise System 200/500TB - 350/600 streams - 2400/3000Mbps variant - SAS connections

1000TB - 600 streams - 3000Mbps variant

The diagrams below shows the cable connections for this variant.

Video and management network connections

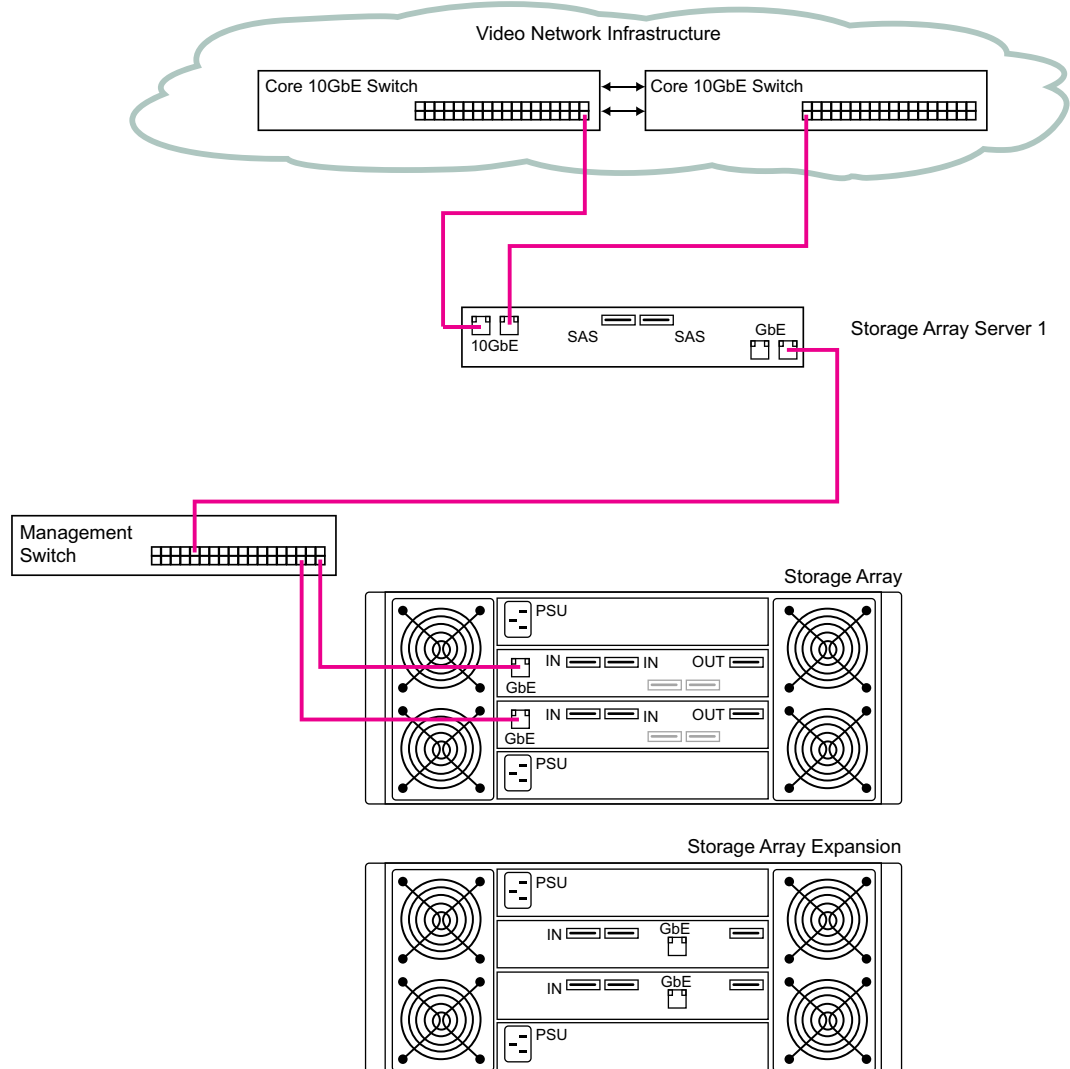


Figure 5: NVR-AS 4000 Large Enterprise System 1000TB - 600 streams - 3000Mbps variant - 10GbE and GbE connections

Storage connections

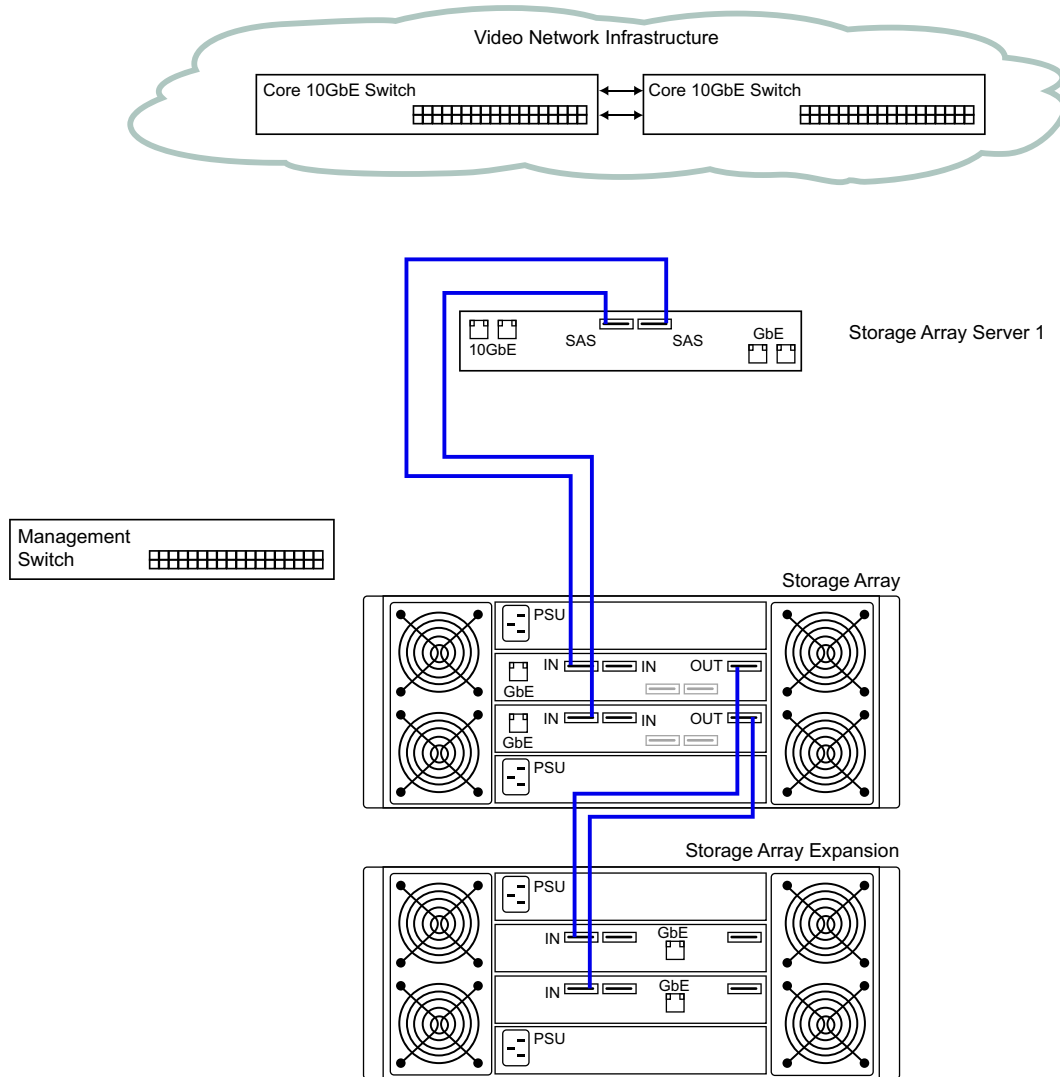


Figure 6: NVR-AS 4000 Large Enterprise System 1000TB - 600 streams - 3000Mbps variant - SAS connections

1.5PB - 600 streams - 3000Mbps variant

The diagrams below shows the cable connections for this variant.

Video and management network connections

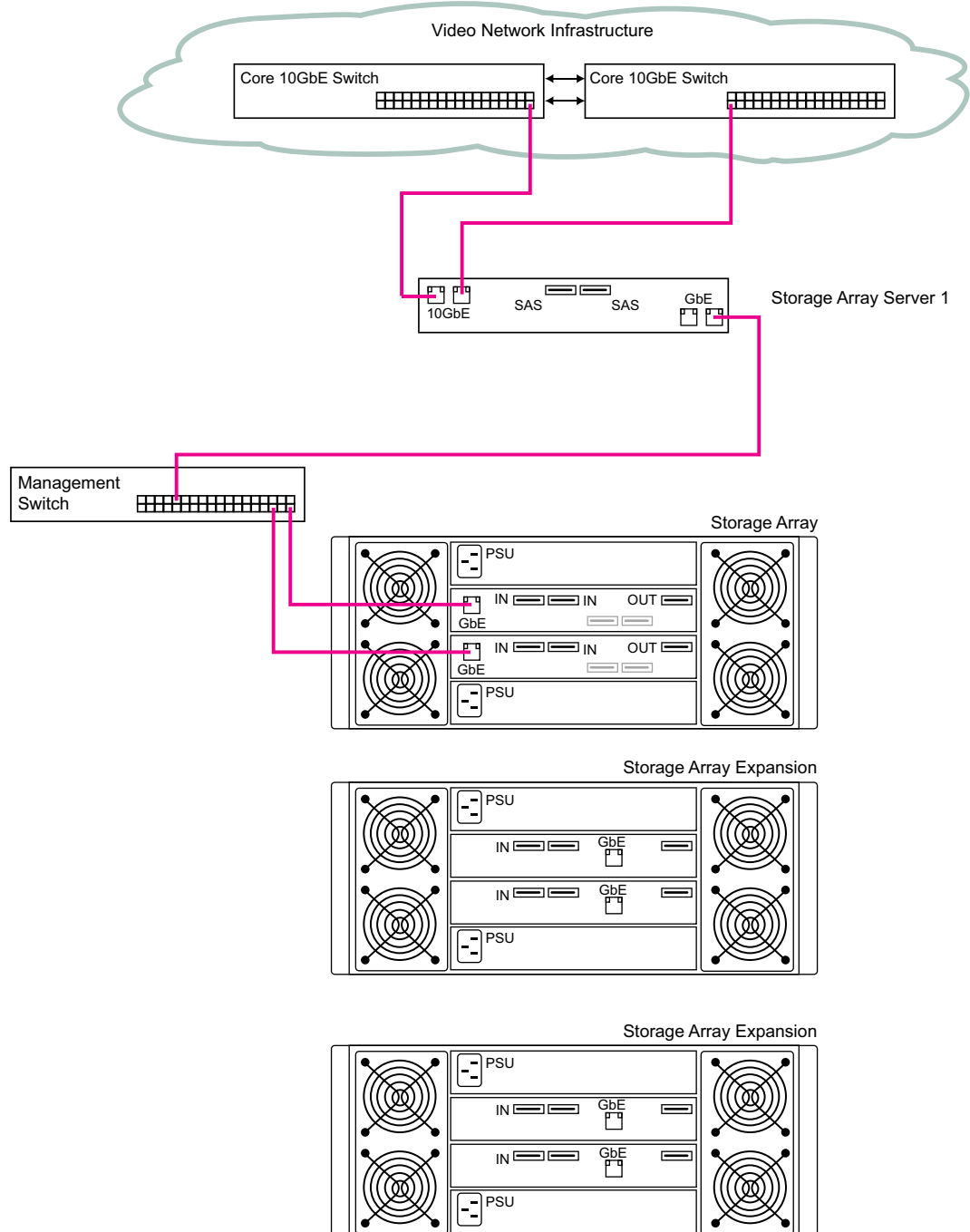


Figure 7: NVR-AS 4000 Large Enterprise System 1.5PB - 600 streams - 3000Mbps variant - 10GbE and GbE connections

Storage connections

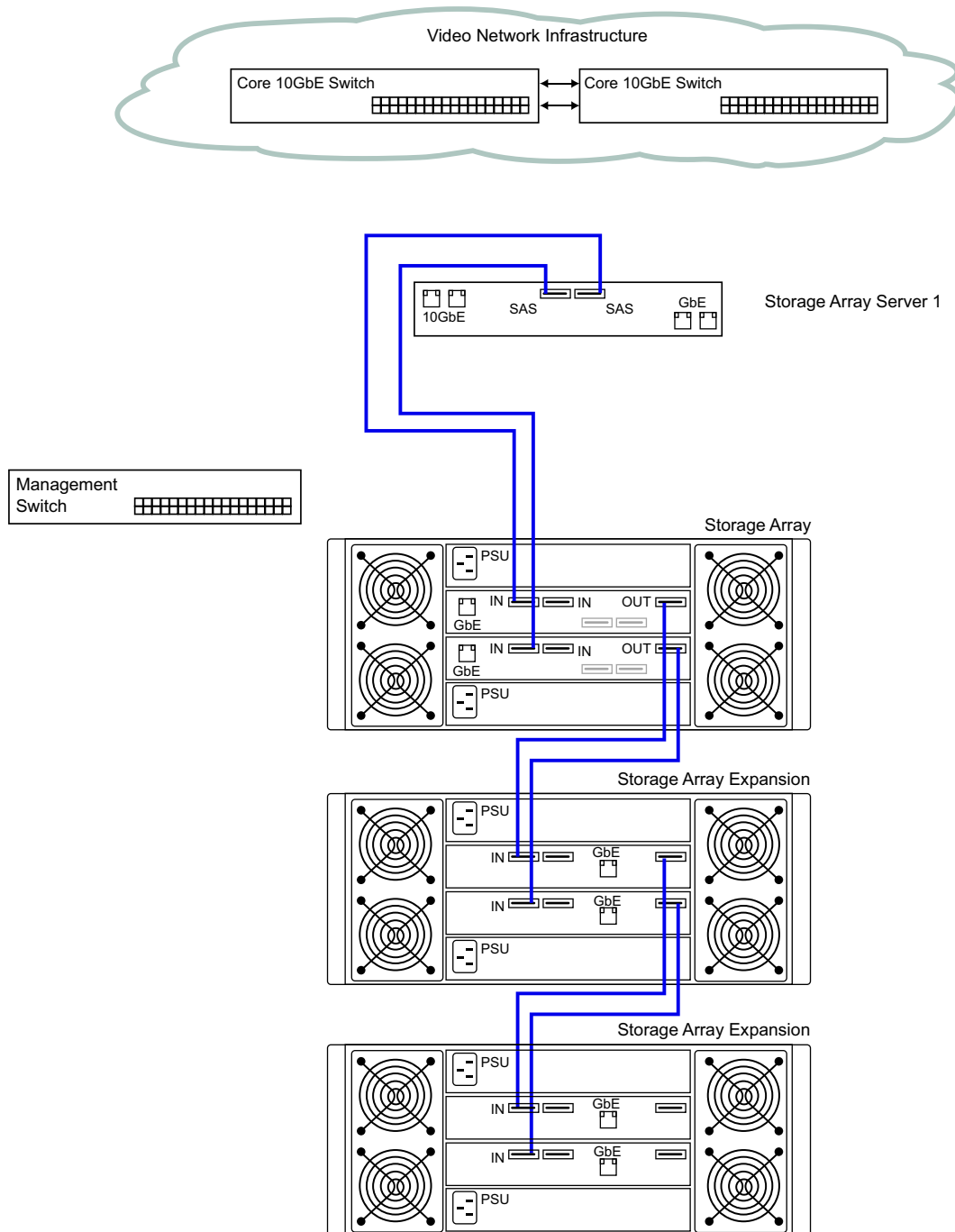


Figure 8: NVR-AS 4000 Large Enterprise System 1.5PB - 600 streams - 3000Mbps variant - SAS connections

B LOGICAL CONFIGURATION

This appendix provides details of the logical configuration for each of the NVR-AS 4000 Large Enterprise System variants.

200/500TB - 350/600 streams - 2400/3000Mbps variant

The following diagram shows the logical configuration for this variant.

Video network: 10.5.1.0/8
Management network: 192.168.0.0/24

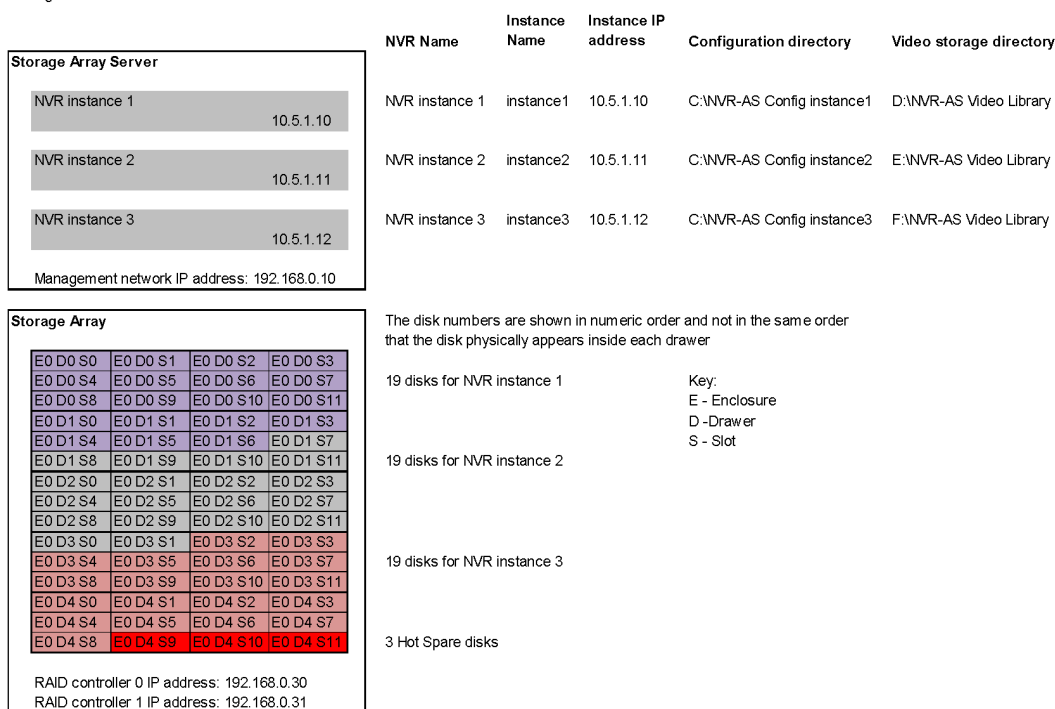


Figure 9: 200/500TB - 350/600 streams - 2400/3000Mbps variant logical configuration

1.0PB - 600 streams - 3000Mbps variant

The following diagram shows the logical configuration for this variant.

Video network: 10.5.1.0/8
Management network: 192.168.0.0/24

Storage Array Server

NVR instance 1	10.5.1.10
NVR instance 2	10.5.1.11
NVR instance 3	10.5.1.12
NVR instance 4	10.5.1.13
NVR instance 5	10.5.1.14
NVR instance 6	10.5.1.15

Management network IP address: 192.168.0.10

NVR Name	Instance Name	Instance IP address	Configuration directory	Video storage directory
NVR instance 1	instance1	10.5.1.10	C:\NVR-AS Config instance1	D:\NVR-AS Video Library
NVR instance 2	instance2	10.5.1.11	C:\NVR-AS Config instance2	E:\NVR-AS Video Library
NVR instance 3	instance3	10.5.1.12	C:\NVR-AS Config instance3	F:\NVR-AS Video Library
NVR instance 4	instance4	10.5.1.13	C:\NVR-AS Config instance4	G:\NVR-AS Video Library
NVR instance 5	instance5	10.5.1.14	C:\NVR-AS Config instance5	H:\NVR-AS Video Library
NVR instance 6	instance6	10.5.1.15	C:\NVR-AS Config instance6	I:\NVR-AS Video Library

Storage Array

E0 D0 S0	E0 D0 S1	E0 D0 S2	E0 D0 S3
E0 D0 S4	E0 D0 S5	E0 D0 S6	E0 D0 S7
E0 D0 S8	E0 D0 S9	E0 D0 S10	E0 D0 S11
E0 D1 S0	E0 D1 S1	E0 D1 S2	E0 D1 S3
E0 D1 S4	E0 D1 S5	E0 D1 S6	E0 D1 S7
E0 D1 S8	E0 D1 S9	E0 D1 S10	E0 D1 S11
E0 D2 S0	E0 D2 S1	E0 D2 S2	E0 D2 S3
E0 D2 S4	E0 D2 S5	E0 D2 S6	E0 D2 S7
E0 D2 S8	E0 D2 S9	E0 D2 S10	E0 D2 S11
E0 D3 S0	E0 D3 S1	E0 D3 S2	E0 D3 S3
E0 D3 S4	E0 D3 S5	E0 D3 S6	E0 D3 S7
E0 D3 S8	E0 D3 S9	E0 D3 S10	E0 D3 S11
E0 D4 S0	E0 D4 S1	E0 D4 S2	E0 D4 S3
E0 D4 S4	E0 D4 S5	E0 D4 S6	E0 D4 S7
E0 D4 S8	E0 D4 S9	E0 D4 S10	E0 D4 S11

RAD controller 0 IP address: 192.168.0.30
RAD controller 1 IP address: 192.168.0.31

The disk numbers are shown in numeric order and not in the same order that the disk physically appears inside each drawer

19 disks for NVR instance 1
Key:
E - Enclosure
D - Drawer
S - Slot

19 disks for NVR instance 2

19 disks for NVR instance 3

3 Hot Spare disks

Storage Array Expansion

E1 D0 S0	E1 D0 S1	E1 D0 S2	E1 D0 S3
E1 D0 S4	E1 D0 S5	E1 D0 S6	E1 D0 S7
E1 D0 S8	E1 D0 S9	E1 D0 S10	E1 D0 S11
E1 D1 S0	E1 D1 S1	E1 D1 S2	E1 D1 S3
E1 D1 S4	E1 D1 S5	E1 D1 S6	E1 D1 S7
E1 D1 S8	E1 D1 S9	E1 D1 S10	E1 D1 S11
E1 D2 S0	E1 D2 S1	E1 D2 S2	E1 D2 S3
E1 D2 S4	E1 D2 S5	E1 D2 S6	E1 D2 S7
E1 D2 S8	E1 D2 S9	E1 D2 S10	E1 D2 S11
E1 D3 S0	E1 D3 S1	E1 D3 S2	E1 D3 S3
E1 D3 S4	E1 D3 S5	E1 D3 S6	E1 D3 S7
E1 D3 S8	E1 D3 S9	E1 D3 S10	E1 D3 S11
E1 D4 S0	E1 D4 S1	E1 D4 S2	E1 D4 S3
E1 D4 S4	E1 D4 S5	E1 D4 S6	E1 D4 S7
E1 D4 S8	E1 D4 S9	E1 D4 S10	E1 D4 S11

19 disks for NVR instance 4

19 disks for NVR instance 5

19 disks for NVR instance 6

3 Hot Spare disks

Figure 10: 1.0PB - 600 streams - 3000Mbps variant logical configuration

1.5PB - 600 streams - 3000Mbps variant

The following diagram shows the logical configuration for this variant.

Video network: 10.5.1.0/8
Management network: 192.168.0.0/24

Storage Array Server

NVR instance 1	10.5.1.10
NVR instance 2	10.5.1.11
NVR instance 3	10.5.1.12
NVR instance 4	10.5.1.13
NVR instance 5	10.5.1.14
NVR instance 6	10.5.1.15
NVR instance 7	10.5.1.16
NVR instance 8	10.5.1.17
NVR instance 9	10.5.1.18

Management network IP address: 192.168.0.10

NVR Name	Instance Name	Instance IP address	Configuration directory	Video storage directory
NVR instance 1	instance1	10.5.1.10	C:\NVR-AS Config instance1	D:\NVR-AS Video Library
NVR instance 2	instance2	10.5.1.11	C:\NVR-AS Config instance2	E:\NVR-AS Video Library
NVR instance 3	instance3	10.5.1.12	C:\NVR-AS Config instance3	F:\NVR-AS Video Library
NVR instance 4	instance4	10.5.1.13	C:\NVR-AS Config instance4	G:\NVR-AS Video Library
NVR instance 5	instance5	10.5.1.14	C:\NVR-AS Config instance5	H:\NVR-AS Video Library
NVR instance 6	instance6	10.5.1.15	C:\NVR-AS Config instance6	I:\NVR-AS Video Library
NVR instance 7	instance7	10.5.1.16	C:\NVR-AS Config instance7	J:\NVR-AS Video Library
NVR instance 8	instance8	10.5.1.17	C:\NVR-AS Config instance8	K:\NVR-AS Video Library
NVR instance 9	instance9	10.5.1.18	C:\NVR-AS Config instance9	L:\NVR-AS Video Library

Storage Array

E0 D0 S0	E0 D0 S1	E0 D0 S2	E0 D0 S3
E0 D0 S4	E0 D0 S5	E0 D0 S6	E0 D0 S7
E0 D0 S8	E0 D0 S9	E0 D0 S10	E0 D0 S11
E0 D1 S0	E0 D1 S1	E0 D1 S2	E0 D1 S3
E0 D1 S4	E0 D1 S5	E0 D1 S6	E0 D1 S7
E0 D1 S8	E0 D1 S9	E0 D1 S10	E0 D1 S11
E0 D2 S0	E0 D2 S1	E0 D2 S2	E0 D2 S3
E0 D2 S4	E0 D2 S5	E0 D2 S6	E0 D2 S7
E0 D2 S8	E0 D2 S9	E0 D2 S10	E0 D2 S11
E0 D3 S0	E0 D3 S1	E0 D3 S2	E0 D3 S3
E0 D3 S4	E0 D3 S5	E0 D3 S6	E0 D3 S7
E0 D3 S8	E0 D3 S9	E0 D3 S10	E0 D3 S11
E0 D4 S0	E0 D4 S1	E0 D4 S2	E0 D4 S3
E0 D4 S4	E0 D4 S5	E0 D4 S6	E0 D4 S7
E0 D4 S8	E0 D4 S9	E0 D4 S10	E0 D4 S11

RAID controller 0 IP address: 192.168.0.30
RAID controller 1 IP address: 192.168.0.31

The disk numbers are shown in numeric order and not in the same order that the disk physically appears inside each drawer

19 disks for NVR instance 1

Key:
E - Enclosure
D - Drawer
S - Slot

19 disks for NVR instance 2

19 disks for NVR instance 3

3 Hot Spare disks

Storage Array Expansion

E1 D0 S0	E1 D0 S1	E1 D0 S2	E1 D0 S3
E1 D0 S4	E1 D0 S5	E1 D0 S6	E1 D0 S7
E1 D0 S8	E1 D0 S9	E1 D0 S10	E1 D0 S11
E1 D1 S0	E1 D1 S1	E1 D1 S2	E1 D1 S3
E1 D1 S4	E1 D1 S5	E1 D1 S6	E1 D1 S7
E1 D1 S8	E1 D1 S9	E1 D1 S10	E1 D1 S11
E1 D2 S0	E1 D2 S1	E1 D2 S2	E1 D2 S3
E1 D2 S4	E1 D2 S5	E1 D2 S6	E1 D2 S7
E1 D2 S8	E1 D2 S9	E1 D2 S10	E1 D2 S11
E1 D3 S0	E1 D3 S1	E1 D3 S2	E1 D3 S3
E1 D3 S4	E1 D3 S5	E1 D3 S6	E1 D3 S7
E1 D3 S8	E1 D3 S9	E1 D3 S10	E1 D3 S11
E1 D4 S0	E1 D4 S1	E1 D4 S2	E1 D4 S3
E1 D4 S4	E1 D4 S5	E1 D4 S6	E1 D4 S7
E1 D4 S8	E1 D4 S9	E1 D4 S10	E1 D4 S11

19 disks for NVR instance 4

19 disks for NVR instance 5

19 disks for NVR instance 6

3 Hot Spare disks

Storage Array Expansion

E2 D0 S0	E2 D0 S1	E2 D0 S2	E2 D0 S3
E2 D0 S4	E2 D0 S5	E2 D0 S6	E2 D0 S7
E2 D0 S8	E2 D0 S9	E2 D0 S10	E2 D0 S11
E2 D1 S0	E2 D1 S1	E2 D1 S2	E2 D1 S3
E2 D1 S4	E2 D1 S5	E2 D1 S6	E2 D1 S7
E2 D1 S8	E2 D1 S9	E2 D1 S10	E2 D1 S11
E2 D2 S0	E2 D2 S1	E2 D2 S2	E2 D2 S3
E2 D2 S4	E2 D2 S5	E2 D2 S6	E2 D2 S7
E2 D2 S8	E2 D2 S9	E2 D2 S10	E2 D2 S11
E2 D3 S0	E2 D3 S1	E2 D3 S2	E2 D3 S3
E2 D3 S4	E2 D3 S5	E2 D3 S6	E2 D3 S7
E2 D3 S8	E2 D3 S9	E2 D3 S10	E2 D3 S11
E2 D4 S0	E2 D4 S1	E2 D4 S2	E2 D4 S3
E2 D4 S4	E2 D4 S5	E2 D4 S6	E2 D4 S7
E2 D4 S8	E2 D4 S9	E2 D4 S10	E2 D4 S11

19 disks for NVR instance 7

19 disks for NVR instance 8

19 disks for NVR instance 9

3 Hot Spare disks

Figure 11: 1.5PB - 600 streams - 3000Mbps variant logical configuration

