IndigoVision

Control Center

Installation Guide

IndigoVision®
a Motorola Solutions Company

This manual was created on Wednesday, November 22, 2023.

Document ID: IU-SMS-MAN001-60

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

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

Table of Contents

1 ABOUT THIS GUIDE

This guide provides an overview of all components of IndigoVision Control Center and how to install them.

Control Center is a powerful and easy-to-use software solution that enables you to manage all your video surveillance operations and investigate security events quickly and effectively in one integrated platform.

The Control Center suite consists of a number of applications that provide a complete end-to-end IP security solution.

IndigoVision documentation

This document must be read in conjunction with the Control Center online help.

IndigoVision product documentation, including hardware guides and configuration guides, is available to authorized partners via the IndigoVision website.

► For a list of the new features for each Control Center release, please refer to the Release Note available from the IndigoVision website

Safety notices

This guide uses the following formats for safety notices:

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

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

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

💡 *Additional information relating to the current section.*

2 CONTROL CENTER SUITE OVERVIEW

The Control Center suite is made up of multiple products which work together to provide a complete end-to-end IP security solution.

All Control Center suite installations have the following core products:

- **Control Center front-end application**

  This is the user interface for the Control Center suite. It is used for configuring and managing Control Center installations, viewing live video, managing recorded video and handling alarms.

- **Site Database Server**

  The Control Center site database comprises configuration data stored in the Site Database Server and files stored in the Site Database Files directory. The Site Database Files directory is created as part of Site Database Server installation.

  The Site Database Server also provides secure authentication of Control Center operators and administrators.

- **NVR-AS**

  The Network Video Recorder / Alarm Server (NVR-AS) is server software which combines video recording and playback with advanced alarm management capabilities.

  It is available in a range of hardware appliances or as Windows software that can be installed on a third party server.

- **License Server**

  This stores the Control Center license and allows NVR-AS and the Control Center front-end application to operate.

To extend the capabilities of a core Control Center suite installation, you can use the following products:

- **Video Stream Manager**

  The Video Stream Manager (VSM) enables cameras from a range of other manufacturers to be seamlessly integrated with the Control Center suite by using the industry standard RTSP protocol or ONVIF standard.

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

- **Camera Gateway**

  Camera Gateway enables third party cameras from a range of manufacturers to be seamlessly integrated with the Control Center suite using their native protocols.

- **Control Center Client**

  Control Center Client is an alternative front end application to Control Center.

  It gives you the same capabilities as Control Center, however it does not allow you to access the site database edit mode.

- **Incident Player**

Incident Player allows video clips exported as incidents from the Control Center front-end application to be played outside of a Control Center installation. It provides all the video review functionality available within the Control Center front-end application.

- **FrontLine Manager**

  FrontLine Manager enables audio and video from FrontLine body worn cameras to be seamlessly integrated with the Control Center suite.

Recommended Architecture

Control Center can be used for security management in a wide range of situations. The following architectures serve as a starting point for your system design.

Recommended architecture for a single site

Many Control Center installations are located at a single physical location, or site.

For single-site installations, IndigoVision recommends the architecture shown in Figure 1:

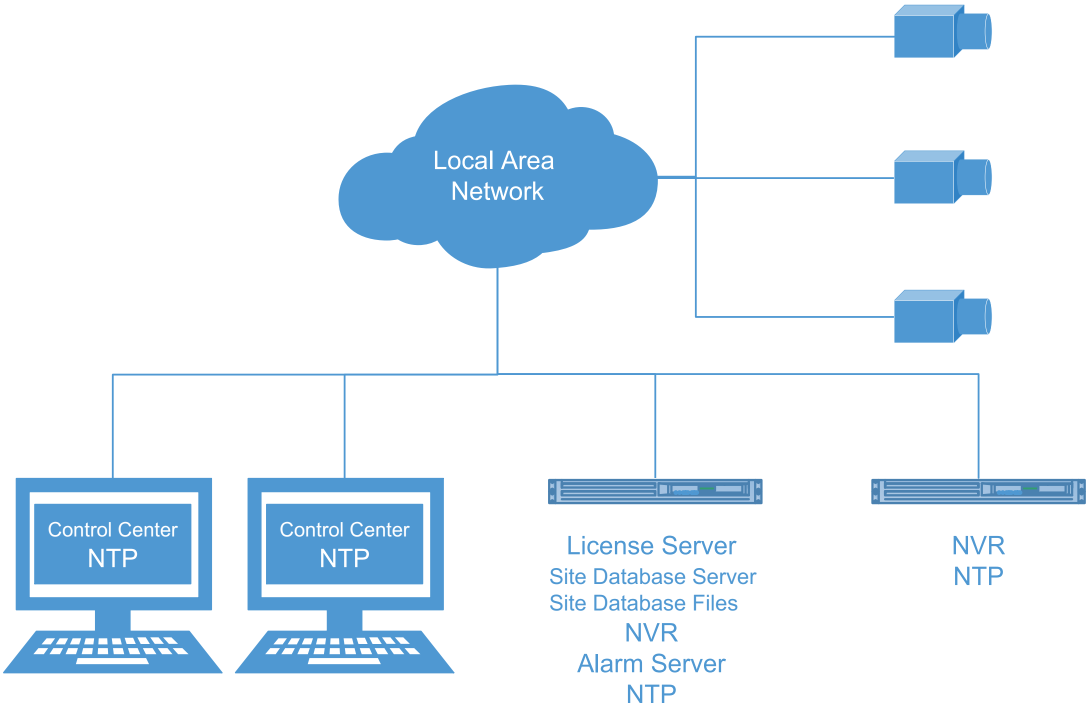

Figure 1: Recommended single site architecture

For this type of installation, IndigoVision recommends running the License Server, Windows NVR-AS and Site Database Server, and hosting the Site Database Files as a Windows file share, together on a suitable server. An IndigoVision NVR-AS 4000 is an ideal choice in this case.

All Control Center workstations should be configured to use this License Server, Site Database Server and Site Database Files location. All NVRs should be configured to use this License Server.

All Control Center and NVR-AS workstations must be time synchronised for correct operation and evidential integrity. The recommended way to achieve this is to have one NVR workstation as the primary NTP time server with all other Control Center and NVR-AS workstations running an NTP client pointed at the primary NTP time server.

All cameras in the site should use their primary NVR as their NTP time source.

Recommended architecture for multiple sites

Control Center can be used to manage sites which span multiple geographic locations.

For Control Center installations comprising multiple sites at separate geographic locations, you can extend single site architecture as shown in Figure 1:

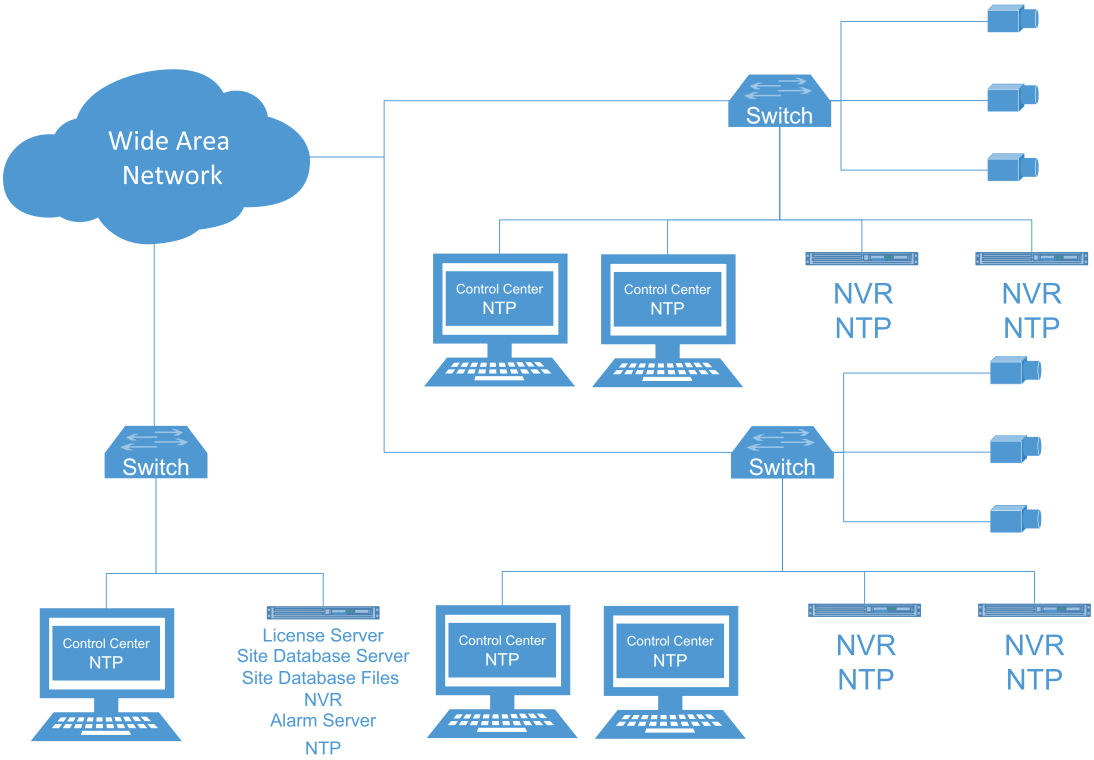

Figure 2: Recommended multiple site architecture

For this type of installation, IndigoVision continues to recommend a single server hosting the License Server, Site Database Server and Site Database Files.

In the event of Wide Area Network failure, Control Center's unique Distributed Network Architecture (DNA) allows you to record and operate locally at each site.

Licensing Overview

To operate the Control Center suite, you must have a Control Center license. A Control Center license covers the number of cameras, encoders and NVR-AS that can be used and the level of software functionality allowed.

The Control Center license is stored on a License Server and contains the following information:

- **Software tier**
  This defines the level of software functionality and the maximum number of device connection licenses allowed.
- **Number of device connections**
  This defines the number of cameras or encoders which can be connected to the Control Center.
  When a camera or encoder is connected to Control Center, you can do the following:

  - View live video
  - Play back video
  - Trigger alarms
  - Record video on an unlimited number of NVR-AS servers

  You can change the NVR-AS server on which video from a camera or encoder is recorded without needing the license to be altered.

- **Number of third party Windows NVR-AS connections**

  This defines the number of Windows servers which can run the IndigoVision NVR-AS software.

  A third party Windows NVR-AS connection license allows a single Windows server to run an instance of IndigoVision NVR-AS software.

  - An NVR-AS running on a third party server without a third party Windows NVR-AS connection license cannot record video from a camera or encoder or manage alarms.
  - IndigoVision NVR-AS 4000 appliances do not require any additional license.

Workstations running the Control Center front-end application and servers running NVR-AS must be connected to the License Server to operate.

The Control Center front-end application and NVR-AS maintain a 30-day rolling backup of their license.

- If connectivity to the License Server is lost, for example due to routine maintenance, then this backup is automatically used, and the Control Center front-end application and NVR-AS continue to operate for 30 days.
- Once connectivity to the License Server is restored, the Control Center front-end application and NVR-AS revert to using the License Server.

Trialling Control Center

The first time the License Server is installed, it allows you to use a time-limited trial license. This allows you to evaluate the Control Center suite.

You can upgrade a trial installation of Control Center by purchasing a full license.

Notice *If you apply an IndigoLite or IndigoPro full license some features which you evaluated during the trial may no longer work and may require reconfiguration.*

Installation Order

► For more information about upgrading an existing Control Center installation, *see "Upgrading from Control Center 17.0 to a later version" on page 88*

To set up a new Control Center site, install the Control Center suite products in the following order:

1. License Server
2. Site Database Server
3. NVR-AS
4. Control Center front-end application

To run a trial installation, no further steps are required.

To run a full installation, you must obtain a license.

► For information about obtaining a license, *see "License management" on page 17*.

3 LICENSE SERVER INSTALLATION

This section details how to install a License Server.

Standalone Licence Server

System requirements

You can install the License Server on one of the following Windows operating systems:

- Windows Server 2022
- Windows Server 2019 (recommended)
- Windows Server 2016
- Windows 11
- Windows 10 64-bit

IndigoVision recommends that you install the License Server on a server-style system, with a server network adaptor, and the following minimum requirements:

- Server class PC
- 4 GB of RAM

The License Server is compatible with common virtualisation software, including VMWare ESXi and Microsoft Hyper-V.

Notice *The License Server is a critical component of the IndigoVision Control Center suite. It is recommended that it is installed on a robust and highly available server.*

Installation

The License Server must be installed and running with a valid license before installing the Site Database Server, Control Center or the NVR-AS software. If this is not the case you will be unable to install any of these products.

Notice *Do not install the License Server on a PC on which IndigoVision integration modules are already installed.*

The License Server can be installed on a PC that is also running the Control Center and/or the NVR-AS software, however this is only recommended for smaller sites.

1. To install the Licence Server, do one of the following:
   - Insert the IndigoVision Control Center CD-ROM.
   - Download the CD image from the support section of the IndigoVision website.

   If the IndigoVision Control Center install screen does not open, do as follows:

   a. Open Windows Explorer.

   b. Navigate to the downloaded image, or CD-ROM drive.

   c. Double-click the ***Installer.exe*** file.
2. Click ***Install*** for the License Server component.
3. Click ***Next***.

   The **End-User License Agreement** dialog opens.
4. Read the agreement, select the check box to accept the agreement, and click ***Next***.

   The **Custom Setup** dialog opens.
5. Select how you want to install features, and click ***Next***.

   The **Ready to Install** dialog opens.
6. Click ***Install***.

   The License Server installation begins.
7. Click ***Finish***.

   The installation is complete.

After the installation process has been completed, the License Server runs as a service. To stop and start the service, use the Windows Service control panel.

License management

The IndigoVision License 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.

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 License Server.

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

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.

4 SITE DATABASE SERVER INSTALLATION

This section details how to install the Site Database Server.

Site database overview

The Control Center site database stores the site configuration information. Control Center is configured to connect to a Site Database Server during installation. You can re-configure Control Center to use a different Site Database Server at any time by using the Control Center Setup tool.

To open the Control Center Setup tool outside of the installation process, from the Start menu select ***Programs > IndigoVision > Control Center Setup***.

There are two components to a Control Center site database:

- The **Site Database Server** which hosts configuration information for users and cameras. This is provided as a network service.
- The **Site Database Files** which hosts additional media files such as maps and audio messages. This is provided as a Windows file share.

It is recommended to host the Site Database Files on the same PC as the Site Database Server.

Segmented site database

A segmented Control Center site database stores information for each site directly under the top site in separate segments of the database. Site wide information, such as user accounts, apply to all segments.

Operators and administrators can view and manage individual segments, or choose to view all segments for an overview of the whole site. Full administrators can grant users access to individual segments.

You should use a segmented site database in the following scenarios:

- Large sites with many devices.

  Sites with many thousands of cameras and alarms will benefit from a segmented site database with improved performance and easier management of devices.
- Multiple administrators.

  For installations where areas are managed independently by different administrators, a segmented site database enables the site to be organized into independent segments.
- Multiple facilities requiring central oversight.

  When monitoring multiple remote facilities, a segmented site database enables each facility to operate independently while providing central oversight.

To create a segmented site database, first create a normal site database then add segments after initial installation and configuration. For more information refer to the Site Database Server Administrator Guide.

Choosing the location of the site database

There are two ways to use the site database:

- **Local** - the Site Database Server, Site Database Files and Control Center front-end application are all installed on the same PC and the Site Database Files directory is not shared on the network. If you have installed the Control Center front-end application on only one PC you should use a local site database.
- **Central** - the Site Database Server and Site Database Files are installed on a central Windows server accessible to all Control Center workstations. If you have installed the Control Center front-end application on several PCs you should use a central site database.

When you use a central site database, the Site Database Server and Site Database Files can be stored in one of the following locations:

- a PC where the Control Center front-end application is installed
- an NVR-AS 4000 Windows Appliance
- a Windows server

Notice *Ensure that the folder you select for the Site Database Files is accessible by all PCs running the Control Center front-end application.*

Central site database network data encryption

Server Message Block (SMB) is the protocol used for communication between a client and the Site Database Files Windows file share. When you use a central site database, consider enabling SMB encryption on the central Site Database Files. Enabling SMB encryption avoids potential eavesdropping of information on the network between Control Center and the file share.

SMB encryption requires that the file server and client machines are configured with domain authentication.

SMB encryption can be configured on the following operating systems:

- Windows 10
- Windows 11
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

Ensure that the latest Windows updates have been applied on all the clients and server machines.

To configure the SMB encryption on the shared site database, follow this procedure:

1. Open a Windows PowerShell, as an administrator, on the system hosting the shared site database.
2. Type the following command:

```
Set-SmbShare -Name <SharedSiteDbFilesName> -EncryptData 1
```

3. Restart the server.

System requirements

Notice *To install IndigoVision Site Database Server, you must have a License Server installed and available, with a valid Control Center license.*

► For more information, see the "IndigoVision Control Center Installation Guide"

You can install the Site Database Server on any of the following operating systems:

- Windows Server 2022
- Windows Server 2019 (recommended)
- Windows Server 2016
- Windows Server 11
- Windows Server 10 64-bit v1607 and later

Ensure that the Universal C Runtime is installed on the Site Database Server PC.

- For Windows 10 and Windows Server 2016 or later, the Universal C Runtime is shipped automatically.
- For earlier operating systems, the Universal C Runtime is distributed through Windows Update.

IndigoVision recommends that you install the Site Database Server on a server-style system, with a server network adaptor, and the following minimum requirements:

- Server class PC
- 4 GB RAM

The Site Database Server is compatible with common virtualization software, including VMWare ESXi and Microsoft Hyper-V.

Notice *The Site Database Server is a critical component of the IndigoVision Control Center suite. It is recommended that it is installed on a robust and highly available server.*

⚠ **Warning** *To get full performance from a multi-processor PC, disable the Non-Uniform Memory Access (NUMA). Leaving NUMA enabled can cause performance problems when writing to the Site Database Server.*

The NUMA option can be disabled in the BIOS settings. If this option does not appear in the BIOS settings, it is disabled by default. When NUMA is disabled, the memory is configured into a single block that is interleaved between the available processors instead of allocated in blocks for each processor.

The Site Database Server can be installed alongside other IndigoVision server software, including the Windows NVR-AS and License Server.

Install the Site Database Server

The Site Database Server must be installed and running before installing Control Center. If this is not the case, you will be unable to start Control Center. The Site Database Server Setup tool will take you through configuring the Control Center site database. It can be run later from the Start Menu to change the configuration.

To install the Site Database Server, follow these steps:

Notice *Your operating system may require you to authorize this installation.*

1. Perform one of the following operations:
   - Insert the IndigoVision Control Center CD-ROM.
   - Download the CD image from the support section of the IndigoVision website.
2. If the IndigoVision Control Center install screen does not open automatically, open Windows Explorer and navigate to the downloaded image or CD-ROM drive, and double-click the ***Installer.exe*** file.
3. Click ***Install*** for the Site Database Server component.
4. Read the **End-User License Agreement**, select the box to accept the agreement, and click ***Next***.

   The Site Database Server installation begins.

Notice *You must complete the steps in the Site Database Server Setup tool before Control Center workstations can be configured to use the site database.*

5. In the Site Database Server Setup tool, you have the following options to set up a site database:
   - ***Use an existing site database***

     Use this option if you have already created a Control Center 17 or later site database which you want to use. This option will also allow you to modify the site database, by changing the License Server address for example.

     ► For more information, *see "Modify or use an existing site database" on page 24*
   - ***Create a new site database***

     Use this option if this is the first time you have installed the Site Database Server and do not have an existing Control Center 16 system to upgrade from.

     ► For more information, *see "Create a new site database" on page 23*
   - ***Upgrade from a Control Center 16 site database***

     Use this option if you are upgrading from Control Center 16 and wish to create a Control Center 17 compatible site database from your Control Center 16 site database.

     ► For more information, *see "Upgrading from Control Center 16 to a later version" on page 89*

Notice *You cannot directly upgrade from versions of Control Center prior to Control Center 16.*

- ► For more information on migrating from Control Center 15 or earlier, *see "Upgrade from Control Center 15 or earlier" on page 89*

- ***Configure as a failover Site Database Server***
  - ► For more information on configuring a failover Site Database Server, *see "Failover Site Database" on page 26*

6. After the Site Database Server Setup tool is closed, click ***Finish*** on the Installer to complete the installation process.

Create a new site database

Use the Site Database Server Setup tool to create a new site database if this is a new installation of Control Center. Site Database Server Setup is run automatically during installation, or it can be started later from the Windows Start menu.

1. In the Site Database Server Setup tool, click ***Next*** to proceed to the **Site Database Configuration** page.
2. Select ***Create a new site database*** and click ***Next***.
3. On the **New Site Database** page, perform the following operations:
   a. Provide a location for the Site Database Files directory. This will be shared as a Windows file share with all Control Center workstations. This could be an empty directory in an existing file share hosted on a different PC.
   b. Provide a location on the local PC for storing the database hosted by the Site Database Server.
   c. Click ***Next***.
4. Enter the IP address of the License Server, then click ***Next***.
5. Select the default site database access permissions for non-administrator users:
   - **None** (recommended) - users are not able to access any database objects by default. An administrator must grant each user permissions to the objects they need to access.
   - **All** - users are able to access all database objects by default, unless explicitly denied permissions.
6. Click ***Next***.

   The Control Center Administrator page opens.
7. Create the initial Control Center administrator account:
   a. Specify a username.
   b. Select either a Windows account or password for authentication.
   c. Click ***Next***.
8. If you have chosen an insecure password, the **Password Strength Warning** will be displayed. Perform one of the following actions:
   - Click ***Yes*** to continue with an insecure password.
   - Click ***No*** to return and change the password.
9. On the ***Site Database Server Administrator*** page, enter a username and password for the authenticating with the database service, then click ***Next***.

Notice *These credentials will be required to configure a failover Site Database Server or recover from a backup in the future.*

10. If you have chosen an insecure password, the **Password Strength Warning** will be displayed. Perform one of the following actions:

- Click ***Yes*** to continue with an insecure password.
- Click ***No*** to return and change the password.

11. On the **Network Binding** page, do the following:
    a. Choose the IP address and port on the local PC that the Site Database Server will bind to. The IP and port selected here must be accessible to all Control Center workstations in the system.
    b. Choose the IP address on the local PC that will be used for replication. The IP selected here must be accessible to the failover Site Database Server.
12. Click ***Next***.
13. On the **Server Certificate** page, choose a TLS certificate for Site Database Server, then click ***Next***.

    The Site Database Server requires a certificate for secure communication with Control Center. If you do not have a valid certificate signed by a trusted Certificate Authority (CA) for this PC, you can select ***Generate a self-signed certificate***.

⚠ **Caution**

IndigoVision recommend that self-signed certificates are only used for initial demonstration and test purposes. Correctly secured systems must use certificates from a trusted CA.

► For more information on security, refer to the "Control Center Security Hardening Guide"

14. If you have chosen to create a self-signed certificate, or if the chosen certificate is otherwise untrusted by Windows, the **Certificate Security Warning** appears. Perform one of the following actions:
    - Check to confirm you have read and understood the warning and click ***Next*** to proceed.
    - Click ***Back*** to choose a different certificate.
15. On the **Camera HTTPS Configuration** page, select if support for HTTPS for communication with cameras is to be enabled for the database, then click ***Next***.

    ► For more information on HTTPS, *see "HTTPS technical notes" on page 103*
16. After the configuration is completed, click ***Finish*** to close the Site Database Server Setup tool.

Modify or use an existing site database

If you have previously created a Control Center 17 or later site database, use the existing database when installing Control Center. The Site Database Server Setup tool will allow you to edit the existing configuration, such as the License Server IP address, at the same time.

1. In the Site Database Server Setup tool, click ***Next*** to proceed to the **Site Database Configuration** page.
2. Select ***Use an existing site database*** and click ***Next***.
3. On the **Site Database Location** page, provide the location on the local PC where the existing Site Database Server database is stored. This is separate from the Site Database Files directory.
4. Click ***Next*** to continue to the License Server page.

   Optionally, change the License Server IP address, and click ***Next*** to continue.
5. On the **Network Binding** page, do the following:

   a. Choose the IP address and port on the local PC that the Site Database Server will bind to. The IP and port selected here must be accessible to all Control Center workstations in the system.
   b. Choose the IP address on the local PC that will be used for replication. The IP selected here must be accessible to the failover Site Database Server.
6. On the **Server Certificate** page, optionally change the TLS certificate for Site Database Server, then click ***Next***.
7. If you have chosen to create a self-signed certificate, or if the chosen certificate is otherwise untrusted by Windows, the **Certificate Security Warning** will display. Perform one of the following actions:
   - Check to confirm you have read and understood the warning and click ***Next*** to proceed.
   - Click ***Back*** to choose a different certificate.
8. After the configuration is completed, click ***Finish*** to close the Site Database Server tool.

Upgrade from a Control Center 16 site database

If you are upgrading from Control Center 16, use the Control Center Setup tool to automatically migrate your old site database.

1. In Control Center Setup tool, click ***Next*** to proceed to the **Site Database Configuration** page.
2. Select ***Upgrade from a Control Center 16 site database*** and click ***Next***.
3. Read introduction to the upgrade process and then click ***Next***.
4. On the ***New Site Database*** page, perform the following operations:
   a. Provide a location for the existing Control Center 16 site database. This will become the Site Database Files location for the upgraded system.
   b. Provide a location on the local PC for storing the database hosted by the Control Center.
5. Click ***Next*** to continue.
6. Enter the IP address of the License Server, then click ***Next***.
7. On the ***Site Database Server Administrator*** page, enter a username and password for the authenticating with the database service, then click ***Next***.

Notice *These credentials will be required to export or recover the database the in the future. Store these credentials for future use.*

8. If you have chosen an insecure password, the **Password Strength Warning** will display. Perform one of the following actions:
   - Click ***Yes*** to continue with an insecure password.
   - Click ***No*** to return and change the password.
9. On the **Network Binding** page, do the following:
   a. Choose the IP address and port on the local PC that the Site Database Server will bind to. The IP and port selected here must be accessible to all Control Center workstations in the system.
   b. Choose the IP address on the local PC that will be used for replication. The IP selected here must be accessible to the failover Site Database Server.

10. On the **Server Certificate** page, choose a TLS certificate for Control Center, then click ***Next***.

    The Control Center requires a certificate for secure communication with Control Center. If you do not have a valid certificate signed by a trusted Certificate Authority (CA) for this PC, you can select ***Generate a self-signed certificate***.

⚠ **Caution** *IndigoVision recommend that self-signed certificates are only used for initial demonstration and test purposes. Correctly secured systems must use certificates from a trusted CA.*

- ► For more information on security, refer to the "Control Center Security Hardening Guide"
- ► For more information on creating certificates for the Control Center, refer to the "Site Database Server Administration Guide".
- ► For more information on changing certificates for the Control Center, refer to the "Site Database Server Administration Guide".

11. If you have chosen to create a self-signed certificate, or if the chosen certificate is otherwise untrusted by Windows, the **Certificate Security Warning** will display. Perform one of the following actions:
    - Check to confirm you have read and understood the warning and click ***Next*** to proceed.
    - Click ***Back*** to choose a different certificate.
12. After the configuration is completed, click ***Finish*** to close the Control Center Setup tool.

Failover Site Database

A failover Control Center site database consists of a failover Site Database Server and a failover Site Database Files directory. If the primary Site Database Server or primary Site Database Files directory is unavailable when an operator or administrator attempts to log into the Control Center front-end application, they will be able to use the failover site database instead. This ensures that there is no interruption of service and makes the system more robust in the face of hardware failures.

Notice *When logged into a failover Site Database Server, administrators are prevented from making changes to the site configuration, such as adding or removing cameras.*

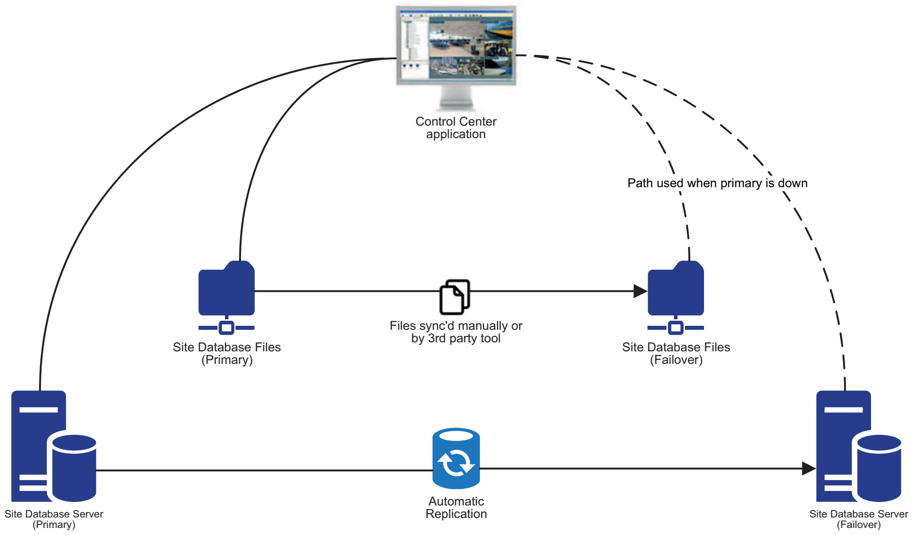
Control Center application
Path used when primary is down
Site Database Files (Primary)
Files sync'd manually or by 3rd party tool
Site Database Files (Failover)
Site Database Server (Primary)
Automatic Replication
Site Database Server (Failover)

Figure 3: Network configuration with the failover Site Database Server

The failover Site Database Server is configured to automatically synchronize all of the configuration information directly from the primary Site Database Server. There must be a persistent network route between the two Site Database Servers in order to achieve this.

The failover Site Database Files directory is expected to be a copy of the primary Site Database Files. There are many tools that can be used to ensure that changes made to the primary Site Database Files directory are synchronized regularly to the failover directory. IndigoVision does not provide automatic tooling to accomplish this.

Configuring a failover Site Database Server

Notice *There can only be one failover Site Database Server for each Control Center system. If you configure a second failover Site Database Server, the first failover is removed from the primary and will stop synchronization.*

To configure a failover Site Database Server, follow these steps:

1. Ensure the Site Database Server is already installed and configured on a separate PC or virtual machine. This is the primary Site Database Server.
   - For more information, *see "Site Database Server installation" on page 19*
2. Ensure that there is no firewall blocking access to the MongoDB service on the primary server.
   - For more information, see "Firewall" in IndigoVision Site Database Server Administrator Guide".
3. On the PC that will host the failover Site Database Server (this must be separate from the primary server), do the following:
   a. Insert the IndigoVision Control Center CD-ROM or download the CD image from the support section of the IndigoVision website.
   b. If the IndigoVision Control Center install screen does not open automatically, open Windows Explorer and navigate to the downloaded image or CD-ROM drive, and double-click the ***Installer.exe*** file.
   c. Click ***Install*** for the Site Database Server component.
   d. Read the **End-User License Agreement**, select the box to accept the agreement, and click ***Next***.

The Site Database Server installation begins.

e. In the Site Database Server Setup tool, choose to ***Configure as a failover Site Database Server***, and click ***Next***.
f. Read the overview page and click ***Next***.
g. On the primary ***Site Database Server connection*** page, enter the address, username, and password for the primary Site Database Server.

   The primary address can be the IPv4 address or a resolvable hostname, or fully qualified domain name.

Notice *To avoid reconfiguring the failover if the IP address of the primary changes, consider using a fully qualified domain name for the primary.*

h. Click ***Next*** and the connection is tested.

   If there is a problem connecting to the primary Site Database Server, the **Site Database Server connection** is shown again. Check that the details entered are correct and that the primary Site Database Server is available.
i. On the ***New failover Site Database Location*** page, enter the location on this PC where the site database server will store the data synchronized from the primary.
j. On the **Network Binding** page, do the following:

- Choose the IP address and port on the local PC that the Site Database Server will bind to. The IP and Port selected here must be accessible to all Control Center workstations in the system.
- Choose the IP address on the local PC that will be used for replication. The IP selected here must be accessible to the primary Site Database Server.

k. On the **Server Certificate** page, specify the TLS certificate for Site Database Server, then click ***Next***.

► For more information on creating certificates for the Site Database Server, see "Request a new certificate from a third party Certificate Authority (CA)" in IndigoVision Site Database Server Administrator Guide".

► For more information on changing certificates for the Site Database Server, see "Replace the certificate used by the Site Database Server" in IndigoVision Site Database Server Administrator Guide".

l. If you have chosen to create a self-signed certificate, or if the chosen certificate is otherwise untrusted by Windows, the **Certificate Security Warning** will display. Check to confirm you have read and understood the warning and click ***Next*** to proceed, or click ***Back*** to choose a different certificate.
m. After the configuration is completed, click ***Finish*** to close the Site Database Server tool.

Notice *There can only be one failover Site Database Server for each Control Center system.*

5 NVR-AS INSTALLATION

This chapter details how to install the Windows Network Video Recorder/Alarm Server (NVR-AS).

System specifications

IndigoVision recommends that you install your NVR-AS on a server-style system, with a server network adaptor and server disk systems.

Notice *To install IndigoVision Windows NVR-AS, you must have a License Server installed and available, with a valid Control Center license.*

For more information, see "Installation" on page 16.

⚠ **Caution** *IndigoVision strongly recommends the use of disk redundancy technology such as RAID to provide a single large partition to the NVR-AS.*

► For more information about requirements for Windows NVR-AS, please refer to the *Windows NVR Specification Guide*

NVR-AS operating system specification

We recommend that you use the following guidelines for the NVR- AS PC or server operating system.

Table 1 Supported operating systems

Operating system	Supported
Windows Server 2022	Y
Windows Server 2019	Y (recommended)
Windows Server 2016	Y
Windows 11	Y
Windows 10 64-bit	Y
Other	N

Notice IndigoVision recommends that you use Windows Server 2019 when using the Windows NVR-AS.

If your NVR-AS is to be used to record more than 16 streams of video or process alarms from more than 100 devices, we recommend using Windows Server 2022, Windows Server 2019 or Windows Server 2016.

Anti-virus software

It is possible to run anti-virus software on the same machine as the IndigoVision Windows NVR-AS. However, IndigoVision recommends that the VideoLibrary directory (containing .vmf recording files) should not be automatically checked while recordings are being made as this could disrupt disk performance, possibly resulting in recordings with lost frames. Scheduling of automatic scans should also be carefully planned with regard to a possible overload of the server CPU. If the virus checker overloads the CPU then the NVR-AS may again lose frames from recordings.

Step 1: Prepare your video library

During installation you are asked for a path to the Video Library. This is the folder where the video files are stored.

⚠ Caution

*The NVR-AS Video Library should **always** be on a separate drive from the NVR-AS configuration data directory, and the NVR-AS configuration directory should always be on a local hard disk.*

Recording onto a local drive

If you plan to store your recordings on a local drive, these should be stored on a partition with as much disk space as possible, and preferably not on the system partition.

⚠ Caution

IndigoVision strongly recommends the use of disk redundancy technology such as RAID to provide a single large partition to the NVR-AS.

Recording onto a network drive

If you plan to store NVR-AS recordings on a network drive, you must first select a temporary location on a local disk. After installation, use the NVR-AS Administrator program to specify a permanent location.

► For more information, *see "NVR-AS Post-Installation Network Drive Configuration" on page 85*.

Step 2: Install the NVR-AS

To install the NVR-AS:

1. Insert the Control Center CD into the CD drive of the PC or server on which you are installing the NVR-AS application. The Control Center install screen opens.

   If the install screen does not open automatically, double-click the ***Installer.exe*** file in your Windows Explorer window, or use the ***Run*** option on the Windows Start menu and enter the path to the ***Installer.exe*** file on the CD ROM.
2. Click ***Install*** for the NVR-AS component. The NVR-AS Installation wizard opens.
3. Click ***Next***. The End-User License Agreement dialog opens.
4. Read the agreement and select the check box to accept the agreement. Click ***Next***. The Custom Set-up dialog opens.
5. Select the way you want features to be installed, and click ***Next***. Then click ***Install***. The NVR-AS installation begins.

   After a period, the NVR-AS Administrator application opens.
6. Enter the server (NVR-AS) name and location as required, then click ***Next***.

   These are the name and location that are used in Control Center applications.
7. Enter the IP address of the License Server, then click ***Next***.
8. Specify the path to the video and configuration data, then click ***Next***.
9. Configure the network settings, then click ***Next***.

   If the NVR-AS is using IP based storage, such as an iSCSI SAN, it is useful to define the IP address.
10. Configure a username and password, then click ***Next***.
11. Configure the disk space management setting, then click ***Next***.
    - If you are recording at a high bit rate, you may want to set the Maximum Chunk Size at a higher value to limit the number of recordings that the NVR-AS and Control Center have to manage.

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

- Enable ***Tamper Protection on recordings*** to verify that recordings made by the NVR have not been tampered with.

  Tamper Protection has an impact on performance. Enabling this feature will increase CPU usage. Consider the capabilities of your NVR-AS server before enabling this option.

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

- Enable video thinning to reduce the storage requirements at the expense of full motion video.

12. Configure the Alarm Management settings, then click ***Next***.

Notice *When alarms are reaped, any activations that contributed to those alarms are also reaped.*

13. Configure the email settings to enable email actions, then click ***Next***.
14. Click ***Finish***. The NVR-AS service starts automatically. Click ***OK*** to confirm.
15. The IndigoVision NVR-AS Set Up wizard is displayed. Click ***Finish*** to complete the installation.

6 CONTROL CENTER FRONT-END APPLICATION INSTALLATION

This chapter describes how to install the Control Center front-end application and Incident Player application. It also explains how to configure a Windows firewall to allow correct operation of the Control Center front-end application with an NVR-AS and Site Database Server.

Notice *To install the IndigoVision Control Center front-end application, you must have a License Server installed and available, with a valid Control Center license, and a Site Database Server installed and available on the network.*

For more information, see "Installation" on page 16.

► For information about specifying a system for Control Center, refer to the *"Control Center Performance Guide"*

Control Center operating system specification

We recommend that you use the following guidelines for the Control Center PC operating system.

Table 2 Supported Operating Systems

Operating System	Supported
Windows 11	Y
Windows 10 64-bit v1607 and later	Y (recommended)
Other	N

Ensure that the Universal C Runtime is installed on all Control Center application PCs.

- For Windows 10, the Universal C Runtime is shipped automatically.
- For earlier operating systems, the Universal C Runtime is distributed through Windows Update.

Audit logging

The Control Center provides an audit logging function that logs many common user and administrator actions in an ODBC compliant database, for example, Microsoft SQL Server.

You can configure audit log settings once you have logged into the Control Center front-end application. You must be logged in as an administrator to change the audit log settings.

Notice *Audit logging is required to use the Spot Monitor Export function.*

► For information about setting up audit logging, refer to the *Audit Log Reference Guide*

Installation procedure

This section describes the installation procedures for the Control Center front- end application and Incident Player.

An alternative variant that does not include site setup functionality, the Control Center Client front-end application, is also available. Use this variant for installations that should only use the site database provided by an administrator.

► For more information, *see "Control Center Client front-end application installation" on page 41*

Control Center front-end application

You must be logged into Windows as an administrator to install the Control Center front-end application.

Notice *Your Operating System may require you to authorize this installation.*

1. Perform one of the following operations:
   - Insert the IndigoVision Control Center CD-ROM.
   - Download the CD image from the support section of the IndigoVision website.
2. If the IndigoVision Control Center install screen does not open automatically, open Windows Explorer and navigate to the downloaded image or CD-ROM drive, and double-click the ***Installer.exe*** file.
3. Click ***Install*** for the Control Center front-end application, and follow the on-screen instructions to complete the installation.
4. Click ***Next***, and the ***Site Database*** page appears.
5. Enter the details for the Site Database Server and Site Database Files location and click ***Next***.

   Note: *The Site Database Server and Site Database Files directory must be available on the network to continue with the Control Center installation.*

   Note: *Consider using a resolvable hostname or fully qualified domain name for the Site Database Server rather than an IPv4 address. This will prevent additional configuration if the Site Database Server IP address changes.*

   The ***Testing Connection*** page appears and automatically connects to the Site Database Server.

- If the Site Database Server is available but the server's certificate is not trusted by this workstation:
  a. Click ***View Certificate*** to view the server certificate and check if it matches the expected server certificate configured when installing the Site Database Server. Then click ***OK*** to close the ***Certificate*** dialog.

If the certificate does not match the certificate configured on the Site Database Server. Check that you are connecting to the correct address and consider if the network could be compromised.

b. To enable Control Center to trust the Site Database Server, click ***Install Certificate*** on the ***Testing Connection*** page. This will install the certificate and retest the connection.

c. Click ***Next*** once the connection is trusted.

- If the Site Database Server cannot be contacted, check if the Site Database Server is available over the network and click ***Retry Connection*** to try again.
- If the Site Database Server is available and the server's certificate is trusted by this workstation:

a. Click ***View Certificate*** to view the server certificate and check if it matches the expected server certificate configured when installing the Site Database Server.

b. Click ***Next***.

The ***Failover Site Database*** page is displayed.

6. If a failover Site Database has been configured:

a. Click ***Specify a failover site database***.

b. Enter the details of the failover Site Database Server and Site Database Files directories.

c. Click ***Next***.

The ***Testing Failover Connection*** page is displayed.

Note: The certificate for the primary should be checked and, if necessary, installed.

7. After configuring the failover site database, or if no failover was specified, click ***Next***.
8. Click ***Finish***.

Incident Player

The Incident Player application can be used to view incidents you have exported using the Control Center front-end application.

1. Insert the Control Center CD into the CD drive of the PC on which you are installing Incident Player. The Control Center install screen opens.

   If the install screen does not open automatically, double-click the ***Installer.exe*** file in your Windows Explorer window, or use the ***Run*** option on the Windows Start menu and enter the path to the ***Installer.exe*** file on the CD ROM.
2. Click ***Install*** for the Incident Player component, and follow the on-screen instructions to complete the installation.

Configure Implicit Windows Authentication

Control Center supports login for both user credentials and Windows authentication.

If you are using Windows authentication, when selecting ***Login with Windows*** in the Control Center login page, you are prompted for your credentials.

It is possible to skip typing credentials and rely on **Windows Security** to securely login with one click.

To configure Implicit Windows Authentication, do as follows:

1. Use the workstation where the Control Center front-end application is installed and open the Control Panel.
2. Select ***Network and Internet > Internet Options***.
3. Select ***Security > Local Intranet > Sites > Advanced***.
4. Add the Site Database Server IP or hostname, for example, https://SDSaddress
5. Click ***Add***.
6. Click ***Close***.
7. Click ***OK***.
8. In the Security tab, select **Custom Level**.
9. Under ***User Authentication > Logon***, enable ***Automatic logon only in Intranet zone***.
10. Click ***OK*** twice.
11. Close the Control Panel.

You can now login to Control Center using your Windows user account details by clicking ***Login with Windows*** in the Control Center Login page.

If multiple workstations are joined to an Active Directory domain, and implicit Windows authentication is required for all of them, configure the workstations by Group Policy as follows:

1. On the domain controller, open the appropriate Group Policy Object in the ***Group Policy Management Editor***.

Notice *For the appropriate Group Policy Object, refer to the relevant Microsoft documentation.*

2. Select ***Computer Configuration > Policies > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page***.
3. Double-click on ***Site to Zone Assignment List***.
4. Select ***Enabled***.
5. Select ***Show***.
6. In ***Value name***, enter the site database server IP or hostname, for example, `https://SDSaddress`.
7. In ***Value***, enter `1` for the local intranet zone.
8. Select ***OK*** twice.
9. Select ***Security Page > Intranet Zone***.
10. Double-click on ***Logon options***.
11. Select ***Enabled***.
12. In the ***Logon options*** list, select ***Automatic logon only in Intranet zone***.
13. Select ***OK***.
14. Close the Group Policy Management Editor.

You can now check that the updated Group Policy is pushed to the workstations.

Partner branding

You can customize the Control Center front-end application to include your company's name and logo. Your company logo appears on the login screen, and company name appears in the title bar of the Control Center front-end application.

IndigoVision provides a .bmp and a .txt file for you to edit with your company details.

1. On the Control Center CD, navigate to ***Resources\Partner Branding***.

   In the ***partnertext.txt*** file, enter the text you want to appear in title bar, and save it in the folder where the Control Center front-end application is installed.
2. Edit the ***partnerlogo.bmp*** file with the image you want to appear in the login screen, and save it in the folder where the Control Center front-end application is installed.

Notice *The dimensions of the partnerlogo.bmp image must be (625 x 65 pixels), otherwise the image may not scale correctly.*

3. Open a DOS prompt and navigate to the Control Center front-end application installation directory. Enter the following at the prompt:

   ```
   ccbrand.exe
   ```
4. Open the Control Center front-end application to check the image is correctly displayed on the login dialog and the text is correctly displayed in the title bar.

Windows firewall

Firewall protection is automatically enabled. The firewall may prevent correct operation of the application and/or the NVR-AS. To ensure these applications work as expected, you can:

- turn off the firewall, or
- create firewall exceptions.

Turning off the firewall

Turning off the firewall completely leaves your computer unprotected against outside attack. IndigoVision recommends the Windows firewall is enabled on all Windows PCs. Refer to the Control Center Security hardening guide for more information on securing a Control Center system.

Creating firewall exceptions

Alternatively, you can create firewall exceptions for a Control Center front-end application and other IndigoVision applications. For more information about creating exceptions, see the Windows help system.

► IndigoVision port numbers are listed in *see "IndigoVision Firewall Requirements" on page 73*

Unattended installation

Unattended installation enables system administrators to install the front-end applications using group policies. This enables system administrators to automate installation to ensure the correct version of the Control Center front-end application or Control Center Client front-end application is available to users.

The following sections provide the information a system administrator requires to implement unattended installation within your organization's environment.

Installer properties

To perform an unattended installation of the front-end applications, you must add the installer property USEEXISTINGSITEDBSETTINGS and set the value to 1.

New Control Center Installation

The Control Center front-end application is available in a range of language packs. English is installed by default.

You can change the language by updating the LANGUAGELCID installer property to one of the values below. If the installer does not include the chosen language pack, the Control Center front-end application will not be installed.

If All Languages are installed you can change the language from the Control Center front-end application.

Language	ID
All Languages	0
Chinese	2052
Chinese (Traditional)	31748
Finnish	1035
French	1036
German	1031
Hebrew	1037
Hungarian	1038
Italian	1040
Japanese	17
Korean	18
Malay	62
Polish	1045
Portuguese	1046
Russian	1049
Slovak	27
Spanish	2058
Vietnamese	42

Upgrading Control Center

When you upgrade the Control Center front-end application, the installed language pack is also upgraded. If the installer does not include that language pack, the Control Center front-end application will not be upgraded.

Prerequisites

The installers for the front-end applications have several prerequisites for the target PC before running the front-end application installer.

The following applications and registry settings are prerequisites for the Control Center front-end applications installation.

- Control Center site database location
    - This is stored in the registry:

      64-bit Windows: `HKLM\SOFTWARE\IndigoVision\Control Center Client 4`.
- Add a string value called `SdsAddress`

  This contains the address to the Site Database Server in the form of `host:port`, for example, `192.168.1.1:8135` or `myserver:8135`
- Add a string value called `SiteDatabaseFilesPath`

  This contains the Site Database Files location, for example, ***C:\IndigoVisionSiteDBFiles***
- The following settings should be added only if Site Database Server Failover is required:
    - Add a string called `FailoverSdsAddress`

      This contains the address to the Site Database Server in the form of `host:port`, for example, `192.168.1.1:8135` or `myserver:8135`
    - Add a string called `FailoverSiteDatabaseFilesPath`

      This contains the Site Database Files location, for example, ***C:\IndigoVisionSiteDBFiles***
- Microsoft .NET Framework 4.8
    - ***ndp48-x86-x64-allos-enu.exe***
    - Available on the Control Center CD in the Control Center folder.
- Microsoft Sync Framework 2.1 core components
    - ***Synchronization-v2.1-x64-ENU.msi***
    - Available on the Control Center CD in the Control Center folder.
- Microsoft Sync Framework 2.1 provider services
    - ***ProviderServices-v2.1-x64-ENU.msi***
    - Available on the Control Center CD in the Control Center folder.
- Microsoft Universal C Runtime
    - Available from Microsoft through Windows Update.
- Site Database Server Certificate
    - If your Site Database Server is using a self signed certificate the certificate must be installed.
    - The Site Database Server certificate should be installed in the Local Machine, Trusted Root Authority store.

Examples

Examples of registry scripts are available on the Control Center CD. The scripts are an example of how to set the Site Database Server Address and the Site Database Files path in the registry to `127.0.0.1:8135` and ***C:\IndigoVisionSiteDBFiles*** respectively.

The scripts are editable in the text editor, for example, Notepad.

If you want to use some advanced settings, for example ***Failover***, you need to add the required registry settings to the registry script.

► For more on registry settings, *see "Prerequisites" on page 38*

The scripts are available in the ***Unattended Installation*** folder on the Control Center CD.

An example Microsoft Windows Installer Transform file (.mst) with the required settings is also available in the ***Unattended Installation*** folder.

7 CONTROL CENTER CLIENT FRONT-END APPLICATION INSTALLATION

This chapter describes how to install the Control Center Client front-end application. It also explains how to configure a Windows firewall to allow correct operation of Control Center Client.

Notice *To install the IndigoVision Control Center Client front-end application, you must have a License Server installed and available, with a valid Control Center license, and a Site Database Server installed and available on the network.*

For more information, see "Installation" on page 16.

For information about system specifications, see the *"Control Center Performance Guide"*.

Control Center Client front-end application operating system specification

We recommend that you use the following guidelines for the Control Center Client front-end application PC operating system.

Table 3 Supported Operating Systems

Operating System	Supported
Windows 11	Y
Windows 10 64-bit v1607 and later	Y (recommended)
Other	N

Ensure that the Universal C Runtime is installed on all Control Center application PCs.

- For Windows 10, the Universal C Runtime is shipped automatically.
- For earlier operating systems, the Universal C Runtime is distributed through Windows Update.

Installation procedure

Control Center Client is available on the Control Center CD. If you need to distribute Control Center Client, you can copy the contents of the ***ControlCenterClient*** folder on to a CD.

Control Center front-end application

You must be logged into Windows as an administrator to install the Control Center front-end application.

Notice *Your Operating System may require you to authorize this installation.*

1. Perform one of the following operations:
   - Insert the IndigoVision Control Center CD-ROM.
   - Download the CD image from the support section of the IndigoVision website.
2. If the IndigoVision Control Center install screen does not open automatically, open Windows Explorer and navigate to the downloaded image or CD-ROM drive, and double-click the ***Installer.exe*** file.
3. Click ***Install*** for the Control Center front-end application, and follow the on-screen instructions to complete the installation.
4. Click ***Next***, and the ***Site Database*** page appears.
5. Enter the details for the Site Database Server and Site Database Files location and click ***Next***.

   Note: *The Site Database Server and Site Database Files directory must be available on the network to continue with the Control Center installation.*

   Note: *Consider using a resolvable hostname or fully qualified domain name for the Site Database Server rather than an IPv4 address. This will prevent additional configuration if the Site Database Server IP address changes.*

   The ***Testing Connection*** page appears and automatically connects to the Site Database Server.

- If the Site Database Server is available but the server’s certificate is not trusted by this workstation:
  a. Click ***View Certificate*** to view the server certificate and check if it matches the expected server certificate configured when installing the Site Database Server. Then click ***OK*** to close the ***Certificate*** dialog.

If the certificate does not match the certificate configured on the Site Database Server. Check that you are connecting to the correct address and consider if the network could be compromised.

  b. To enable Control Center to trust the Site Database Server, click ***Install Certificate*** on the ***Testing Connection*** page. This will install the certificate and retest the connection.
  c. Click ***Next*** once the connection is trusted.
- If the Site Database Server cannot be contacted, check if the Site Database Server is available over the network and click ***Retry Connection*** to try again.
- If the Site Database Server is available and the server’s certificate is trusted by this workstation:
  a. Click ***View Certificate*** to view the server certificate and check if it matches the expected server certificate configured when installing the Site Database Server.
  b. Click ***Next***.

     The ***Failover Site Database*** page is displayed.

6. If a failover Site Database has been configured:
   a. Click ***Specify a failover site database***.
   b. Enter the details of the failover Site Database Server and Site Database Files directories.
   c. Click ***Next***.
      The ***Testing Failover Connection*** page is displayed.

Note: The certificate for the primary should be checked and, if necessary, installed.

7. After configuring the failover site database, or if no failover was specified, click ***Next***.
8. Click ***Finish***.

Windows firewall

Firewall protection is automatically enabled. The firewall may prevent correct operation of the application and/or the NVR-AS. To ensure these applications work as expected, you can:

- turn off the firewall, or
- create firewall exceptions.

Turning off the firewall

Turning off the firewall completely leaves your computer unprotected against outside attack. IndigoVision recommends the Windows firewall is enabled on all Windows PCs. Refer to the Control Center Security hardening guide for more information on securing a Control Center system.

Creating firewall exceptions

Alternatively, you can create firewall exceptions for a Control Center front-end application and other IndigoVision applications. For more information about creating exceptions, see the Windows help system.

► IndigoVision port numbers are listed in *see "IndigoVision Firewall Requirements" on page 73*

Unattended installation

Unattended installation enables system administrators to install the front-end applications using group policies. This enables system administrators to automate installation to ensure the correct version of the Control Center front-end application or Control Center Client front-end application is available to users.

The following sections provide the information a system administrator requires to implement unattended installation within your organization's environment.

Installer properties

To perform an unattended installation of the front-end applications, you must add the installer property USEEXISTINGSITEDBSETTINGS and set the value to 1.

New Client Control Center Installation

The Control Center front-end application is available in a range of language packs. English is installed by default.

You can change the language by updating the LANGUAGELCID installer property to one of the values below. If the installer does not include the chosen language pack, the Control Center front-end application will not be installed.

Language	ID
Chinese	2052
Chinese (Traditional)	31748
Finnish	1035
French	1036
German	1031
Hebrew	1037
Hungarian	1038
Italian	1040
Japanese	17
Korean	18
Malay	62
Polish	1045
Portuguese	1046
Russian	1049
Slovak	27
Spanish	2058
Vietnamese	42

Upgrading Control Center

When you upgrade the Control Center front-end application, the installed language pack is also upgraded. If the installer does not include that language pack, the Control Center front-end application will not be upgraded.

Prerequisites

The installers for the front-end applications have several prerequisites for the target PC before running the front-end application installer.

The following applications and registry settings are prerequisites for the Control Center front-end applications installation.

- Control Center site database location
  - This is stored in the registry:
    64-bit Windows: `HKLM\SOFTWARE\IndigoVision\Control Center Client 4`.
- Add a string value called `SdsAddress`

This contains the address to the Site Database Server in the form of `host:port`, for example, `192.168.1.1:8135` or `myserver:8135`

- Add a string value called `SiteDatabaseFilesPath`

  This contains the Site Database Files location, for example, ***C:\IndigoVisionSiteDBFiles***
- The following settings should be added only if Site Database Server Failover is required:
  - Add a string called `FailoverSdsAddress`

    This contains the address to the Site Database Server in the form of `host:port`, for example, `192.168.1.1:8135` or `myserver:8135`
  - Add a string called `FailoverSiteDatabaseFilesPath`

    This contains the Site Database Files location, for example, ***C:\IndigoVisionSiteDBFiles***
- Microsoft .NET Framework 4.8
  - ***ndp48-x86-x64-allos-enu.exe***
  - Available on the Control Center CD in the Control Center folder.
- Microsoft Sync Framework 2.1 core components
  - ***Synchronization-v2.1-x64-ENU.msi***
  - Available on the Control Center CD in the Control Center folder.
- Microsoft Sync Framework 2.1 provider services
  - ***ProviderServices-v2.1-x64-ENU.msi***
  - Available on the Control Center CD in the Control Center folder.
- Microsoft Universal C Runtime
  - Available from Microsoft through Windows Update.
- Site Database Server Certificate
  - If your Site Database Server is using a self signed certificate the certificate must be installed.
  - The Site Database Server certificate should be installed in the Local Machine, Trusted Root Authority store.

Examples

Examples of registry scripts are available on the Control Center CD. The scripts are an example of how to set the Site Database Server Address and the Site Database Files path in the registry to `127.0.0.1:8135` and ***C:\IndigoVisionSiteDBFiles*** respectively.

The scripts are editable in the text editor, for example, Notepad.

If you want to use some advanced settings, for example ***Failover***, you need to add the required registry settings to the registry script.

► For more on registry settings, *see "Prerequisites" on page 44*

The scripts are available in the ***Unattended Installation*** folder on the Control Center CD.

An example Microsoft Windows Installer Transform file (.mst) with the required settings is also available in the ***Unattended Installation*** folder.

8 CAMERA GATEWAY INSTALLATION

This chapter details how to install the Camera Gateway.

Camera Gateway overview

The IndigoVision Camera Gateway enables third party cameras from a range of manufacturers to be connected to IndigoVision Control Center. The Camera Gateway takes video streams from third party cameras using their native protocols and enables users to view the streams in a Control Center front-end application and record them using NVRs.

The cameras do not need to support ONVIF in order to connect to the IndigoVision system, giving customers a wide choice of cameras to choose from.

The Camera Gateway supports video streams from H.264, MPEG-4 and MJPEG cameras, PTZ control, and events.

The Camera Gateway is a software service that can be installed on a Windows server, giving total flexibility. The Camera Gateway service enables multiple clients to stream video from the same camera, whilst only requiring a single stream from the camera to the Camera Gateway.

Intended use

The Camera Gateway enables third party cameras from a range of manufacturers to be connected to IndigoVision Control Center. If, for example, you want to use Control Center to view a location in which third party cameras are already installed, the Camera Gateway allows you to do so without having to change the cameras.

System specifications

The IndigoVision Camera Gateway can be installed on one of the following Windows operating systems:

- MS Windows 10 (64-bit)
- MS Windows 11
- MS Windows Server 2016

For systems with more than 16 streams it is recommended to use Windows Server 2016.

IndigoVision recommends that you install Camera Gateway on a server-style system, with a server network adaptor, and the following minimum requirements:

- Server class PC
- Current generation Intel Xeon processor
- 4GB RAM

- At least 5GB of disk space

IndigoVision recommends that for Camera Gateway installations on VMWare the minimum specification is:

- 4 vCPUs
- 4GB RAM
- VMXNET3 network adapter

For improved performance, configure the VMXNET3 network adapter with the following settings:

- **Receive Side Scaling**: Enabled
- **Tx Ring Size**: 4096
- **Rx Ring #1 Size**: 4096
- **Rx Ring #2 Size**: 4096

Installation procedure

The Camera Gateway installer first checks the system for the prerequisite components:

- Microsoft .NET Framework 4.5.2
- Microsoft SQL Server 2014 Express SP1.

The installer then installs each prerequisite component required, before installing the three components of the Camera Gateway.

Prerequisites

To install and use the Camera Gateway, the Microsoft .NET framework must be enabled:

- In Windows 10, click ***Start > Control Panel > Programs > Turn Windows features on or off***. Verify that Microsoft .NET Framework 3.5.1 is selected.

Installation

1. Insert the Control Center CD into the CD drive of the PC or server on which you are installing the Camera Gateway application. The Control Center install screen opens.

   If the install screen does not open automatically, double-click the ***Installer.exe*** file in your Windows Explorer window, or use the ***Run*** option on the Windows Start menu and enter the path to the ***Installer.exe*** file on the CD ROM.
2. Click ***Other Products...***, navigate to the ***CameraGateway*** folder and double-click ***setup.exe***.
3. If Microsoft SQL Server 2014 Express SP1 is not installed, you will be prompted to install it. Follow the on-screen instructions.

   If the Microsoft SQL Server 2014 Express SP1 installation fails to complete, you must manually remove the components.

   For more information, *see "Microsoft SQL Server 2014 Express installation fails to complete " on page 71*
4. If Microsoft .NET Framework 4.5.2 is not installed, you will be prompted to install it. Follow the on-screen instructions.
5. You may need to restart your computer. Restart the computer, then open the Control Center CD and select ***Camera Gateway***.
6. The Camera Gateway Core installation wizard opens. Follow the on-screen instructions.

7. When the Camera Gateway Core is successfully installed, click ***Finish***.

   The Camera Gateway Administrator installation wizard opens. Follow the on-screen instructions.

8. When the Camera Gateway Administrator is successfully installed, click ***Finish***.

   The Camera Gateway Interface installation wizard opens. Follow the on-screen instructions.

9. Optionally, you can configure the password and Camera Gateway Interface IP address.

   Cameras added to Camera Gateway are visible on this address.

   When you first install the Camera Gateway, the default username is `admin` and the default password is `password`.

   If only one IP address exists on the Windows server, the **IP Address** option is disabled.

10. When the Camera Gateway Interface is successfully installed, click ***Finish***.

9 FrontLine installation

This chapter details how to install FrontLine.

FrontLine System Overview

The IndigoVision FrontLine System allows recording of evidential quality video and audio using body worn cameras.

- Lightweight, easy-to-use cameras designed from the ground up to support lone workers
- Automatic import of video and audio from docked FrontLine Cameras into the Control Center suite.
- Digital signatures and tamper protection of recordings.
- Play back and export of recordings.

The system comprises the following components:

- **License Server**: An IndigoVision License Server with a Control Center license that includes the Body Worn Video feature.
- **VideoManager**: Software used for managing FrontLine Cameras and automatically importing video.
- **FrontLine Manager Interface**: Software used to interface between VideoManager and the rest of the Control Center product suite.
- **FrontLine Dock**: Hardware device connected to the PC that is running FrontLine (the FrontLine PC).

  The FrontLine Dock provides ports for docking multiple FrontLine Cameras.
- **FrontLine Cameras**: Portable cameras that connect to the FrontLine PC using the FrontLine Dock.
- **NVR-AS**: An IndigoVision Network Video Recorder/Alarm Server (NVR-AS) that is used to store and manage recordings downloaded from the FrontLine Cameras.

  The NVR-AS must be installed on the FrontLine PC.
- **Control Center front-end application**: The IndigoVision Control Center front-end application provides a powerful and flexible user interface for viewing and exporting the video and audio recordings created by FrontLine Cameras.
- **Camera wearer**: The person who uses a FrontLine Camera and may or may not be able to review their recordings in Control Center, depending on their access permissions.

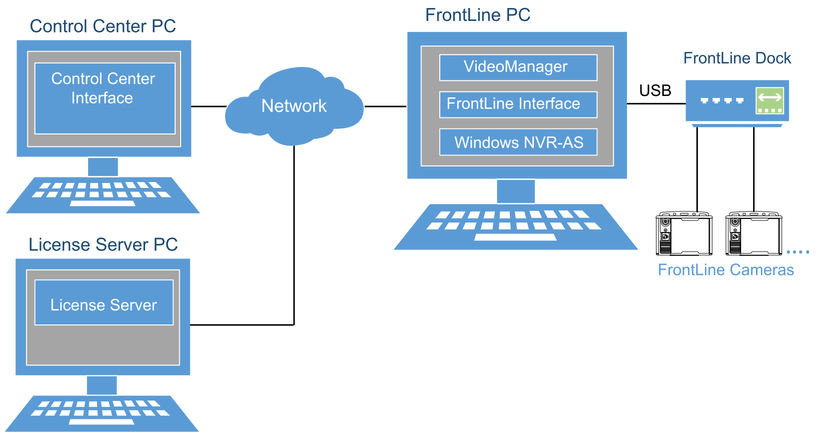

Figure 4: FrontLine overview

Installation

To use the IndigoVision FrontLine System, the NVR-AS, VideoManager and FrontLine Manager Interface must be installed on a FrontLine PC. An IndigoVision License Server with a Control Center license that includes the Body Worn Video feature must also be available on the network. Additionally, a VideoManager license must also be installed.

Notice *Upgrading the legacy FrontLine Manager solution to the latest VideoManager requires a new VideoManager license. The license will only be available if new VB400 or VT100 cameras are also being purchased.*

If you do not require any additional camera hardware then we recommend that you remain using the legacy FrontLine Manager solution.

After you have installed FrontLine you must adjust the VideoManager footage directory. This is required if you are using multiple FrontLine Cameras.

Also each FrontLine Camera needs to be commissioned for use with the FrontLine PC.

The IndigoVision Enterprise NVR-AS 4000 Windows Appliance can also be used as a powerful FrontLine PC.

The Control Center front-end application can be installed elsewhere on the network in order to manage camera wearers and review and export footage.

The Control Center front-end application can also be installed on the FrontLine PC to allow camera wearers to review their recordings when they return the FrontLine Cameras to a FrontLine Dock.

Configuration

Notice *This functionality is only available if you have administrator permissions.*

To create camera wearers and review footage you need to add the NVR-AS installed on the FrontLine PC to your Control Center site database.

1. Open Control Center and select ***Setup view***.
2. Add the NVR-AS installed on the FrontLine PC to the site database.
   - ► For more information about adding an NVR-AS to a Control Center site database, refer to the Control Center Help
3. In the ***Video explorer***, select the NVR-AS.

   The FrontLine tab is displayed in the main window.

   This tab provides access to VideoManager where camera wearers can be assigned to cameras.

Notice *When using multiple NVR-AS instances on the same FrontLine PC only the default instance can be used as the FrontLine NVR. It is not possible to use an alternative instance as the FrontLine NVR.*

Before a FrontLine Camera can be used, at least one camera wearer must be created. Camera wearers are created using Control Center.

System requirements

- At least 11 GB of disk space
- License Server version 18.2 or later
- NVR-AS version 18.2 or later

Before installing FrontLine, the IndigoVision NVR-AS software must be installed.

► For more information, *see "NVR-AS installation" on page 29*

FrontLine operating system requirements

Table 4 Supported operating systems

Operating system	Supported
Windows Server 2022	Y
Windows Server 2019	Y
Windows Server 2016	Y
Windows 11	Y
Windows 10 64-bit	Y
Other	N

FrontLine installation

The installation of the IndigoVision FrontLine software consists of the following stages:

1. Install VideoManager.
   - ► See "Install VideoManager" on page 54

Notice *If FrontLine Manager 6.1.6 or earlier is installed it must be manually uninstalled before starting this installation.*

2. Set up the VideoManager.
   - ► See "Set up VideoManager" on page 54

Notice *Any users which were created using FrontLine Manager 6.1.6 or earlier, through the web interface (i.e. not the bodyworn camera users added through Control Center), will not be migrated to VideoManager. These must be manually recreated through the VideoManagerweb interface (with the appropriate roles and permissions) after the initial installation and configuration is complete.*

3. Install the FrontLine Manager Interface.
   - ► See "Install the FrontLine Manager Interface" on page 55

Install VideoManager

You must first ensure that VideoManager is installed. You can get the latest version tested with the FrontLine Manager Interface from the IndigoVision Control Center CD.

1. Insert the Control Center CD.

   The Control Center install screen opens.

   If the install screen does not open automatically, locate and double-click the ***Installer.exe***.
2. Click ***Other Products***, navigate to theVideoManager folder, and double-click ***videomanager-setup-x64-<version>.exe***.
3. Follow the instructions within VideoManager installer to complete installation.

Set up VideoManager

After VideoManager is installed you need to do the initial setup and configuration.

1. In a web browser on the FrontLine PC, navigate to http://127.0.0.1:9080. We recommend Chrome, Edge or Firefox.
2. Click ***Setup***.
3. Read the agreement and click ***Accept*** to accept the agreement.
4. Choose your Database Setup option, then click ***Confirm***. We recommend that you use the built-in database.
5. Enter the credentials for an initial system administrator user, then click ***Confirm***.

   This administrator account can be used for any advanced configuration and is not expected to be used for day-to-day operations. We recommend giving this a unique username such as `VideoManagerAdmin`.

6. Set up your storage where VideoManager will store footage before it is imported into the NVR-AS video library, then click ***Confirm***.

The size of the disk space will be set-up later in the process.See "Configure the VideoManager footage directory" on page 56.

The VideoManager footage directory can be located on the same partition as the NVR-AS video library. If the video library is full when FrontLine cameras are docked, then the oldest un-protected recordings in the video library will be reaped.

Setup should now be complete. Click OK and optionally close the browser.

Set up HTTPS

You can optionally setup HTTPS.

1. In a web browser on the FrontLine PC, navigate to http://127.0.0.1:9080. We recommend Chrome, Edge or Firefox.
2. Log in using administrator account.
3. Navigate to ***Admin->System->Web server***.
4. Click the ***Use SSL?*** button to toggle it to ***On***.
5. Click the ***Configure*** button to configure an SSL certificate file
6. In the **Configure** dialog, click the ***Choose File*** button and use the file selector to navigate to an appropriate certificate file (saved as either ****.pfx*** or ****.p12*** format).
7. Verify that the details of the uploaded file are as expected, then click ***OK*** to close the dialog.
8. Click the ***Save Settings*** button, tick the box in the dialog to confirm that you understand the web server will briefly go offline, then click ***Yes***.
9. The browser should return to a screen showing that the settings have been saved but it does not automatically redirect to HTTPS. In order to continue with any additional setup, navigate to https://127.0.0.1:9080 and log back in.

Install the FrontLine Manager Interface

The final stage to install FrontLine Manager is to install the IndigoVision FrontLine Manager Interface.

1. Insert the IndigoVision Control Center CD.

   The IndigoVision Control Center install screen opens.

   If the install screen does not open automatically, locate and double-click the ***Installer.exe***.
2. Click ***Other Products***, navigate to the FrontLine folder, and then double-click ***setup.exe***. The Welcome dialog opens.
3. Click ***Next***.
4. The End-User License Agreement dialog opens. Read the agreement and select the check box to accept the agreement. Click ***Next***.
5. The Custom Set-up dialog opens. Enter the desired installation location or accept the default location and then click ***Next***. The Ready to Install dialog opens.
6. Click Install.

7. The installer opens a new window that lets you configure the FrontLine System administrator login credentials.

Notice *This is a separate user to the previous VideoManager administrator. You can use these credentials to log intoVideoManager in order to configure and assign cameras.*

We recommend that you provide a unique name, such as `FrontLineAdmin`, and a different password to the VideoManager administrator.

Do not use the same username for both accounts.

8. Click ***Finish***.

Configure the VideoManager footage directory

FrontLine automatically downloads recordings from docked FrontLine Cameras. These recordings are then temporarily stored in the VideoManager footage directory before being moved to the NVR-AS video library.

The VideoManager footage directory default location is on the system drive and is limited to 10GB.

This amount of temporary storage space is adequate when using a single FrontLine Camera. However, when using multiple FrontLine Cameras with the FrontLine PC the VideoManager footage directory needs to be increased by 16GB for each additional camera.

1. In a web browser on the FrontLine PC, navigate to https://127.0.0.1:9080 or http://127.0.0.1:9080 depending on your installation. We recommend that you use Chrome, Edge or Firefox.
2. Log into VideoManager as the system administrator.
3. Navigate to ***Admin->System->Storage***.
4. Select the ***Go to file space*** arrow.
5. Configure an appropriate maximum size.

   For a FrontLine PC using 21 cameras, the VideoManager footage directory should be limited to 330GB.
6. Click ***Confirm***.

Commissioning cameras

After the FrontLine software is installed, each FrontLine Camera that you wish to use with this FrontLine PC must be commissioned.

Prerequisite

Before you commission a camera, you must create an access control key for this FrontLine PC, if you have not already done so.

► For more information about configuring access control keys, refer to the FrontLine Administrators Guide

Notice *It is recommended that you create and use your own access control keys as this will prevent anyone from accessing footage on your cameras without the key.*

Commission a camera

1. In a web browser on the FrontLine PC, navigate to https://127.0.0.1:9080 or http://127.0.0.1:9080 depending on your installation. We recommend that you use Chrome, Edge or Firefox.
2. Log into VideoManager as the system administrator.
3. Select the ***Devices*** tab.
4. Put the FrontLine Camera into the FrontLine Dock.

   The camera appears in the devices list in the VideoManager.

   One of the following states is shown, depending on the camera history:

   - **Unassigned**: the device is ready to have a user assigned.
   - **Locked**: the device is configured with an access control key from another FrontLine PC. If you are sure you wish to commission this device for use with this PC, the camera must be reset. After reset, you can continue with the commissioning process.

Notice *A factory reset will remove all recorded footage from the camera.*

► For more information, *see "How to factory reset a FrontLine Camera" on page 57*

5. Click ***View Device Info*** > for the device you are commissioning.
6. If the camera has ***Touch Assign*** enabled, click ***Edit Device Properties*** ✎, disable ***Touch Assign*** and click ***Save Changes***.
7. To rename the device, click ***Edit Device Properties*** ✎, change the ***Device Name*** and click ***Save Changes***.
8. If the camera reports that it is using the built-in demonstration key, it must be factory reset to use the access control key for this PC.

   ► See "How to factory reset a FrontLine Camera" on page 57
9. Ensure the camera firmware is up to date.

   ► For more information about updating the camera firmware, refer to the FrontLine Administrators Guide

The FrontLine Camera is now commissioned and ready for use.

How to factory reset a FrontLine Camera

Notice *A factory reset will remove all recorded footage from the camera. To retrieve the footage from the camera, return it to the FrontLine Dock attached to the FrontLine PC where the camera wearer was assigned.*

To peform a factory reset, follow these steps:

1. In a web browser on the FrontLine PC, navigate to https://127.0.0.1:9080 or http://127.0.0.1:9080 depending on your installation. We recommend that you use Chrome, Edge or Firefox.
2. Log into VideoManager as the system administrator.
3. Select the ***Devices*** tab.
4. Click ***View Device Info*** > for the device you want to reset.
5. On the ***Device Actions*** toolbar, click ⚡.
   A warning message is displayed.
6. Click ***Yes, Reset Device*** to accept the warning message.

After a short period the device is reset and the status is shown as ***Unassigned***.

10 VIDEO STREAM MANAGER INSTALLATION

This chapter details how to install the Video Stream Manager.

Video Stream Manager Overview

The IndigoVision Video Stream Manager (VSM) allows IndigoVision Ultra 5K Fixed Cameras, IndigoVision or third-party ONVIF cameras, IndigoVision proprietary cameras, and RTSP cameras to be integrated into IndigoVision Control Center.

The VSM connects to ONVIF cameras, RTSP cameras, IndigoVision proprietary cameras, and Ultra 5K Fixed Cameras to stream video, and in the case of ONVIF and RTSP cameras, audio. The streams can then be relayed to IndigoVision Control Center to be viewed live, or recorded on NVRs.

The VSM is a software service that can be installed on a Windows server, giving total flexibility. The VSM service enables multiple clients to stream video from the same camera, whilst only requiring a single stream from the camera to the VSM.

Notice *A license is required for IndigoVision proprietary cameras.*

Intended use

The VSM enables IndigoVision Ultra 5K Fixed Cameras, ONVIF, and RTSP cameras to be connected to Control Center. If, for example, you want to use Control Center to view a location in which third-party RTSP capable cameras are already installed, the VSM allows you to do so without having to change the cameras.

The VSM can be used on the client side of a low bandwidth link to allow multiple clients to use a single stream that the VSM is receiving across that link.

System specifications

The IndigoVision VSM can be installed on one of the following Windows operating systems:

- Windows Server 2022
- Windows Server 2019 (recommended)
- Windows Server 2016

For systems with more than 16 streams it is recommended to use Windows Server 2016.

IndigoVision recommends that you install VSM on a server-style system, with a server network adaptor, and the following minimum requirements:

- Server class PC
- Current generation Intel Xeon processor
- 4GB RAM

Installation procedure

The VSM installer installs the VSM service and its prerequisites.

Notice *When the installer is installing the prerequisite of the VSM service, it may require a reboot. If prompted to reboot, follow the instructions. When the system has completed the reboot, manually run the VSM installer again.*

1. Insert the Control Center CD into the CD drive of the PC or server on which you are installing the VSM application.

   The Control Center install screen opens.
2. Click ***Other Products...***, navigate to the ***Video Stream Manager*** folder and double-click ***setup.exe***.
3. The VSM installation wizard opens. Follow the on-screen instructions.
4. Optionally, you can configure the Configuration Directory and VSM service IP address.

   Cameras added to the VSM are visible on this address.

   If only one IP address exists on the Windows server, the **IP Address** option is disabled.
5. When the VSM is successfully installed, click ***Finish***.

Proxy overview

Each proxy setup on the VSM consists of two parts.

- The source camera that the VSM is proxying. This provides input, for example stream, for the VSM.
- The virtual ONVIF camera that the VSM creates as an output. This is the virtual ONVIF camera that clients can access in order to stream from the VSM.

The VSM supports proxying four different types of source camera.

ONVIF proxies

The VSM can proxy ONVIF cameras. This allows a single stream taken from the source camera to be efficiently distributed to multiple clients.

When configuring an ONVIF proxy, you specify the endpoint used by the ONVIF service of the camera. The endpoint consists of an IP and port. The VSM uses the endpoint to retrieve the ONVIF profile configuration from the source camera. This configuration is used to set up the same profiles on the virtual ONVIF camera.

RTSP proxies

The VSM can proxy third-party RTSP cameras. This allows RTSP cameras to be added to your Control Center site.

When configuring an RTSP Proxy, you specify an RTSP URL. The VSM uses the video and optional audio streams described by this RTSP URL to configure the virtual ONVIF camera.

As ONVIF cameras use RTSP for streaming, it is possible to set up an RTSP Proxy for an ONVIF camera by using the RTSP URL for one of the profiles of the camera. However, in this case, the virtual ONVIF camera can only proxy one of the profiles of the source camera. All camera profiles can only be proxied if a dedicated ONVIF Proxy is used.

Ultra 5K proxies

The VSM can proxy IndigoVision Ultra 5K cameras in order to allow their high resolution streams to be efficiently distributed to multiple ONVIF clients. An Ultra 5K proxy supports two configuration modes.

In ***Simple Mode***, the VSM automatically creates high and low bitrate profiles on the Ultra 5K. The virtual ONVIF camera generated for the proxy will have two profiles that mirror these.

In ***Advanced Mode***, the profile configuration on the Ultra 5K is left to the user. The VSM will automatically update the virtual ONVIF camera to mirror the profiles set up on the Ultra 5K.

Notice *For all types of proxy, making changes to the configuration of the source camera must be done directly on the source camera. Changes to the source camera setup cannot be made using a virtual ONVIF camera.*

IndigoVision Proprietary Camera Proxies

The VSM can now proxy H.264 video from IndigoVision fixed and PTZ proprietary cameras.

VSM Administrator can be used to add cameras, remove or edit them. Managed IndigoVision proprietary PTZ cameras can be panned, tilted and zoomed in Control Center. Custom commands and PTZ presets are supported. If the camera has custom preset names configured, they are displayed in Control Center.

11 CONTROL CENTER WEB INSTALLATION

This section details how to install Control Center Web.

System requirements

You can install Control Center Web on one of the following Windows operating systems:

- Windows Server 2019 (recommended)
- Windows Server 2016
- Windows 11
- Windows 10 64-bit

IndigoVision recommends that you install Control Center Web on a server-style system, with a server network adaptor, and the following minimum requirements:

- Server class PC
- 8 GB of RAM

The IndigoVision Enterprise NVR-AS 4000 1U and 2U and IndigoVision Hybrid NVR Workstation are all compatible with Control Center Web. These platforms can be used to run both the NVR-AS software and Control Center simultaneously.

Control Center Web is compatible with common virtualization software, including VMWare ESXi and Microsoft Hyper-V.

Browser compatibility

The Control Center Web client application is compatible with the following web browsers:

- Mozilla Firefox 54.0 or later
- Google Chrome™ 60.0 or later
- Microsoft Edge 79 or later

IndigoVision recommends that all browsers are kept up to date with the latest security updates.

Certificates

Control Center Web requires a certificate to secure the service. You must use one of the following options:

- **Use a certificate signed by a trusted public Certificate Authority (CA)**

  Using a public CA to secure the service is the best option in several ways.

  It has the major advantage of not requiring certificates to be installed on the client devices. This is particularly useful when you wish to deploy Control Center Web on the Internet to give access to individuals outside of your organization.

However, it will usually involve paying a fee to the CA vendor.

- No need to install certificates on client devices
- No need to setup a private CA server

- **Use a certificate signed by a private Certificate Authority (CA)**

  You can set up a private CA service using Microsoft Active Directory Certificate Services or other tools.

  ► For more information, refer to "Types of Certification Authorities", at https://technet.microsoft.com/en-us/library/cc732368(v=ws.11).aspx

  Many IT departments in a corporate environment will have set up a private CA as part of their network infrastructure.

  - No fee to a CA vendor
  - CA root certificate must be installed on all client devices
  - CA service must be set up separately

- **Use a self-signed certificate**

⚠ Warning

Using a self-signed SSL/TLS certificate introduces a significant security risk to your system and may allow attackers to access sensitive data. IndigoVision always recommend using a signed certificate from a trusted Certificate Authority.

Control Center Web can generate and install a self-signed certificate automatically. This allows the system to be set up quickly, and has no cost implications. However, self-signed certificates do not provide the same level of security as CA signed certificates.

- No need to setup a private CA server
- No fee for CA vendor
- Easy to set up
- Insecure

When installing Control Center Web, it is important that you are aware of these options, and understand which option best fits your deployment. This choice is not permanent and you can change the certificate after installation.

To securely deploy Control Center Web for use over the Internet, separate SSL/TLS certificates will be required for the Control Center Web application server and the media server.

*Alternatively, a wildcard SSL/TLS certificate can be used for both servers (e.g. *.yourdomain.com).*

Install the media server

The first component to install for Control Center Web is the media server. This is distributed as a live CD ISO image for installation on any modern virtualization technology.

The following instructions assume that you are using Microsoft Hyper-V, on Windows Server 2016.

Enable Hyper-V

To use Hyper-V on Windows Server 2012 R2, you must enable it as a server role.

1. In the Server Manager application, select ***Add Roles and Features***.
2. In the **Installation Type** screen, select ***Role-based or feature based installation***.
3. In the **Server Selection** screen, select the local server.
4. In the **Server Roles** screen, select ***Hyper-V***.
5. In the **Features** screen, go to ***Remote Server Administration Tools > Role Administration Tools*** and ensure that ***Hyper-V Management Tools*** is selected.
6. Click ***Install***, accept all confirmations, and restart the PC.

   Hyper-V is installed on Windows Server 2012 R2.

Configure Hyper-V networking

In order to install Control Center Web correctly, the media server must be accessible to both the application server and the client web browsers. IndigoVision recommends using an External Switch configuration on the Hyper-V host to achieve this.

1. Open the Hyper-V Manager tool.
2. In the pane on the left of the screen, ensure that the local PC is selected.
3. In the ***Actions*** pane, select ***Virtual Switch Manager...***.
4. In ***Virtual Switches***, select ***New virtual network switch***.
5. In ***Switch type***, select ***External***.
6. Click ***Create Virtual Switch***.
7. In ***Switch name***, enter `External Switch`.
8. In ***External network***, select the physical network adapter which you want to use.

   If you are using an Enterprise NVR-AS 4000, select one of the following adapters:

   - ***10 Gbps Team*** (preferred)
   - ***1 Gbps Team***
9. Ensure that ***Allow management operating system to share this network adapter*** is selected.
10. Click ***OK***.

    A new network adapter named `vEthernet (External Switch)` is created on the server.

    Use this adapter if you want to change the IP address on the teamed interface.

Create the virtual machine for the media server

You must create a virtual machine on which to install the media server.

1. Open the Hyper-V Manager tool.
2. In the pane on the left of the screen, ensure that the local PC is selected.
3. In the ***Actions*** pane, select ***New > Virtual Machine***.
4. In **Specify Name and Location** specify the following for the new virtual machine:
   - **Name**: for example `Control Center Web Media Server`
   - **Location**: the location to store the virtual machine. If you are using an NVR-AS 4000, then IndigoVision recommends that you use the default location on the C: drive.
5. In the **Specify Generation** screen, select ***Generation 1***.

6. In the **Assign memory** screen, select the required memory.

   IndigoVision recommends that you configure Hyper-V to dynamically assign memory to the media server when it is required, by doing the following:

   - Enable ***Dynamic Memory***
   - Set the startup memory to 1024 MB
   - Set the maximum to the amount of memory on the host PC

7. In the **Configure Networking** screen, select ***External Switch***.
8. In the **Create Virtual Hard Disk** screen, do the following:

   - Create a new virtual hard disk.
   - If required, edit the name and location for the disk.

     If you are using an NVR-AS 4000, IndigoVision recommends using the C: drive as the default location.
   - Set the disk size to 10 GB.

9. Select ***Install the Operating System later*** and complete the wizard.

   The new virtual machine is created.

Install the media server on the virtual machine

You must install the media server on the Hyper-V virtual machine.

1. Open the Hyper-V Manager tool.
2. In the pane on the left of the screen, ensure that the local PC is selected.
3. Right-click the virtual machine to which you want to install the media server, and select ***Settings***.
4. Select the IDE controller with a DVD drive and click ***Browse...***.
5. Navigate to the ***mediaserver.iso*** file.

   This is on the IndigoVision Control Center CD-ROM, in the Control Center Web directory.
6. Select ***Processor*** and set ***Number of virtual processors*** to the maximum value.
7. Close the dialog.
8. Right-click the virtual machine to which you want to install the media server, and select ***Start***.
9. Right-click the virtual machine to which you want to install the media server, and select ***Connect***.

   A dialog opens, showing the progress of the media server installation.
10. When prompted, enter the following to set the network configuration for the media server:

    - IP address for the media server
    - Netmask of the network
    - Gateway IP address
    - Name server IP address

    You can change the IP configuration for the media server after installation.

    ► For more information, see the Control Center Web Administrator's Guide

    The server restarts and presents a login prompt.
11. Login to the media server with the following details:

    - Username: `msuser`
    - Default password: `1234`

12. Change the password using the following command:

    ```
    passwd
    ```

13. Follow the prompts to change the password for the ***msuser*** user.
    - ► For more information, see the Control Center Web Administrator's Guide

The media server can now be used with the application server as part of Control Center Web.

Site Database Server configuration

Control Center requires access to the Site Database Server. To communicate securely, a service authentication token must be generated on the Site Database Server.

To generate a service authentication on the Site Database Server, do the following:

1. Open the Windows Start menu and select ***IndigoVision > Site Database Server Setup***.
2. In the Site Database Server Setup tool, click ***Next***.
3. On the Site Database Configuration page select ***Generate a service authentication token*** and click ***Next***.
4. Take note of the token displayed on the **Generate a Service Authentication Token** page. This will be needed later.
5. Click ***Next*** to add it to the Site Database Server.
6. After the configuration has completed, click ***Finish*** to close the Site Database Server tool.

Notice *If you have already generated a service authentication token, there is no need to generate another. The same token can be used by multiple applications.*

If the Site Database Server is using a self-signed certificate, the Site Database Server certificate must be installed on the PC that hosts the Control Center application server.

Notice *This is only required if you are using a self-signed certificate on the Site Database Server.*

To export the self-signed Site Database Server certificate and install it on the Control Center Web host, follow these steps::

1. On the Site Database Server, navigate to ***Start > Control Panel***.
2. Search for the Manage computer certificates application within the Control Panel and open it.
3. Select ***Personal > Certificates***.
4. Search for the certificate with the following in the friendly name column: ***Self Signed Site Database Server Certificate***.
5. Right click on the certificate and select ***All tasks > Export...***
6. Follow the wizard to export the certificate.
   - Do not export the private key
   - Accept the other default options
7. Copy the resulting `.cer` file to the Control Center application server host PC.
8. Open the certificate on the Control Center application server host PC and click ***Install...***
9. Follow the wizard and do the following:

- Install the certificate to the Local Machine
- Select the Trusted Root Certificate Authorities store

10. The Control Center application server host PC will now trust connections with the Site Database Server.

Install the application server

Install the application server component after the media server.

1. Insert the IndigoVision Control Center CD-ROM.

   The IndigoVision Control Center install screen opens.
2. In Windows Explorer, navigate to the Control Center Web directory on the CD-ROM and double-click the ***ControlCenterWeb.exe*** file.

   The **End-User License Agreement** dialog opens.
3. Read the agreement, select the check box to accept the agreement, and click ***Install***.

   The Control Center Web Setup Wizard opens.
4. Click ***Next***.

   The **Configuration Options** dialog opens.
5. Update the following fields:
   - **Install IndigoVision Control Center Web to:**

     Enter the location to which you want to install the Control Center Web.
   - **Specify the Media Server URL:**

     Enter the URL that will be used by Control Center Web to access the media server.

     You must replace SET_MEDIA_SERVER_HOST_HERE with the hostname or IP address of your media server.
6. Click ***Next***.

   The **Site Database Server Configuration** dialog opens.
7. Enter the hostname or IP address and port of the Site Database Server and the service authentication token noted earlier.
8. Click ***Next***.

   The **Certificate Configuration** dialog opens.
9. A valid SSL/TLS certificate must be installed in order for Control Center Web to operate.

For more information on SSL/TLS certificates, see "Certificates" on page 63

Choose from the following options:

- **Supply a certificate file**

  If you have an existing certificate, do the following:
  a. Select the ***Supply an Existing certificate file (.pfx)*** radio button.
  b. Click ***Select***, and select the desired file.
  c. Enter the password for the certificate.
  d. Click ***Next***.
- ***Automatically generate a self-signed certificate***

Control Center Web can automatically generate and install a self-signed certificate. These do not provide as much security as signed certificates but allow installations to be set up quickly and easily. To configure:

a. Select the ***Generate an untrusted self-signed certificate*** radio button and click ***Next***.
b. A warning message will be displayed to highlight the security issues associated with this type of certificate. Read the information provided and click ***Confirm*** to proceed.

- **Continue without installing a certificate**

  If you wish to configure a certificate later, you can skip this step. However, Control Center Web will not operate until a valid certificate is correctly installed. To continue:

  a. Select the ***Configure later*** radio button and click next.
  b. A warning will appear highlighting that a certificate is required for Control Center Web to operate. Click ***Next*** to proceed.

10. Click ***Install***.

    The application server installation begins.

11. If prompted to restart the PC, enter `Y`.

    When your PC restarts, the installer automatically starts again when you log back in.

12. When the installation is finished, click ***Close***.

13. If you wish to configure a TLS/SSL certificate after the installation completes, do one of the following:

    - Request a certificate from a Certificate Authority (CA)
    - Use an existing certificate

    ► For more information, see the Control Center Web Administrator's Guide

12 TROUBLESHOOTING

This chapter provides troubleshooting information for the installation of Control Center applications.

My trial license has expired

You can upgrade to a full license.

► For more information, *see "License management" on page 17*.

I've installed the License Server, but I don't have a trial license

If you have previously used the trial license, then you will not get access to another trial if you reinstall the License Server.

To use Control Center, you can upgrade to a full license.

► For more information, *see "License management" on page 17*.

Part of the Control Center suite reports it is unable to contact the License Server

- Check that the License Server service is running and has a valid license.
- Check that TCP port 8133 on the License Server is not being blocked by a firewall on the License Server PC, or the PC running the Control Center software which is reporting the issue.

Microsoft SQL Server 2014 Express installation fails to complete

If the Microsoft SQL Server 2014 Express installation fails to complete, you must remove the following components using ***Control Panel > Programs and Features*** before reinstalling.

- Microsoft SQL Server 2014
- Microsoft SQL Server 2008 Native Client
- Microsoft SQL Server 2012 Native Client
- Microsoft SQL Server Setup Support Files
- Microsoft VSS Writer for SQL Server 2014
- Microsoft SQL Server Browser for SQL Server 2014
- Microsoft SQL Server 2014 Transact-SQL ScriptDom

Site database cannot be edited

Control Center stores site information in the site database. Control Center may not be able to edit the database for the following reasons:

- The user account may not have permission to edit the database.
  - Ensure the user has the following file permissions to edit the site database:

    Windows Share Permissions: Full Control (to enable control by the NTFS Security permissions)

    NTFS Security Permissions: Synchronize, Read Permissions, Read Attributes, Read Extended Attributes, Write Attributes, Write Extended Attributes, Delete, and Change Permissions

A INDIGOVISION FIREWALL REQUIREMENTS

When setting up a network of IndigoVision equipment that includes firewalls, the following information should be used to configure the firewalls.

Notice *This information applies only if communication occurs between equipment on opposite sides of the firewall. Ports need not be opened in a firewall if the network protocol is exchanged entirely within a subnet or subnets that do not cross a firewall boundary.*

Firewalls should also support TCP and UDP connection tracking. UDP timeouts should be at least 30 seconds.

The direction specified for each port refers to the direction in which a new connection is initiated:

Direction	Connections
IN	Connection made to the device on the specified port
OUT	Connection made by the device to the specified destination port
IN/OUT	Connection made either to or from the specified port

Ports required by the License Server

Service	Prot.	Destination Port	Dir.	Comments
License Server	TCP	8133	IN	Used by Control Center front-end application, NVR-AS and CyberVigilant to request access to licensed functionality.
Discovery	UDP	49000	IN/OUT	Used by the License Server Administrator utility for broadcast discovery of License Servers.

Ports required by the Site Database Server

Service	Port	Destination port	Dir	Comments	Windows Firewall exception automatically added
Site Database Server	TCP	8135 (default)	IN	Provides Control Center with secure access to the configuration data for the site.	Yes
MongoDB	TCP	8134	IN	Required on both primary and failover Site Database Server only if the site is configured with a failover Site Database Server.	No

Ports required by an NVR-AS

Service	Prot.	Destination Port	Dir.	Comments
Control Data	UDP	49300	IN	Mandatory for communications with other IndigoVision devices including front-end application
Control Data	UDP	49300	OUT	Mandatory for the NVR-AS to initiate recording on Transmitters. Also required to receive alarm events from Transmitters, Receivers and Alarm Panels
License Server	TCP	8133	OUT	Mandatory for communication with the License Server
NVR Control Data	TCP	8130	IN	Mandatory for communication between the NVR and front-end application
NVR Control Data	TCP	8130	OUT	Used for Alarm Server Record Actions and fault monitoring
Alarm Server Control Data	TCP	8131	IN	Mandatory for communication between the Alarm Server and Control Center front-end application
Playback	TCP	49299	IN	Used to playback video in front-end application
TCP Video	TCP	49400-49402,49420-49422	OUT	See separate section for details on ports used for different stream configurations.
TCP Audio	TCP	49410	OUT	
PTZ Control	TCP	49500 - 49509	OUT	Used for Alarm Server PTZ Actions
ONVIF communication over HTTP	TCP	80	OUT	Communication with ONVIF devices over HTTP
Firewall Friendly transport type ONVIF streams over HTTP	TCP	80	OUT	Video and Audio may be tunneled through HTTP for ONVIF devices
ONVIF communication over HTTPS	TCP	443	OUT	Communication with ONVIF devices over HTTPS
Firewall Friendly transport type ONVIF streams over HTTPS	TCP	443	OUT	Video and Audio can be tunneled through HTTPS for ONVIF devices that support it

Service	Prot.	Destination Port	Dir.	Comments
RTSP Communication	TCP	554	OUT	RTSP Communication with ONVIF devices
Reliable transport type ONVIF streams	TCP	554	OUT	
UDP Unicast Video, Audio & Control	UDP	12000-20001	IN	Used for Video, Audio & Control when using the Best Effort transport
UDP Multicast Video	UDP	49400, 49402, 49404, 49420, 49422, 49424	IN	
UDP Multicast Video Control	UDP	49401, 49403, 49405, 49421, 49423, 49425	IN/OUT	
UDP Multicast Audio	UDP	49410, 49430	IN	
UDP Multicast Audio Control	UDP	49411, 49431	IN/OUT	
Multicast routing	IGMP	N/A	IN/OUT	Mandatory for correct multicast operation
NVR Events	UDP	49301	IN	Used to receive events from CyberVigilant, as well as from IndigoVision Integrations and custom integration software built using the IndigoVision SDK.
Bandwidth Management	UDP	49600	OUT	Used to request a bandwidth allocation from the Bandwidth Manager
Email	TCP	25, 587	OUT	Used by Alarm Server Email Actions. Port is configurable. Port 25 is generally used for unencrypted SMTP access. Port 587 is generally used for TLS-encrypted SMTP access. Ports may vary between email providers.

Ports required by a Compact NVR-AS 4000 or Enterprise NVR-AS 4000 Linux appliance

Service	Prot.	Destination Port	Dir.	Comments
Web Configuration	TCP	80	IN	Only required for administration.
Secure Web Configuration	TCP	443	IN	Only required for administration.
NTP	UDP	123	OUT	Used for NTP time synchronisation.
SSH	TCP	22	IN	Only required for administration.
DNS	UDP	53	OUT	Used by Alarm Server Email Actions and NTP where a text hostname is used rather than an IP address
DNS	TCP	53	OUT	Used by Alarm Server Email Actions and NTP where a text hostname is used rather than an IP address
Open Manage Server Administrator	TCP	1311	IN	Enterprise NVR-AS 4000 only. Only required for administration.

Ports required by an NVR-AS 3000

Service	Prot.	Destination Port	Dir.	Comments
Web Configuration	TCP	80	IN	Only required for administration
telnet	TCP	23	IN	Only required for administration
FTP cmd	TCP	21	IN	Used for archiving recordings via FTP
FTP data	TCP	1024-4999	IN	Used for archiving recordings via FTP
NTP	UDP	123	OUT	Used for NTP time synchronisation
Syslog	UDP	514	OUT	External system logging support
SNMP	UDP	161	IN	Used for SNMP monitoring by third party network management tools
SNMP	UDP	161	OUT	Used to monitor UPS status
DNS	UDP	53	OUT	Used by Alarm Server Email Actions and NTP where a text hostname is used rather than an IP address
DNS	TCP	53	OUT	Used by Alarm Server Email Actions and NTP where a text hostname is used rather than an IP address

Ports required by Windows NVR-AS

These may include further Windows services such as NTP and Remote Desktop

Ports required by a FrontLine capable NVR-AS

Service	Prot.	Destination Port	Dir.	Comments
Web User Interface	TCP	9080	IN	Required for user and camera management, footage retrieval and VideoManager configuration.
FrontLine Interface	TCP	8132	IN	Mandatory for communication between Control Center and the FrontLine Manager Interface.

Ports required by Control Center front-end application

Service	Prot.	Destination Port	Dir.	Comments
Control Data	UDP	49300	OUT	Mandatory for communications to all IndigoVision devices
License Server	TCP	8133	OUT	Mandatory for communication with the License Server
NVR Control Data	TCP	8130	OUT	Mandatory for communication between the NVR-AS and front-end application
NVR Control Events	UDP	49303	IN	Mandatory for NVR event notifications and the front-end application
Alarm Server Control Data	TCP	8131	OUT	Mandatory for communication between the Alarm Server and front-end application

Service	Prot.	Destination Port	Dir.	Comments
FrontLine	TCP	8132	OUT	Used to manage users on a FrontLine capable NVR-AS
Playback	TCP	49299	OUT	Used to playback video from an NVR
TCP Video	TCP	49400-49402,49420-49422	OUT	See separate section for details on ports used for different stream configurations
TCP Audio	TCP	49410	OUT	
UDP Unicast Video, Audio & Control	UDP	12000-20001	IN	Used for Video, Audio & Control when using the Best Effort transport
UDP Multicast Video	UDP	49400, 49402, 49404, 49420, 49422, 49424	IN	
UDP Multicast Video Control	UDP	49401, 49403, 49405, 49421, 49423, 49425	IN/OUT	
UDP Multicast Audio	UDP	49410, 49430	IN	
UDP Multicast Audio Control	UDP	49411, 49431	IN/OUT	
Multicast routing	IGMP	N/A	IN/OUT	Mandatory for correct multicast operation
Serial Data	TCP	49500 - 49509	OUT	Used to access PTZ cameras connected to transmitter serial ports
Communication	TCP	80	OUT	Configuration of devices
Secure Communication	TCP	443	OUT	Secure configuration of devices
Firewall Friendly transport type ONVIF streams over HTTP	TCP	80	OUT	Communication with ONVIF devices
Firewall Friendly transport type ONVIF streams over HTTPS	TCP	443	OUT	Secure communication with ONVIF devices
Version check	TCP	80	OUT	Check for newer version of Control Center at login
RTSP Communication	TCP	554	OUT	RTSP Communication with ONVIF devices
Reliable transport type ONVIF streams	TCP	554	OUT	
FTP cmd	TCP	21	OUT	Used for passive FTP during bulk upgrade
FTP data	TCP	1024-4999	OUT	Used for passive FTP data transfer during bulk upgrade
WS-Discovery	UDP	3702	OUT	Used for discovery of ONVIF cameras

Additional ports may be required for Windows services including:

- NTP for time synchronisation
- Access to network drives for the site database
- Access to ODBC database for audit logging
- Telnet for administration of IndigoVision devices

Ports required by 8000, 9000, 11000, Ultra 2K Range cameras and encoders

Service	Prot.	Destination Port	Dir.	Comments
Control Data	UDP	49300	IN	Mandatory for communications with other IndigoVision devices including front-end application and NVR-AS. This is also used for UDP Video. Does not apply when using ONVIF firmware.
Serial Data	TCP	49500 - 49509	IN	Used to access PTZ cameras and other devices connected to the transmitter serial ports. Does not apply when using ONVIF firmware.
Serial Data 2	TCP	49510 - 49519	IN	An additional second serial data channel for integration purposes. This service may not be used for PTZ camera control through Control Center. Does not apply when using ONVIF firmware.
TCP Video	TCP	49400-49402,49420-49422	IN	See separate section for details on ports used for different stream configurations.
TCP Audio	TCP	49410	IN	
UDP Multicast Video	UDP	49400, 49402, 49404, 49420, 49422, 49424	OUT	
UDP Multicast Video Control	UDP	49401, 49403, 49405, 49421, 49423, 49425	IN/OUT	
UDP Multicast Audio	UDP	49410, 49430	OUT	
UDP Multicast Audio Control	UDP	49411, 49431	IN/OUT	
Multicast routing	IGMP	N/A	IN/OUT	Mandatory for correct multicast operation
Bandwidth Management	UDP	49600	OUT	Used to request a bandwidth allocation from the Bandwidth Manager
Web Configuration	TCP	80	IN	Only required for administration.
Secure Web Configuration	TCP	443	IN	Only required for administration.
telnet	TCP	23	IN	Only required for administration.
SSH	TCP	22	IN	Only required for administration.
FTP cmd	TCP	21	IN	Used for passive FTP during bulk upgrade. Does not apply when using ONVIF firmware.
FTP data	TCP	1024-4999	IN	Used for passive FTP data transfer during bulk upgrade. Does not apply when using ONVIF firmware.
NTP	UDP	123	OUT	Used for NTP time synchronization
DNS	UDP	53	OUT	Used by NTP where a text hostname is used rather than an IP address
DNS	TCP	53	OUT	Used by NTP where a text hostname is used rather than an IP address
Syslog	UDP	514	OUT	External system logging support
SNMP	UDP	161	IN	Used for SNMP monitoring by third party network management tools

Service	Prot.	Destination Port	Dir.	Comments
VBLTM	UDP	50000	IN/OUT	Used for VBLTM monitor
ONVIF Web Services	TCP	8080	IN	To allow ONVIF clients to use the camera. Only applies when using ONVIF firmware.
RTSP video and audio	TCP	554	IN	RTSP session control for Reliable, Best Effort and Multicast transports. Also used for reliable video and audio streams. Best effort video and audio streams use ephemeral ports. Only applies when using ONVIF firmware.
WS-Discovery	UDP	3702	IN/OUT	Unicast and multicast discovery of ONVIF devices. Only applies when using ONVIF firmware.

Ports required by BX and GX Range cameras

Service	Prot.	Destination Port	Dir.	Comments
RTSP video and audio	TCP	554 [1]	IN	RTSP session control for Reliable, Best Effort and Multicast transports. Also used for reliable video and audio streams. Best effort video and audio streams use ephemeral ports.
UDP Multicast video	UDP	49400, 49402, 49412 ‡	OUT	Video streams for Multicast transports.
UDP Multicast audio	UDP	49410 ‡	OUT	Audio streams for multicast transports.
Multicast routing	IGMP	N/A	IN/OUT	Mandatory for correct multicast operation
Web Configuration	TCP	80, 443 [1]	IN	Web configuration pages on the BX and GX Range devices.
NTP	UDP	123	OUT	Used for NTP time synchronization
SNMP	UDP	161	IN	Used for SNMP monitoring by third-party network management tools.
Email	TCP	25, 587	OUT	Used by email actions direct from the camera. Port is configurable on BX Range cameras. Port 25 is generally used for unencrypted SMTP access. Port 587 is generally used for TLS-encrypted SMTP access. Ports may vary between email providers.
DNS	UDP	53	OUT	Used by NTP and email where a text hostname is used rather than an IP address
DNS	TCP	53	OUT	Used by NTP and email where a text hostname is used rather than an IP address
WS-Discovery	UDP	3702	IN/OUT	Unicast and multicast discovery of ONVIF devices
WS-Discovery	UDP	Any in range 1024-65535	OUT	Unicast and multicast discovery of BX Range cameras.

1 = This is configurable through the device web page.

‡ = This is configurable through the ONVIF Configuration Utility.

Ports required by Ultra 5K Range cameras

Service	Prot.	Destination Port	Dir.	Comments
JPEG2000 video	TCP	8888	IN	JPEG2000 video streaming from Ultra 5K Fixed Cameras.
RTSP Video	TCP	554	IN	RTSP session control for Reliable and Best Effort transports. Also used for Reliable video streams. Best Effort video streams use ephemeral ports.
Web Configuration	TCP	80	IN	Web configuration pages on the Ultra 5k range device.
WS-Discovery	UDP	3702	IN/OUT	Unicast UDP and multicast discovery of ONVIF devices.
Multicast Routing	IGMP	N/A	IN/OUT	Mandatory for correct multicast operation

Ports required by 8000 and 9000 Range receivers

Service	Prot.	Destination Port	Dir.	Comments
Control Data	UDP	49300	IN	Mandatory for communications with other IndigoVision devices including front-end application and NVR-AS.
Control Data	UDP	49300	OUT	Used to initiate live video from transmitters. This is also used to receive UDP Video.
Serial Data	TCP	49500 - 49509	OUT	Used for serial connections between a PTZ keyboard attached to the receiver and a PTZ camera on a remote transmitter.
TCP Video	TCP	49400-49402,49420-49422	OUT	See separate section for details on ports used for different stream configurations.
TCP Audio	TCP	49410	OUT	
UDP Multicast Video	UDP	49400, 49402, 49404, 49420, 49422, 49424	IN	
UDP Multicast Video Control	UDP	49401, 49403, 49405, 49421, 49423, 49425	IN/OUT	
UDP Multicast Audio	UDP	49410, 49430	IN	
UDP Multicast Audio Control	UDP	49411, 49431	IN/OUT	
Multicast routing	IGMP	N/A	IN/OUT	Mandatory for correct multicast operation
Video Playback	TCP	49299	OUT	Playback of footage from an NVR-AS
Web Configuration	TCP	80	IN	Only required for administration
telnet	TCP	23	IN	Only required for administration
FTP cmd	TCP	21	IN	Used for passive FTP during bulk upgrade

Service	Prot.	Destination Port	Dir.	Comments
FTP data	TCP	1024-4999	IN	Used for passive FTP data transfer during bulk upgrade
NTP	UDP	123	OUT	Used for NTP time synchronization
DNS	UDP	53	OUT	Used by NTP where a text hostname is used rather than an IP address
DNS	TCP	53	OUT	Used by NTP where a text hostname is used rather than an IP address
Syslog	UDP	514	OUT	External system logging support
SNMP	UDP	161	IN	Used for SNMP monitoring by third party network management tools

Ports required by AP100 and AP110 Alarm Panels

Service	Prot.	Destination Port	Dir.	Comments
Control Data	UDP	49300	IN	Mandatory for communications with other IndigoVision devices including front-end application and NVR-AS.
Web Configuration	TCP	80	IN	Only required for administration
telnet	TCP	23	IN	Only required for administration
FTP cmd	TCP	21	IN	Used for passive FTP during bulk upgrade
FTP data	TCP	1024-4999	IN	Used for passive FTP data transfer during bulk upgrade
NTP	UDP	123	OUT	Used for NTP time synchronisation
Syslog	UDP	514	OUT	External system logging support
SNMP	UDP	161	IN	Used for SNMP monitoring by third party network management tools

Ports required by Bandwidth Manager

Service	Prot.	Destination Port	Dir.	Comments
Bandwidth Management	UDP	49600	IN	Used to issue bandwidth allocations to Transmitters and NVR-ASs

Ports required by Camera Gateway

Service	Prot.	Destination Port	Dir.	Comments
Control Data	TCP	80	IN	Camera Gateway Configuration
Control Data	TCP	25473	IN	Camera Gateway Configuration
Media Streaming	TCP	554	IN	RTSP session control and Reliable transport video streaming for each Camera Gateway managed camera

Service	Prot.	Destination Port	Dir.	Comments
Media Streaming	TCP	554	OUT	RTSP session control and Reliable transport video streaming for each unmanaged RTSP camera
Control Data	TCP	47002	IN	Mandatory for communications with front-end application
Events	TCP	29170	IN	Used to listen for events from cameras
WS-Discovery	UDP	3702	IN/OUT	Multicast discovery of cameras
Multicast Routing	IGMP	N/A	IN/OUT	Mandatory for correct multicast operation

The ports required for communication between a camera and the Camera Gateway vary depending on the camera. If these details are not provided, please contact the camera manufacturer.

Ports required by Video Stream Manager (VSM)

Service	Prot.	Destination Port	Dir.	Comments
JPEG2000 video	TCP	8888	OUT	JPEG2000 video streaming from Ultra 5K Fixed Camera.
Web Services	TCP	80	OUT	ONVIF web services requests and Firewall Friendly streaming over HTTP.
Secure Web Services	TCP	443	OUT	Secure ONVIF web services requests and Firewall Friendly streaming over HTTPS.
Web Services	TCP	12000-12999	IN	ONVIF web services for each managed camera.
RTSP	TCP	10000-10999	IN	RTSP session control and Reliable transport video streaming for each managed camera.
WS-Discovery	UDP	3702	IN/OUT	Unicast UDP and multicast discovery of ONVIF devices.
Multicast Routing	IGMP	N/A	IN/OUT	Mandatory for correct multicast operation
RTSP	TCP	554	OUT	RTSP session control and Reliable transport video streaming for each unmanaged RTSP camera.

Ports required by Control Center Web

Ports required by Control Center Web Application server

Service	Prot.	Destination Port	Dir.	Comments
Web Services	TCP	443	IN	Web site and API provided using HTTPS. The port number is configurable.
Media Server Control	TCP	8888	OUT	Media server web socket API for controlling video streams.

Service	Prot.	Destination Port	Dir.	Comments
ONVIF	TCP	80	OUT	Communication with ONVIF devices for starting video.
Alarm Server	TCP	8131	OUT	Receive alarm information from Alarm Server.
Site Database Server	TCP	8135 (default)	OUT	Read the site database from the Site Database Server.

Ports required by Control Center Media Server

Service	Prot.	Destination Port	Dir.	Comments
STUN/TURN	TCP/UDP	5349	IN	Listen for STUN/TURN requests from clients and stream WebRTC (SRTP) video to allow NAT traversal.
Media Server Control	TCP	8888	IN	Web socket API for use by application server to control video streams.
RTSP	TCP	554	OUT	RTSP session control for streaming video from cameras.
WebRTC	UDP	49152-65535	IN	Serve WebRTC (SRTP) video streams.

Ports required by CyberVigilant

Service	Prot.	Destination Port	Dir.	Comments
Web Configuration	TCP	80	IN	Web configuration. Only required for administration.
Secure Web Configuration	TCP	443	IN	Secure HTTPS-based web configuration. Only required for administration.
SSH	TCP	22	IN	Only required for administration.
NTP	UDP	123	OUT	Used for NTP time synchronisation.
DNS	UDP	53	OUT	Used by NTP and remote logging where a text hostname is used rather than an IP address
DNS	TCP	53	OUT	Used by NTP and remote logging where a text hostname is used rather than an IP address
Syslog	UDP	514	OUT	External system logging support
File Sharing	TCP	445	OUT	Microsoft-DS SMB file sharing
NVR Events	UDP	49301	OUT	CyberVigilant alarm notifications

Ports required for IndigoVision VPN

Service	Protocol	Destination Port	Dir	Comments
OpenVPN Server	UDP	1194	IN	Connections from remote VPN clients
OpenVPN Client	UDP	User defined	OUT	Connections to remote VPN servers

Video stream configuration port usage

Each IndigoVision Transmitter can have 3 separate stream configurations on up to two independent encoders giving a total of 6 stream configurations. For TCP and UDP multicast video the ports used will depend on the stream configurations that have been set up. It should be noted that multiple video streams from the same stream configuration would use the same TCP/IP port. The table below illustrates how the ports are used by different video transport protocols and stream configurations:

Stream Configuration	UDP Unicast Video	UDP Multicast Video	UDP Multicast Video Control	TCP Video
Encoder 1 Stream 1	49300	49400	49401	49400
Encoder 1 Stream 2	49300	49402	49403	49401
Encoder 1 Stream 3	49300	49404	49405	49402
Encoder 2 Stream 1	49300	49420	49421	49420
Encoder 2 Stream 2	49300	49422	49423	49421
Encoder 2 Stream 3	49300	49424	49425	49422

B NVR-AS POST-INSTALLATION NETWORK DRIVE CONFIGURATION

If you are recording to a network drive, IndigoVision recommends that you do the following:

- Create a special user account for this purpose.
- Change the temporary Video Library folder that you set up during installation.

Creating a user account

To allow the NVR-AS to record to this folder, you must enter the account's user name (which includes the domain name) and password as follows:

1. From the ***Start*** menu, select ***Settings>Control Panel>Administrative Tools>Services***.
2. Right-click ***Indigovision NVR-AS*** and select ***Properties***.
3. Click the Log on tab and select the required account. The user name you enter must have read/write access to the Video Library.
4. Enter and confirm the password, then click ***OK***.

Only video data should be stored on a network share; configuration information should be stored on a local drive which is directly attached to the NVR-AS machine.

Changing the video library folder

You will have set up a temporary Video Library folder during installation.

To change this to a permanent location:

1. From the ***Start*** menu, select ***Programs>IndigoVision>NVR-AS>NVR-ASAdministrator***.
2. In the ***Video Library*** field, enter the required Video Library folder (UNC path). To browse to select a network share, click ... .

⚠ Caution

Take care not to select a mapped network drive as this will not be recognized by the NVR-AS.

3. Click ***Set***.

Notice *For optimal performance, the UNC path should be either:*
an IP address, for example, ***\\192.168.1.2\VideoLibrary***
a fully qualified domain name, for example, ***\\nvrtest.indigovision.com\VideoLibrary***
It should not be a NetBIOS name, for example, ***\\NVRTEST\VideoLibrary****.*

Restarting the NVR-AS

1. From the Start menu, select ***Settings>Control Panel>Administrative Tools>Services***.
2. Right-click ***Indigovision NVR-AS*** and select ***Restart***.

C UPGRADING CONTROL CENTER

Depending on your current version of Control Center, you need to follow different upgrade procedures to ensure you have all the resources required to run the latest version of the application.

Upgrading to Control Center 17.1 or later

To upgrade from Control Center 17.0 or earlier to Control Center 17.1 or later, you need to complete the following procedures:

1. 64-bit migration
2. NVR-AS Authentication

64-bit migration

Control Center is a 64-bit application from 17.1 onwards.

Upgrading an installation from an earlier version keeps all settings from the earlier version with the following exceptions:

- If you use audit logging, through either IndigoReports or Legacy Reports, you need to install a 64-bit version of the ODBC driver and reselect the driver in Control Center using ***File > Audit Log Settings > Change…***.
- If you use Custom Objects or plugins compiled for 32-bit Windows, they will need to be recompiled for 64-bit to work with Control Center.
- If you use Unattended Installation, you need the latest files.
  - ► For more information, *see "Unattended installation" on page 37*

NVR-AS authentication

A username and password must be configured for each NVR-AS from 17.1 onwards. When migrating from a version earlier than 17.0, it is important to take the following additional steps to minimize NVR service interruption:

1. Enable the option to allow unauthenticated access when upgrading each NVR-AS:
   - For Windows NVR-AS, run the NVR-AS Administrator.
   - For Linux appliances, visit the Network Security web configuration page.
2. Upgrade all Control Center front-end applications.

⚠ Caution

If any Control Center front-end applications are not upgraded, service will be interrupted when authentication is configured.

3. For each NVR-AS:

a. Disable the option to allow unauthenticated access.
b. Configure NVR-AS Authentication credentials.
c. In Control Center, configure Device Access credentials for the NVR-AS.

Caution *Control Center operators and administrators will not be able to use the NVR-AS if authentication has been configured on the NVR-AS, but not in Control Center.*

Upgrading from Control Center 17.0 to a later version

Notice *Control Center is a 64-bit application from 17.1 onwards. This may affect some settings from the earlier versions.*

► For more information, *click here.*

To upgrade Control Center from version 17.0 or later, do the following.

1. Backup the following configuration data:
   - Control Center front-end application site database
   - NVR-AS configuration
2. Upgrade the License Server.
3. Upgrade the Site Database Server.
4. Upgrade each NVR-AS.
5. Upgrade each Control Center front-end application.

License Server compatibility

Warning *To ensure system compatibility and on-going operation, IndigoVision recommends that the License Server version matches the versions of all NVR-AS and Control Center workstations.*

After you have upgraded the License Server, all licensed products may need to use their backup license. You must upgrade all licensed products to a compatible version before the backup license expires. A backup license is valid for 30 days from the last successful connection to a compatible License Server.

Site Database Server compatibility

After you have upgraded the Site Database Server, all installations of the previous version of the Control Center front-end application will still be able to login and read the site database. However, previous versions of the Control Center front-end application may be prevented from changing the site configuration until the Control Center front-end application is upgraded.

Upgrading from Control Center 16 to a later version

Notice *Control Center is a 64-bit application from 17.1 onwards. This may affect some settings from the earlier versions.*

➢ For more information, *click here.*

To upgrade Control Center from version 16.0 or later, do the following.

1. Backup the NVR-AS configuration
2. Copy the Control Center site database directory to a new location for use with the Control Center 17.0 system. This will become the Site Database Files in the upgraded system.

Notice *Do not upgrade using the live version of the Control Center 16 site database to avoid potential data loss.*

3. Upgrade the License Server.
4. Install the Site Database Server.

   Follow the installation instructions and select ***Upgrade from a Control Center 16 site database***.

   ➢ For more information, *see "Upgrade from a Control Center 16 site database" on page 25*
5. Upgrade each NVR-AS.
6. Upgrade each Control Center front-end application.

After all Control Center workstations have been upgraded, you should delete the old Control Center 16 site database, and the following files from within the Site Database Files directory:

- ***sites.vdc***
- ***users.vdc***
- ***tasks.vdc*** (if it exists)

Upgrade from Control Center 15 or earlier

Notice *Control Center is a 64-bit application from 17.1 onwards. This may affect some settings from the earlier versions.*

➢ For more information, *click here.*

If the current system is running Control Center 15 or earlier, a direct upgrade is not possible. At least one Control Center Workstation and License Server must first be upgraded to version 16 to ensure that the Control Center site database is compatible before upgrading to Control Center 17 or later.

1. Follow the Control Center 16 installation guide to upgrade at least one installation of the Control Center front-end application and the License Server to version 16.

You can use a copy of the Control Center 15 or earlier site database during this upgrade to avoid impacting the existing live system.

2. Log in to the Control Center 16 front-end application as an administrator and make a small temporary change to the user configuration, to ensure that the underlying database is upgraded as required.

   For example, add a new user and then delete them.
3. Make a small temporary change to the site configuration, to ensure that the underlying database is upgraded as required. For example, add a subsite and then delete it.

If you are upgrading a segmented site database, you must login to each segment in turn and make a temporary change to all of them.

4. Close the Control Center front-end application.
5. Follow the Control Center Installation guide to upgrade from Control Center 16 as normal.

D INSTALLING A WINDOWS NTP SERVER

Accurate time synchronization is critical for all elements in an IndigoVision security system. IndigoVision cameras and NVR-AS 3000 units have built in network time protocol (NTP) software accessible through the device web page.

Windows-based devices, including the NVR-AS 4000, VSM, Camera Gateway servers and workstations running the Control Center front-end application must be time synchronized.

To synchronize your devices it is recommended that you use the Windows network time protocol (NTP) server software included on the Control Center product CD.

Installation and configuration

This procedure tells you how to install and configure the Windows network time protocol (NTP) server software.

⚠ Caution

*When the Windows NTP daemon is installed, the standard Windows Time service (***W32Time***) is disabled and can no longer be used.*

1. On the Control Center CD, navigate to ***Resources\NTP Server***.
2. Run ***vc_redist_x86.exe***.

   This installs the Microsoft Visual C++ 2008 Redistributable Package (x86) C++ runtime required by the NTP software.
3. Run ***ntp-4.2.8p13-win32-setup.exe***

   This installs the Windows NTP daemon.
4. Accept the license agreement, default installation folders, and default settings.
5. On the **Configuration Options** dialog specify the time source for the NTP daemon.
6. Specify the upstream NTP servers using a comma separated list.
   - If you are installing the NTP daemon on a server (for example, NVR-AS 4000, Windows NVR-AS, VSM, or Camera Gateway) which is to be used as an NTP server for downstream clients:

     Select the check box ***Add local clock as a last resort reference***.
   - If you are installing the NTP daemon on a Control Center PC, use these settings:

     Do not select the check box ***Add local clock as a last resort reference***.
7. Choose whether to create a new account or use an existing one to run the daemon.

   If adding a new account the password must meet the criteria :

   a. Be at least six characters in length.

   b. 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, !, $, #, %)

If the password does not meet the requirements you get the error message ***ERROR 2245***.

8. Use the default ***NTP Service Settings***.

The Windows NTP daemon is now configured to synchronize the system clock with the upstream NTP servers. You can check the current state of time synchronization by running the **Quick NTP Status** utility.

To run the utitlity:

Select ***Start Menu > All Programs > Meinberg > Network Time Protocol > Quick NTP Status***.

E INSTALLING WINDOWS NVR-AS IN A HIGH-AVAILABILITY CLUSTER

The IndigoVision NVR-AS software can be used in a failover cluster to provide high availability and redundancy. Multiple servers can be configured within a cluster so that if the NVR-AS software or the server that it is running on encounters a critical failure, the NVR-AS can start running on another server.

This section explains how to configure the NVR-AS software to operate within a failover cluster environment on Microsoft Windows Server 2012 R2 using two servers and shared iSCSI storage with the following failover policies:

- If the NVR-AS software encounters a problem it restarts.
- A failure to restart the NVR-AS software, or two failures within 15 minutes results in a failover onto another node.
- A failover occurs if the node cannot be contacted by the majority of online nodes.
- If more than 10 failures are encountered within a time period of 1 hour the cluster service remains offline.

Prerequisites

To configure the NVR-AS software to operate within a failover cluster you must configure the following elements:

- Domain and IP address
- Storage and server hardware requirements

Domain and IP address requirements

Ensure that both servers you want to add as cluster nodes have joined the same Active Directory domain.

Notice *To configure failover clusters you will need to be logged in as a domain administrator.*

Notice *Static IP addresses must be used by the two servers and at least two unassigned IP addresses must be available for configuration of the cluster and the NVR-AS role. Both servers must be on the same network.*

Storage and server hardware requirements

iSCSI storage must be connected to both servers and configured with three targets, each with one mapped LUN. The recommended sizes for the mapped LUNs are:

- Cluster Disk Witness: 512MB
- NVR-AS configuration files: 1GB
- NVR-AS Video Library: Remainder of storage space.

► For details on creating iSCSI targets on the storage array, refer to the manufacturer's instructions.

Server grade PCs should be used with the following specifications:

- Windows Server 2012 R2
- We recommend that you use two matching computers that contain the same or similar components.
- Servers should have at least two network adapters.
- Each network adapter should be dedicated to either network communication or iSCSI, not both.

► For more details on hardware requirements, refer to the Microsoft Technet article Failover Clustering Hardware Requirements and Storage Options

Setup process

This section details the process for setting up the NVR-AS failover cluster.

A summary of the process is as follows:

1. Connect to iSCSI storage
2. Install NVR-AS on the first node
3. Install failover clustering
4. Create and configure failover cluster
5. Complete the configuration of the cluster

Step 1: Connect to iSCSI storage

Both nodes need to connect to the three iSCSI targets. Repeat the following on both nodes:

1. Click ***Start***, type `iSCSI`, and then click ***iSCSI Initiator***.
2. Enter the IP address or DNS name of the storage then click ***Quick Connect…***.

   This may take a few minutes to connect.
3. Select each discovered target from the storage and click ***Connect***.

   After all three targets are connected, click ***Done***.
4. Select the ***Volumes and Devices*** tab, then click ***Auto Configure***.
5. Click ***OK*** to close the dialog.

You need to create a volume before the storage can be used. Complete the following steps on the first node:

1. Start **Server Manager**.
2. Select ***Files and Storage Services > Disks***.
3. Create a volume for each disk in turn:
   a. Right-click on the disk and select ***Bring Online***.

b. Right-click on the disk and select ***New Volume…***.
c. Click ***Next***.
d. Select the first node from the ***Server*** section and the disk from the ***Disk*** section, then click ***Next***.
e. Ensure that the available capacity is entered in the ***Volume size***, then click ***Next***.
f. Select a drive letter, then click ***Next***.
g. Provide a suitable volume label, then click ***Next***.

   For the NVR-AS Video Library volume, the recommended allocation unit size is 64K.
h. Click ***Create***.
i. Click ***Close***.

Step 2: Install NVR-AS on the first node

- For instructions on how to install the NVR-AS, *see "Step 2: Install the NVR-AS" on page 30*.

Complete the NVR-AS Administrator wizard, using the default settings:

1. On the **Identification** page, click ***Next***.
2. On the **Storage Locations** page enter temporary locations on the local drive, then click ***Next***.

   Click ***OK*** to any warnings.
3. On the **Network Settings** page, click ***Next***.
4. On the **Disk Space Management** page, click ***Next***.

   Click ***Yes*** to any warnings.
5. On the **Alarm and Data Record Management** page, click ***Next***.
6. On the **Email Settings** page, click ***Next***.
7. On the **Finish** page, click ***Finish***.
8. Click ***Finish*** to complete the installation process.

Step 3: Install failover clustering

The Failover Cluster feature must be installed on both servers that are added as nodes in the cluster.

1. Start **Server Manager**.
2. On the ***Manage*** menu, click ***Add Roles and Features***.
3. On the **Before you begin** page, click ***Next***.
4. On the **Select installation type** page, click ***Role-based or feature-based installation***, then click ***Next***.
5. On the **Select destination server** page, click the server being configured, then click ***Next***.
6. On the **Select server roles** page, click ***Next***.
7. On the **Select features** page, select the ***Failover Clustering*** check box.
8. To install the failover cluster management tools, click ***Add Features***, and then click ***Next***.
9. On the **Confirm installation selections** page, click ***Install***.
10. When the installation is completed, click ***Close***.
11. Repeat this process for all nodes.

Step 4: Create and configure failover cluster

Notice *To configure failover clusters you will need to be logged in as a domain administrator.*

To create and configure a failover cluster, you must do the following:

- Validate the configuration
- Create the cluster
- Add storage
- Configure the Quorum

Validate the configuration

Validate your cluster configuration and both nodes that will be used in the cluster. This only needs to be performed on one node.

On the first node:

1. Run **Failover Cluster Manager**.

   Click ***Start***, type `Failover`, and then click ***Failover Cluster Manager***.
2. In the right hand panel, click ***Validate Configuration…***.
3. On the **Before you begin** page, click ***Next***.
4. Either type the names of two servers that will be used as nodes and click ***Add*** or use ***Browse…*** to find them.
5. When both nodes have been added to the ***Selected servers*** list, click ***Next***.
6. On the **Testing Options** page select ***Run all tests***, then click ***Next***.
7. On the **Confirmation** page, click ***Next***.
8. Review the report provided. If any errors or warnings are displayed, these should be reviewed and if necessary addressed before proceeding.

   If any changes were made to address issues found during validation, repeat ***Validate Configuration***.
9. Check ***Create the cluster now using validated nodes***, then click ***Finish***.

   The ***Create Cluster Wizard*** starts.

► For further details on the validation process, refer to the Microsoft Technet article Validate Hardware for a Failover Cluster .

Create the cluster

1. Create a new cluster using the ***Create Cluster Wizard***.
2. On the **Before you begin** page, click ***Next***.
3. The cluster appears as a machine on the network with the settings specified on this page.
   a. Enter a suitable meaningful cluster name, for example `IV NVR-AS Cluster`.
   b. Uncheck any networks that are not to be used.

      Only the network for communication with Control Center should be selected.
   c. Provide an IP address for the cluster in the ***Address*** field for the selected network.

      This should be a unique IP address that is not already used by any PC or device.
4. Click ***Next***.

5. On the **Confirmation** page, uncheck ***Add all eligible storage to the cluster***, then click ***Next***.
6. On the **Summary** page, click ***Finish***.

Add storage

1. On the left hand side expand the tree to see **Storage**, and select ***Disks***.
2. In the right hand panel, click ***Add Disk***.
3. Select all disks to be used for NVR-AS configuration files, NVR-AS video library and quorum witness disk, then click ***OK***.
4. View the ***Owner Node*** column for each of the disks.

   If the ***Owner Node*** is not the first node where the NVR-AS software was installed, the storage must be moved:

   a. In the right hand panel, click ***Move Available Storage*** then ***Select Node...***.

   b. Select the node where the NVR-AS was installed, then click ***OK***.

Configure the Quorum

For the cluster to remain online and function there must be a majority of nodes online and able to communicate. This is described as achieving quorum. With an even number of nodes a majority is not possible. A disk witness must be configured to achieve quorum.

1. Select the cluster from the tree and then on the right hand side click ***More Actions > Configure Cluster Quorum Settings...***.
2. On the **Before you begin** page, click ***Next***.
3. Select the option ***Select the quorum witness***, then click ***Next***.
4. Select ***Configure a disk witness***, then click ***Next***.
5. Select the desired disk, then click ***Next***.
6. Click ***Next***.
7. On the **Summary** page, click ***Finish***.

Step 5 : Complete the configuration of the cluster

To complete the configuration of the cluster you must do the following:

- Create NVR-AS role
- Configure NVR-AS
- NVR-AS role configuration
- Install on the second node

Create NVR-AS role

1. Select ***Roles*** from the tree and then on the right hand side, click ***Configure Role...***.
2. On the **Before you begin** page, click **Next**.
3. Select ***Generic Service***, then click ***Next***.
4. Select ***IndigoVision NVR-AS***, then click ***Next***.
5. Provide the name and IP address for the NVR-AS Role.

   a. Enter a suitable meaningful name for the role, for example `NvrAsRole`.

   b. Uncheck any networks that are not to be used.

   Only the network for communication with Control Center should be selected.

   c. Provide the IP address that is to be used by the NVR-AS in the ***Address*** field for the selected network.

This should be a unique IP address that is not already used by any PC or device.

6. Click ***Next***.
7. Select the storage volumes to be used for the NVR-AS configuration files and the NVR-AS Video Library, then click ***Next***.
8. The Replicate Registry Settings must not be set at this point. Click ***Next***.
9. On the **Confirmation** page, click ***Next***.
10. On the **Summary** page, click ***Finish***.
11. Expand the tree and select ***Roles***.
12. Select the NVR-AS role just created then select the ***Resources*** tab at the bottom of the window.
13. Right click ***IndigoVision NVR-AS*** under Roles, then click ***Properties***.
14. In the ***Dependencies*** tab click in the empty row to add a new dependency, selecting the IP address from the dropdown. The ***AND/OR*** field should be left as ***AND***.
15. Click ***OK*** to confirm and close.
16. View the ***Owner Node*** column for the role.

    If the ***Owner Node*** is not the first node where the NVR-AS software was installed, the role should be moved:

    a. Select the NVR-AS role in the top half of the window.
    b. From the right hand side, click ***Move > Select Node…***.
    c. Select the node where the NVR-AS was installed, then click ***OK***.

Configure NVR-AS

1. Run NVR-AS Administrator.

   Click ***Start***, type `NVR-AS`, and then click ***NVR-AS Administrator***.
2. Update the ***Server Name*** and ***Location***. Click ***Next***.

   The name and location specified here will be used by all nodes.
3. Update the Video and Configuration paths to point to shared storage locations, then click ***Next***.
4. Change the NVR IP Address to the IP address specified when creating the NVR-AS role.

   Configure all other settings, then click ***Next***.

   ► For more details, *see "Step 2: Install the NVR-AS" on page 30*
5. Configure all other pages, and click ***Next*** to continue.
6. Select ***No, I will restart the NVR-AS service later***.
7. Click ***Finish*** to conclude the process.

NVR-AS role configuration

1. Return to the **Failover Cluster Manager**.
2. Expand the tree and select ***Roles***.
3. Right click on the NVR-AS role then select ***Properties***.
4. Select the ***Failover*** tab.
5. Enter a the following values:

   a. Maximum failures in the specified period: 10
   b. Period (hours): 1
6. Click ***OK***.
7. Select the NVR-AS role then select the ***Resources*** tab at the bottom of the window.
8. Right click on ***IndigoVision NVR-AS*** under Roles, then click ***Take Offline***.

9. Right click on ***IndigoVision NVR-AS*** under Roles, then click ***Properties***.
10. Select the Registry Replication tab, then click ***Add…***.
11. Type the following, then click ***OK***:
    `SOFTWARE\Wow6432Node\IndigoVision\Networked Video Recorder`
12. Click ***OK***.
13. Right click on ***IndigoVision NVR-AS*** under Roles, then click ***Bring Online***.

Install on the second node

Perform this for the remaining node within the cluster.

1. To display the NVR-AS Administrator, *see "Step 2: Install the NVR-AS" on page 30* and follow steps 1-6.
2. Accept default settings to complete NVR-Administrator setup.
3. Run **Failover Cluster Manager** from any node within the cluster.

   Click ***Start***, type `Failover`, and then click ***Failover Cluster Manager***.
4. Expand the tree and select ***Roles***.
5. Right click on the ***NVR-AS*** role, click ***Move > Select Node…***.
6. Select the node where the NVR-AS has just been installed, then click ***OK***.
7. Move ownership back to the first node by right clicking on the NVR-AS role, click ***Move > Select Node…***.
8. Select the first node, then click ***OK***.

Updating the configuration

The configuration settings of the IndigoVision NVR-AS are replicated between nodes when running in a cluster. When looking to configure the NVR-AS software using NVR-AS Administrator you should follow these steps:

1. Run **Failover Cluster Manager**.

   Click ***Start***, type `Failover`, and then click ***Failover Cluster Manager***.
2. Expand the tree and select ***Roles***.
3. Identify the current ***Owner Node***.
4. On the node that is the current ***Owner Node***, run NVR-AS Administrator.

   Click ***Start***, type `NVR-AS`, and then click ***NVR-AS Administrator*** .
5. Complete the NVR-AS Administrator wizard, providing the desired new settings:
   a. On the **Identification** page enter the appropriate settings, then click ***Next***.
   b. On the **Storage Locations** page enter the appropriate settings, then click click ***Next***.
   c. On the **Network Settings** page enter the appropriate settings, then click ***Next***.
   d. On the **Disk Space Management** page enter the appropriate settings, then click ***Next***.

      Click ***Yes*** to any warnings.
   e. On the **Alarm and Data Record Management** page enter the appropriate settings, then click ***Next***.
   f. On the **Email Settings** page enter the appropriate settings, then click ***Next***.
   g. On the **Finish** page ensure that ***Yes, I would like to restart the NVR-AS service*** is enabled, then click ***Finish***.
   h. Click ***Finish*** to complete the installation process.

Maintenance and upgrading

When performing maintenance, for example when upgrading the version of NVR-AS software, it is possible to reduce downtime and keep the NVR-AS service running by manually moving the service to the second node.

To upgrade the version of NVR-AS software follow these steps:

1. Run **Failover Cluster Manager**.

   Click ***Start***, type `Failover`, and then click ***Failover Cluster Manager***.
2. Expand the tree and select ***Roles***.
3. Identify the current ***Owner Node***.
4. On the node that is not the current ***Owner Node***, display the NVR-AS Administrator.
   - ► See "Step 2: Install the NVR-AS" on page 30 steps 1-6.
5. Complete the NVR-AS Administrator wizard, using the default settings:
   a. On the **Identification** page, click ***Next***.
   b. On the **Storage Locations** page enter temporary locations on the local drive, then click ***Next***.

      Click ***OK*** to any warnings.
   c. On the **Network Settings** page, click ***Next***.
   d. On the **Disk Space Management** page, click ***Next***. Click ***Yes*** to any warnings.
   e. On the **Alarm and Data Record Management** page, click ***Next***.
   f. On the **Email Settings** page, click ***Next***.
   g. On the **Finish** page, click ***Finish***.
   h. Click ***Finish*** to complete the installation process.
6. Run Windows Services.

   Click ***Start***, type `Services`, and then click ***Services***.
7. Right click on ***IndigoVision NVR-AS***, then click ***Stop***.
8. Close Windows Services.
9. Run **Failover Cluster Manager**.
10. Expand the tree and select ***Roles***.
11. Right click on the NVR-AS role, click ***Move > Select Node...***.
12. Select the node where the NVR-AS has just been updated, then click ***OK***.
13. Repeat steps 4 to 12 for the node no longer running the NVR-AS service.
14. Optionally move the NVR-AS role back to your preferred node.

Troubleshooting NVR-AS in a high-availability cluster

Use the following sections to correct errors in the NVR-AS configuration.

Unable to perform any operations within Failover Cluster Manager

Ensure that you are logged in to the server as domain administrator. If you are not logged in as a domain administrator then a warning is displayed when the **Failover Cluster Manager** is started and the ability to validate, create or edit clusters is not enabled.

The NVR-AS role fails to start

Ensure that the role has the following resources:

- Storage: Two disks
- Roles: IndigoVision NVR-AS
- Server Name: Name of your role. Expand to show IP address.

View the **Properties** of the resource IndigoVision NVR-AS and check the **Dependencies**. This should include the storage, server name and IP address.

Run NVR-AS Administrator on the node currently set as the owner. Ensure that the correct **Video** and **Configuration** storage locations are used and the IP address configured, matches the IP address listed within the resources of the NVR-AS role.

Details of devices are inconsistent

View the Properties of the resource IndigoVision NVR- AS and verify that the registry settings have been set for the resource IndigoVision NVR- AS. Perform the process to update the configuration.

► For more information, *see "Updating the configuration" on page 99*.

Cluster does not failover as expected

On the first failure the IndigoVision NVR- AS service restarts on the same node. If the restart attempt fails or a second failure occurs within 15 minutes, the IndigoVision NVR-AS, and all resources, failover onto the second node.

If 10 failures occur within an hour the cluster service is deemed to have failed and will remain in a stopped state.

F HTTPS TECHNICAL NOTES

Control Center is capable of secure communications with ONVIF cameras that support HTTPS, including ONVIF Core Spec Ver. 19.06, sections 7.3.2.3 and 8.1.2.2.

TLS versions

The Control Center suite supports the TLS cryptographic protocol versions 1.0 to 1.3. The SSL cryptographic protocol has been deprecated due to security weaknesses and is not supported.

Certificates

The Control Center suite supports Certificate Authority (CA) and self-signed certificates. CA certificates are not validated. The use of HTTPS still provides security of traffic between endpoints using encryption; however it cannot be used to provide non-repudiation[1].

Streaming over HTTPS

HTTPS support in the Control Center suite includes both ONVIF communication and video and audio streaming.

To stream or record video using HTTPS from a camera which supports HTTPS, cameras must be configured to use a **Firewall Friendly – RTP/RTSP/HTTPS/TCP** connection in Control Center.

Some cameras reporting HTTPS support may only support ONVIF communication over HTTPS. In this situation the Control Center suite will use HTTPS for ONVIF communication and HTTP for video and audio streaming.

Sending audio to a Camera

Audio sent to a camera by Control Center, or the NVR-AS, is not sent over HTTPS.

Alarm server configuration tool

When using the Alarm Server Configuration Tool to create detectors for ONVIF cameras, the cameras must first be set to HTTPS only. If the camera is configured to use HTTP and HTTPS, the detectors will use HTTP.

[1] Non-repudiation is the assurance that someone cannot deny the validity of something.

IndigoVision recommends that you disable HTTP support on a camera when enabling HTTPS support and that this is done before creating any detectors.

Camera compatibility

When configured to use HTTPS, the Control Center suite makes best efforts to do so. However, it is limited by camera behavior.

Some cameras report HTTPS support but actually use HTTP. In this situation, the Control Center suite will use HTTP. IndigoVision recommends contacting your camera supplier to address this issue.

How to enable HTTPS for a new site database

To enable HTTPS for a new site database, do the following:

1. Enable HTTPS on each camera for ONVIF communication and streaming.

   If the camera supports it, you can choose to use both HTTP and HTTPS to minimize down time. This allows the camera to be used by any existing HTTP sites and be added to the new site as HTTPS.
2. Create a new Site Database using the Site Database Server Setup tool.

   Select that support for HTTPS for communication with cameras is to be enabled for the database.
3. Start Control Center.
4. Add each new HTTPS camera to the site.
5. Configure each camera, or the parent site, to use Firewall-friendly for Live Video and Recording.
6. Check for the lock icon in the HTTPS column of the Device List.

   In Setup mode, select the site containing the camera you are interested in, and select the ***Devices*** tab in the main window.

   Ensure the camera is correctly configured to use HTTPS for live video.
7. Create a recording job on the camera, ensuring that Firewall-friendly is selected.
8. Check for the lock icon in the HTTPS column of the Recording Schedule.

   In Setup mode, select the camera you are interested in, and select the ***Recording Schedule*** tab in the main window.

   Ensure the camera is correctly configured to use HTTPS for live video.
9. Optionally, configure the camera to use HTTPS only if both HTTP and HTTPS was configured.

Notice *Existing recording jobs, detectors, or actions created before this process will not be configured to use HTTPS.*