

IndigoVision Site Database Server

Administrator Guide

THIS MANUAL WAS CREATED ON WEDNESDAY, DECEMBER 21, 2022.

DOCUMENT ID: IU-SDS-MAN001-11

Legal Considerations

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

Copyright

COPYRIGHT © INDIGOVISION LIMITED. ALL RIGHTS RESERVED.

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

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

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

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

Contact address



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

Table of Contents

	Legal Considerations	2
	Copyright	2
	Contact address	2
1	About this guide	5
	Safety notices	5
2	Site Database Server overview	7
	Site database overview	7
	Segmented site database	7
3	Installation	9
	Choosing the location of the site database	9
	System requirements	9
	Install the Site Database Server	10
	Create a new site database	11
	Modify or use an existing site database	13
	Upgrade from a Control Center 16 site database	14
4	Failover Site Database	17
	Configuring a failover Site Database Server	18
	Configuring Control Center to use a failover site database	19
5	Operations	21
	Add segments to an existing Control Center site database	21
	Remove segments from an existing Control Center site database	22
	Change the Site Database Server Administrator username or password	22
	Changing session duration for Keep me logged in	23
	Change the address or port used by the Site Database Server	23
	Back up and restore the Control Center site database	24
	Restore the Site Database Server after a hardware failure	25
	Request a new certificate from a third party Certificate Authority (CA)	26
	Replace the certificate used by the Site Database Server	26
	Upgrade from Control Center 15 or earlier	27
	Re-configure a failover Site Database Server	28
	Generate a service authentication token for use by Control Center Web or other services ..	29
	Change the service authentication token	29
6	Troubleshooting	31
	Control Center cannot connect to the Site Database Server or Site Database Files	31
	Site Database Server is unavailable	31
	The Site Database Server certificate is untrusted	31
	No issue with the Site Database Server connection is reported	32

	The Site Database Server Setup tool warns about the security of a certificate	32
	Error “Service ‘IndigoVision Site Database Server’ (IVSDS) could not be installed” during installation	32
	Failure to configure the failover Site Database Server	32
7	Firewall	35

1 ABOUT THIS GUIDE

This guide is written for users of IndigoVision Site Database Server. It provides installation and configuration information for the system, as well as a description of the hardware and details of operation.

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

Safety notices

This guide uses the following formats for safety notices:



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



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



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



Additional information relating to the current section.

2

SITE DATABASE SERVER OVERVIEW

The Control Center suite is made up of multiple products which work together to provide a complete end-to-end IP security solution. The IndigoVision Site Database Server provides:

- A secure store for the Control Center site database.
- An authentication service for the Control Center operators and administrators.
- Resilience to hardware failures through use of a failover Site Database Server.

Site database overview

The Control Center site database stores the site configuration information.

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.

IndigoVision recommends hosting 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 see *"Add segments to an existing Control Center site database" on page 21*.

3

INSTALLATION

This section details how to install the Site Database Server.

- For more information on installing the complete Control Center system, refer to the "IndigoVision Control Center Installation 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.*

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 2019 (recommended)
- Windows Server 2016
- Windows Server 2012 R2

- Windows 11
- Windows 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.



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 13*
 - **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 11*
 - **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 *"Upgrade from a Control Center 16 site database" on page 14*

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 27*
 - **Configure as a failover Site Database Server**
 - For more information on configuring a failover Site Database Server, see *"Failover Site Database" on page 17*
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**.



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 Site Database Server, see *"Request a new certificate from a third party Certificate Authority (CA)" on page 26*
 - For more information on changing certificates for the Site Database Server, see *"Replace the certificate used by the Site Database Server" on page 26*
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" in "IndigoVision Control Center Installation Guide".
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**.
 - For more information on creating certificates for the Site Database Server, see *"Request a new certificate from a third party Certificate Authority (CA)" on page 26*,

- For more information on changing certificates for the Site Database Server, see *"Replace the certificate used by the Site Database Server" on page 26.*
- 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 Site Database Server Setup tool to automatically migrate your old site database.

1. In Site Database Server 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 Site Database Server.
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 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**.



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 Site Database Server, see *"Request a new certificate from a third party Certificate Authority (CA)" on page 26.*
 - ▶ For more information on changing certificates for the Site Database Server, see *"Replace the certificate used by the Site Database Server" on page 26.*
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 Site Database Server Setup tool.

4

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.*

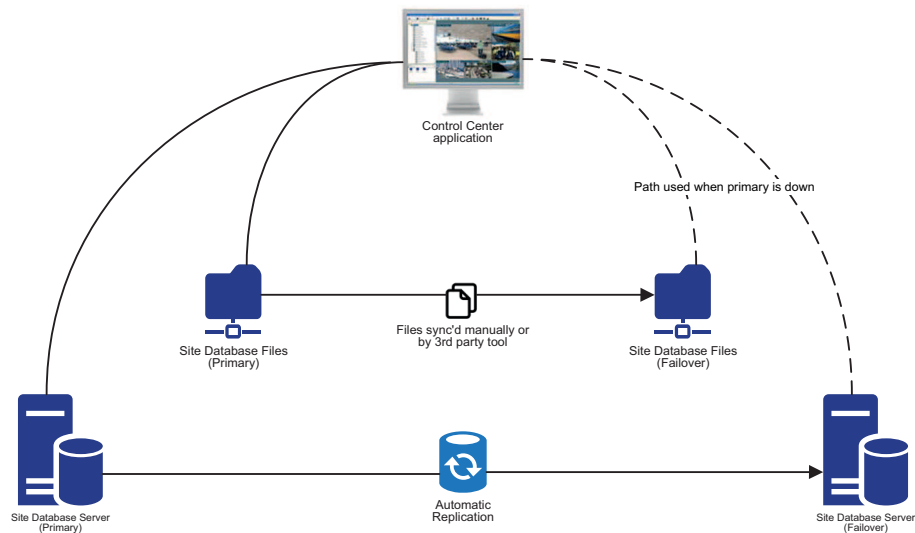


Figure 1: Network configuration with the failover Site Database Server

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 *"Installation" on page 9*
2. Ensure that there is no firewall blocking access to the MongoDB service on the primary server.
 - For more information, see *"Firewall" on page 35*
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)" on page 26*
 - For more information on changing certificates for the Site Database Server, see *"Replace the certificate used by the Site Database Server" on page 26*.
- 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.*

Configuring Control Center to use a failover site database

After the failover site database files and failover Site Database Server have been configured, each Control Center workstation must be configured to use the failover when the primary site database is unavailable.

To configure the Control Center front-end application to use a failover site database:

1. Run the Control Center Setup tool from **Start > IndigoVision > Control Center Setup**.
2. On the **Site Database** page, modify the existing primary site database details if necessary, then click **Next**.
3. After the primary Site Database Server has been tested, click **Next** to continue.
4. The **Failover Site Database** page is shown.
5. Select **Specify a failover site database** and then enter the details of the failover Site Database Server and Site Database Files directories.
6. Click **Next** and the **Testing Failover 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.

After updating the Control Center front-end application with a configured failover site database, it is worthwhile testing the failover by temporarily shutting down or disconnecting the primary Site Database Server, then logging into Control Center.

5

OPERATIONS

This chapter describes common tasks required for the administration of the Site Database Server.

Add segments to an existing Control Center site database

An existing site database can be divided into a segmented site database in order to increase system scalability or partition responsibility among administrators and operators. For more information refer to see *"Segmented site database" on page 7*.

Notice

If this is the first time segments have been added to the site database, the site database becomes a segmented site database. The login behavior will change in the Control Center front-end application such that administrators must choose a specific segment on login if they wish to modify the database.

**Warning**

If there is more than one segment in the database, and the system is not licensed for segmented site databases, users will not be able to login to Control Center until the license is upgraded or all but one of the segments are removed.

To add one or more new empty segments to an existing database:

1. Open the Windows Start menu and select **IndigoVision > Site Database Server Setup**.
If you have a failover Site Database Server, it is the primary server where the tool should be run.
2. In the Site Database Server Setup tool, click **Next**.
3. Select **Configure segments for an existing site database** and click **Next**.
4. On the Add or Remove Segments page, enter the number of segments that you wish to add.
5. Click **Next** and the tool will make the changes to the site database.
6. Click **Finish** to close the tool.
The new segments will be automatically named with a number such as "Segment 003".
7. Login to the new segments as an administrator using the Control Center front-end application to populate the new segments, change their names, or change the access permissions..

Remove segments from an existing Control Center site database

Existing segments in a segmented site database can be removed if there are already multiple segments in the site database.



Removing segments from the site database cannot be reversed unless you have taken a suitable backup of the site database.



If there will only be one segment left after removal, the database is no longer treated as a segmented site database. In this case, a segment choice will not be presented during login in the Control Center front-end application and the segment access properties will not be accessible. Before proceeding, ensure the appropriate users have segmented access permissions for the remaining segment or they will not be able to log in to Control Center. Refer to the Control Center Help for more information on configuring segment access.

To remove a segment from an existing database:

1. Open the Windows Start menu and select **IndigoVision > Site Database Server Setup**.
If you have a failover Site Database Server, it is the primary server where the tool should be run.
2. In the Site Database Server Setup tool, click **Next**.
3. Select **Configure segments for an existing site database** and click **Next**.
4. On the Add or Remove Segments page, select the **Remove segment option** then carefully choose the segment that you wish to remove from the list, then click **Next**.
 - a. If there will only be one segment left after removal a warning is displayed.
Choose to continue by clicking **Next** or cancel by clicking **Cancel**.
5. Click **Finish** to close the tool.

Change the Site Database Server Administrator username or password

The Site Database Server Administrator account is used by the Site Database Server to access the database and protects the data from rogue users with access to the host operating system. IndigoVision recommend that these credentials are changed regularly.

To change the Site Database Server Administrator username or password:

1. Open the Windows Start menu and select **IndigoVision > Site Database Server Setup**.
If you have a failover Site Database Server, it is the primary server where the tool should be run.
2. In the Site Database Server Setup tool, click **Next**.
3. Select **Change the Site Database Server administrator password** and click **Next**.
4. On the Site Database Server Administrator page, enter the current username and password for the Site Database Server administrator, and click **Next**.

These are the credentials specified when the database was originally created with this tool, or when you last changed them following this procedure.

5. Enter the new username and password for the Site Database Server administrator, then click **Next**.
6. 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.
7. The configuration changes are applied.
To close the application, click **Finish**.
8. If there is a failover Site Database Server configured, you must also reconfigure it after changing the credentials to keep the database synchronized.
 - For more information, see *"Re-configure a failover Site Database Server"* on page 28

Changing session duration for Keep me logged in

After logging into your Control Center session with **Keep me logged in** selected, it remains active for 30 days without re-logging into Control Center. Each time you start a Control Center session, the session is extended for 30 days from the point you started.

If it is more than 30 days since you last logged in, the session expires and you will need to re-enter your credentials. It is possible to change the default 30 days for the active session.

To override the default 30 days session duration, do the following:

1. From the Windows start menu, type `REGEDIT`.
The **Registry Editor** opens.
2. Navigate to **HKEY_LOCAL_MACHINE\SOFTWARE\IndigoVision\Site Database Server**
3. Create a **DWORD** called **AuthenticationCookieDurationSeconds**
4. Edit the **DWORD** and specify the session duration to be used.
The **DWORD** key and duration is specified in seconds. For example, 30 days would be 2592000 seconds.
5. Close the **Registry Editor**.
6. Restart the Site Database Server after editing the registry key.

Notice *The registry key should be set on the system running the Site Database Server.*

Change the address or port used by the Site Database Server

If the network environment for the Site Database Server changes, you may want to adjust the IP address and port that it binds to.

Notice *If you change the binding address for the Site Database Server, any Control Center workstations configured to connect using the IP address, rather than a DNS address, will need to be reconfigured as well. Consider using fully qualified domain names for the Site Database Server when configuring Control Center to avoid this in the future.*

To change the address or port used by the primary Site Database Server, perform the following operations:

1. Open the Windows Start menu and select **IndigoVision > Site Database Server Setup**.
2. In the Site Database Server Setup tool, click **Next**.
3. Select **Use an existing site database**.
4. Leave the **Site Database Location** page unchanged and click **Next**.
5. Leave the **License Server** page unchanged and click **Next**.
6. On the **Network Binding** page, perform one of the following actions:
 - Choose the IP address on the local PC that the Site Database Server will bind to.
 - Choose **All** to bind to all addresses.

The IP and Port selected here must be accessible to all Control Center workstations in the system.
7. Continue through the wizard to the final page.
8. After the configuration is completed, click **Finish** to close the Site Database Server Setup tool.
9. If there is a failover Site Database Server configured, and it was using the old IP address rather than a DNS hostname for the primary Site Database Server, you must reconfigure it after changing the IP address to keep the database synchronized.
 - For more information, see *"Re-configure a failover Site Database Server" on page 28*
10. Update any installations of the Control Center front-end application to use the new Site Database Server address and port using the Control Center Setup tool on each workstation.

To change the address or port used by a failover Site Database Server:

1. To change the IP address or port, see *"Re-configure a failover Site Database Server" on page 28*
2. Update any installations of the Control Center front-end application to use the new failover Site Database Server address and port using the Control Center Setup tool on each workstation.

Back up and restore the Control Center site database

You can make back ups without interruption to the Site Database Server service. To back up or restore the Control Center site database, perform the following operations:

Notice *When restoring the database, you will also need the Site Database Server Administrator username and password.*

To back up the Control Center site database:

1. Open an administrator command prompt on the server where the primary Site Database Server was installed.

2. Navigate to the directory that contains ***mongodump.exe***.

Typically, the path is ***C:\Program Files\MongoDB\Server\4.2\bin***.

3. To get a backup of the site database, execute the following command:

```
mongodump.exe --host="127.0.0.1:8134" -u="<SDS administrator username>" -p="<SDS administrator password>" --ssl --tlsInsecure
```

4. After the command has completed, create a copy of output folder generated by ***mongodump.exe***.

Typically, the output folder path is ***dump/***.

To restore a backup of the Control Center site database:

Notice *Any changes made to the Control Center Site Database since the backup will be lost in this process.*

1. Create a new site database using Site Database Server Setup tool.

2. Navigate to the directory that contains ***mongorestore.exe***

Typically, the path is ***C:\Program Files\MongoDB\Server\4.2\bin***.

3. Copy the output folder, generated by ***mongodump.exe***, into the same directory as ***mongorestore.exe***.

4. To restore the dump of the site database, execute the following command:

```
mongorestore.exe --host="127.0.0.1:8134" -u="<SDS administrator username>" -p="<SDS administrator password>" --ssl --drop --preserveUUID --tlsInsecure dump/
```

The database will be restored from the dump output folder.

5. Restart the IndigoVision Site Database Server and the MongoDB Server services.
6. Restart any instances of Control Center that use the Site Database Server that has been replaced.

Notice *To fully back up a Control Center site database, both the Site Database Server and the Site Database Files must be backed up. Ensure that you make regular copies of the Site Database Files alongside backups of the Site Database Server.*

As the Site Database Files are stored as a regular Windows directory and file share, you can back them up using a third-party solution.

Restore the Site Database Server after a hardware failure

If the Site Database Server host PC has failed and needs to be rebuilt from a backup of the database, follow this procedure.

1. Copy the backed up Site Database Server database directory to the new PC.
2. Install the Site Database Server, following the steps to “Modify or use an existing site database”.
 - For more information, see *"Modify or use an existing site database" on page 13*
3. If the same PC was used to host the Site Database Files, it can be recovered by copying the backed up directory and creating a new Windows file share.

4. If a new self-signed certificate has been generated, install it on each Control Center workstation that will use the Site Database Server.
 - a. On each Control Center workstation, from the Start menu: **IndigoVision > Control Center Setup** run the Control Center Setup tool.
 - b. To proceed to the **Testing Connection** page, click **Next**.
If the certificate is not trusted by the workstation, you can install it here by clicking **Install Certificate**.
 - For more information, refer to the "IndigoVision Control Center Installation Guide"

Request a new certificate from a third party Certificate Authority (CA)

IndigoVision recommend that the Site Database Server is secured with a certificate from a trusted CA.

1. Use the CA's recommended tooling to request a new certificate and ensure that:
 - a. The private key is at least 2048 bits in length.
 - b. The **Common Name (Subject)** field matches the address (IP address or hostname) that Control Center workstations will use when connecting to the Site Database Server.



Subject Alternate Name fields can also be used for Control Center workstations using Windows 10 or later.

- c. The **Enhanced Key Usage** field contains Server Authentication (1.3.6.1.5.5.7.3.1).
 - d. The PC that will host the Site Database Server generates the request, or that the private key is later imported to that PC.
2. When you have a .pfx or .cer file from the CA, install the certificate on the Site Database Server PC.
 - a. Double-click on the certificate file (.pfx or .cer).
 - b. In the **Windows Certificate** dialog, click **Install Certificate...** to open the Certificate Import Wizard.
 - c. Select **Local Machine**, then click **Next**.
 - d. When asked to confirm that the application can make changes to your device, click **Yes** to continue.
 - e. Allow the tool to determine the correct certificate store and complete the import wizard by clicking **Next**, then **Finish**.
3. Now that the certificate is installed, you can choose it from the Site Database Server Setup tool.
 - For more information, see *"Replace the certificate used by the Site Database Server" on page 26*

Replace the certificate used by the Site Database Server

To choose a different certificate to use with the Site Database Server, for example when your existing certificate is expiring, or after you have received a certificate from a trusted CA, follow these steps.

If this is a primary Site Database Server:

1. To use the new certificate, from **Start > IndigoVision > Site Database Server Setup** run the Site Database Server Setup tool.
2. To open the **Site Database Configuration** page, click **Next**.
3. Ensure the **Use an existing site database** option is selected.
4. Proceed through the wizard clicking **Next** until you get to the **Server Certificate** page.
5. To choose a different certificate, click **Browse**, then **More choices** to find the new certificate.
Certificates stored in the local machine certificate store that are not expired are listed here.
6. To close the Windows security dialog, click **OK**.
7. Proceed to the end of the Site Database Server Setup tool by clicking **Next**.
8. To close the application, click **Finish**.
9. If this is a failover Site Database Server, it must be re-configured as a failover with the new certificate.
 - For more information, see "Re-configure a failover Site Database Server" on page 28

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, see Control Center Installation Guide
-

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.

Re-configure a failover Site Database Server

If the primary Site Database Server IP address, Site Database Administrator credentials, or database location is changed, then the failover Site Database Server must be re-configured to continue synchronizing.

To re-configure the failover Site Database Server:

1. On the failover Site Database Server PC, run the Site Database Server Setup tool from **Start > IndigoVision > Site Database Server Setup**.
2. On the **Site Database Configuration** page, choose to **Configure as a failover Site Database Server** and click **Next**.
3. On the primary **Site Database Server connection** page enter the address, username and password for the primary Site Database Server.
4. 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.
5. On the **New failover Site Database Location** page, enter a new location on this PC where the site database server will store the data synchronized from the primary.

Notice *You must choose a new location for the failover database each time the failover Site Database is configured.*

6. On the **Network Binding** page, choose the IP address 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.
7. On the **Server Certificate** page, optionally change 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)" on page 26*,
 - For more information on changing certificates for the Site Database Server, see *"Replace the certificate used by the Site Database Server" on page 26*.
8. 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.
9. After the configuration is completed, click **Finish** to close the Site Database Server tool.

Generate a service authentication token for use by Control Center Web or other services

A service authentication token is needed for use by Control Center Web and other services that access the site database through IndigoVision SDKs.

There is no need to generate a service authentication token if you are not using Control Center Web or another product which instructs you to do as part of its installation and configuration process.

To generate a service authentication token, follow these steps:

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 when configuring the service that requires authenticated access to the site database, for example, Control Center Web.
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.

Change the service authentication token

If you are using a service, for example, Control Center Web, that requires a service authentication token, it is good practice to change the token on a regular basis.

Notice	<i>When changing the service authentication token, any existing services using the old token will not be able to access the Control Center site database until the service is reconfigured with the new token.</i>
---------------	--

To change the service authentication token follow the steps to generate a service authentication token, see *"Generate a service authentication token for use by Control Center Web or other services"* on page 29. The existing token is replaced with the new token when the changes are applied.

6 TROUBLESHOOTING

Control Center cannot connect to the Site Database Server or Site Database Files

If the Control Center front-end application cannot connect to the Site Database Server or Site Database Files, it will not start unless the Control Center user has permission for caching the site database.

To diagnose this problem, perform the following operations:

1. On the workstation where the Control Center front-end application is installed, access **Start menu > IndigoVision > Control Center Setup** to run the Control Center Setup tool.
2. To progress to the Site Database page, click **Next**.
3. Check that the configured address and port for the Site Database Server and the location of the Site Database Files directory are correct and accessible over the network.
4. Click **Next**.

The tool will test the connection to the Site Database Server. Further steps depend on the problem that was detected.

Site Database Server is unavailable

If the Site Database Server is unavailable, perform the following operations:

1. Check that there is a valid network route from the workstation to the server and that all firewalls are correctly configured.
2. Check that the Site Database Server service is running on the Site Database Server PC:
 - a. On the Site Database Server PC, click on the **Start** menu and type `services.msc` to open the Windows services applet.
 - b. Check that **IndigoVision Site Database Server** is running and start it if is not.
 - c. If the service will not start, re-run the Site Database Server Setup tool (**Start menu > IndigoVision > Site Database Server Setup**) and check that the configuration is correct.

The Site Database Server certificate is untrusted

If the Site Database Server certificate is untrusted, perform the following operations:

1. View the certificate and check it has not expired or changed unexpectedly
If the certificate has expired, you need to install a new certificate on the Site Database Server.

- For more information, see *"Replace the certificate used by the Site Database Server" on page 26*
- 2. If not already done so, install the certificate on the workstation by clicking the **Install Certificate** button.

No issue with the Site Database Server connection is reported

If the Control Center Setup tool does not report any problems connecting to the Site Database Server, check the following:

- Are the clocks of the Site Database Server and Control Center workstation synchronized?
 - If the clocks are more than 5 minutes apart, it is not possible to log in to Control Center.
- IndigoVision recommend that all devices, including workstations and the PC hosting the Site Database Server, are synchronized using NTP.
 - For more information, refer to *Installing a Windows NTP Server* in the Control Center Installation Guide.
- Check that there is a stable network connection between the Control Center workstation, Site Database Files directory and the Site Database Server.

If you continue to experience difficulties, contact IndigoVision Technical Support for more assistance.

The Site Database Server Setup tool warns about the security of a certificate

When running the Site Database Server Setup tool, the application checks that the local Operating System trusts the server certificate. If the certificate is revoked by the CA, or is self-signed or has other such security issues, a warning is shown after the **Server Certificate** page.

It is still possible to use the certificate with Control Center and the Site Database Server, if it meets specific criteria. However, IndigoVision recommend that a certificate from a trusted CA is used instead.

- For the list of criteria the certificate needs to meet, see *"Request a new certificate from a third party Certificate Authority (CA)" on page 26*

Error "Service 'IndigoVision Site Database Server' (IVSDS) could not be installed" during installation

When installing, upgrading or uninstalling the Site Database Server, if the following error is shown:

```
Service 'IndigoVision Site Database Server' (IVSDS) could not be installed
```

Check if the Windows services applet is open and close it, then click the **Retry** button to continue.

Failure to configure the failover Site Database Server

If you experience difficulty configuring a failover Site Database Server, check the following:

- Is the primary Site Database Server available on the network from the failover PC?
- Is there a firewall blocking access to the MongoDB service on either the failover or the primary PC?
 - For more information, see *"Firewall"* on page 35
- For more information on failover Site Database Server, see *"Failover Site Database"* on page 17

7

FIREWALL

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 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

Additional ports may be required for Windows services including access to network drives for the Site Database Files.