

IndigoVision

IndigoReports

Administrator Guide

THIS MANUAL WAS CREATED ON WEDNESDAY, APRIL 7, 2021.

DOCUMENT ID: IU-IR-MAN001-7

Legal Considerations

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

Copyright

COPYRIGHT © INDIGOVISION LIMITED. ALL RIGHTS RESERVED.

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

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

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

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

Contact address



IndigoVision Limited
Charles Darwin House,
The Edinburgh Technopole,
Edinburgh,
EH26 0PY

TABLE OF CONTENTS

| | | |
|----------|---|-----------|
| | Legal Considerations | 2 |
| | Copyright | 2 |
| | Contact address | 2 |
| 1 | About this guide | 5 |
| | References | 5 |
| | Safety notices | 5 |
| 2 | Overview | 7 |
| | IndigoReports and the IndigoVision Distributed Network Architecture | 7 |
| | VMS reporting | 7 |
| | Audit logs | 8 |
| | Security incident reporting | 8 |
| | Prerequisites | 8 |
| | Software | 8 |
| | Hardware | 8 |
| | Network connectivity | 9 |
| 3 | Installation | 11 |
| | Preliminary steps | 11 |
| | Check your IndigoReports License | 11 |
| | Prepare the server to install IndigoReports | 11 |
| | Prepare Control Center | 11 |
| | Installing the server component of IndigoReports | 12 |
| | Troubleshooting installation errors | 13 |
| | Preparing IndigoReports for Control Center Audit Logging | 13 |
| | Prepare IndigoReports for compatibility with earlier versions of Control Center | 14 |
| 4 | Initial setup | 17 |
| | Accessing IndigoReports and logging in for the first time | 17 |
| | Access IndigoReports from another computer | 17 |
| | Access IndigoReports on the IndigoReports server | 17 |
| | Log in to IndigoReports | 17 |
| | Licensing | 17 |
| | Auto | 18 |
| | Manual | 19 |
| | Extend | 20 |
| | Creating a user account | 20 |
| | To create a new user account | 20 |
| | Connecting IndigoReports to the Control Center site database | 20 |
| | To connect IndigoReports to the Control Center site database | 20 |
| | To troubleshoot the IndigoReports connection to the Control Center site database ... | 21 |

| | | |
|----------|--|-----------|
| 5 | Using IndigoReports | 23 |
| | Navigating the IndigoReports interface | 23 |
| | Available modules | 23 |
| | To change modules | 23 |
| | Global reporting features | 23 |
| | Filtering reports and searches | 23 |
| | Sending reports by email | 24 |
| | Downloading reports | 24 |
| | VMS Reporting module | 24 |
| | My Reports | 24 |
| | Canned Reports | 25 |
| | Audit Report | 25 |
| | Health Report | 26 |
| | Inventory Report | 27 |
| | Detector Report | 28 |
| | CyberVigilant Report | 29 |
| | Recording Report | 30 |
| | System Administration module | 31 |
| | User roles | 31 |
| | Lists | 32 |
| | Site database connection | 32 |
| | SMTP Settings | 33 |
| A | HTTPS Certificates | 35 |
| | Installing a trusted certificate (recommended) | 35 |
| | Generate the CSR | 35 |
| | Install the signed certificate | 36 |
| | Trusting the IndigoReports server's built-in certificate authority | 36 |
| | Obtain the built-in certificate authority's HTTPS certificate | 37 |
| | Generating a new certificate if your server's host name changes | 37 |

1 ABOUT THIS GUIDE

IndigoReports is a Control Center add-on application used for reporting purposes.

The guide covers the following topics:

- Prerequisites
- Installation and configuration of IndigoReports
- Usage of IndigoReports

References

- IndigoVision website: <https://www.indigovision.com/>

Safety notices

This guide uses the following formats for safety notices:



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



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

Notice

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



Additional information relating to the current section.

2

OVERVIEW

IndigoReports is a web-based application consisting of the IndigoReports server and web-browser clients.

IndigoReports and the IndigoVision Distributed Network Architecture

This section describes how IndigoReports fits in and interacts with the other components of the IndigoVision Distributed Network Architecture (DNA).

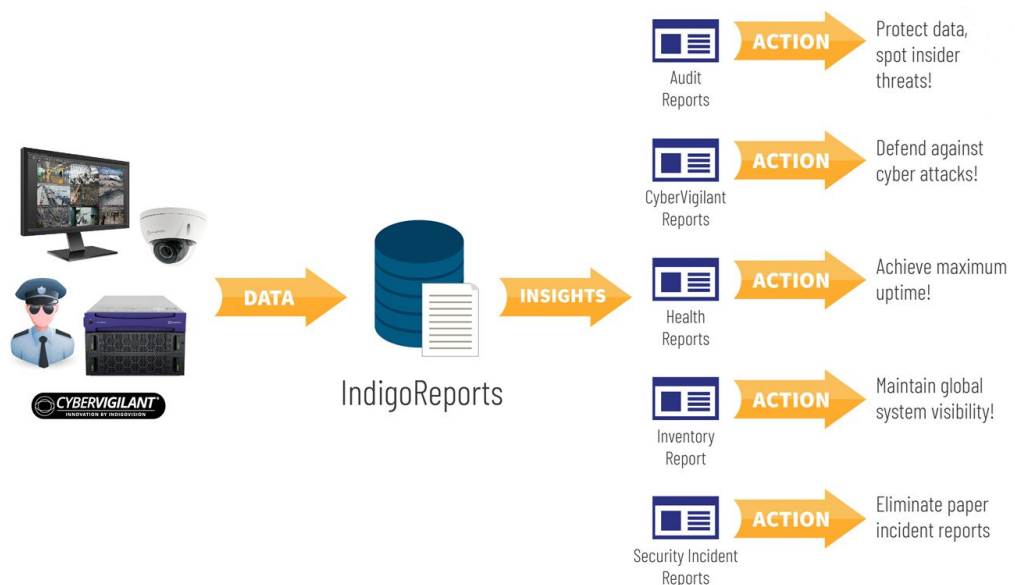


Figure 1: How IndigoReports works

VMS reporting

IndigoReports learns about your Control Center video management system (VMS) by communicating with the site database. After connection to the Control Center Site Database, IndigoReports periodically gathers updated information from your cameras, NVR-AS, and CyberVigilant to enable system inventory, health, and cyber-security reporting.



IndigoReports is designed to communicate with a single site database. Therefore, you need a single IndigoReports server and a single IndigoReports license for use with the Control Center Site Database – regardless of the number of cameras, NVRs, or user accounts.

Audit logs

IndigoReports also provides a self-contained audit logging system for Control Center, eliminating the need for you to deploy your own database servers. After installation, Control Center can be configured to log administrator and operator actions to IndigoReports for unified audit and compliance reporting.

Security incident reporting

The IndigoReports Incident Reporting module contains powerful security incident reporting features. Operators can use customizable forms to capture incident information, narratives, alarm and audit log records from Control Center, and media attachments for evidence.

Incident reporting allows the operators to combine exported video evidence with personal accounts, summaries, and other information that can later be used to support investigations. Media attachments can include artifacts such as documents, photos, videos, or audio files. These reports can be saved, printed, e-mailed, or viewed by the operators who have the appropriate permissions and a web browser.

Prerequisites

Software

System requirements

The IndigoReports server can be installed on the following Windows operating systems:

- Windows 10 (64-bit)
- Windows Server 2012 R2 (64-bit)
- Windows Server 2016
- Windows Server 2019

Supported web browsers

IndigoReports is compatible with the following web browsers:

- Microsoft Internet Explorer 11 or later
- Microsoft Edge 83.0 or later
- Google Chrome 83.0 or later
- Mozilla Firefox 77.0 or later
- Apple Safari 13.1 or later

IndigoVision Control Center

Before installing IndigoReports, you should have an IndigoVision Control Center system installed and running.

Hardware

The IndigoReports server has the following minimum hardware requirements:

- 64-bit Intel processor
- 16 GB RAM minimum

Recommended:

- Hardware RAID controller
- 300 GB storage (or more if Incident Reporting will be used with media attachments)



IndigoVision recommends installing IndigoReports on a robust server platform with redundant hardware and backup.



IndigoReports is compatible with common virtualization software, including VMWare and Microsoft Hyper-V.

Installing IndigoReports on IndigoVision NVR-AS4000 appliances

You can install IndigoReports on IndigoVision NVR-AS4000 appliances that meet the requirements listed in this section, but recording performance may be affected. Therefore, IndigoVision recommends installing IndigoReports on a dedicated server or virtual machine.

A separate storage volume should be created with at least 300 GB capacity so that IndigoReports data directory is not located in the same logical volume as Windows NVR-AS video recording files.

► For more information on storage configuration, refer to the NVR-AS4000 user guide.

Network connectivity

IndigoReports maintains a persistent connection to the Control Center Site Database. It also contacts cameras, NVRs, and alarm servers frequently to maintain updated health and configuration data. If IndigoReports is used for Control Center audit logging, Control Center PCs connect frequently to the IndigoReports server to write audit logs when Control Center is in use.



IndigoVision recommends installing IndigoReports on the same server where the Control Center Site Database is hosted. Such setup allows IndigoReports to access the database files using a local file path.

Connectivity requirements

The following are the firewall port connectivity requirements:

| Application | Service | Protocol | Port | Source | Destination |
|------------------------------|---------------|----------|------|----------------------|---|
| Web interface | HTTPS | TCP | 4398 | Web browser | IndigoReports server |
| Audit logging | MySQL | TCP | 4396 | Control Center | IndigoReports server |
| Control Center Site Database | SMBv2 / SMBv3 | TCP | 445 | IndigoReports server | Windows file share hosting Control Center site database |

| Application | Service | Protocol | Port | Source | Destination |
|--|--------------|----------|------------|------------------------|--|
| NVR information, historical alarms, and data records | IndigoVision | TCP | 8130, 8131 | IndigoReports server | NVRs and Alarm Servers |
| Real-time alarms and detector activations | IndigoVision | TCP | 49303 | NVRs and Alarm Servers | IndigoReports server |
| ONVIF camera details | HTTP/HTTPS | TCP | 80/443 | IndigoReports server | Cameras |
| Customer-initiated 'auto' license request | HTTPS | TCP | 443 | IndigoReports server | IndigoVision Order Management https://www.indigovision.com |

3

INSTALLATION

This section details how to install the server component of IndigoReports.

Preliminary steps

Before installing IndigoReports, you need to have the right information and access to different related systems.

Check your IndigoReports License

Ensure that you have your order number for your IndigoReports license. This number will be referenced by IndigoVision Order Management when activating your IndigoReports license.

Prepare the server to install IndigoReports

IndigoReports requires the following:

- A Windows account on your domain or the server that will host IndigoReports, with permissions for the following:
 - IndigoReports installation
 - Reading the file share that contains the Control Center Site Database
- Network connectivity to and from the file share containing the Control Center site database, as well as all cameras and NVR-AS in your Control Center system.
- .NET Framework 4.7.2 or later must be installed on the server where IndigoReports will be installed.

Prepare Control Center

In Control Center, complete the following steps:

1. Create a new user which will be used by IndigoReports as a Service Account for connecting to the site database.



*IndigoVision recommends assigning the new user to the **Restricted Administrator** role and using a strong password.*

2. If you intend to use IndigoReports for Control Center audit logging, install the latest version of the MySQL ODBC connector on each Control Center PC.
 - A 64-bit (winx64) version is required for Control Center 17.1 and later.
 - A 32-bit (win32) version is required for earlier versions of Control Center.As part of the installation files, two versions of the connector have been provided:

- **mysql-connector-odbc-8.0.21-winx64.msi** (to be used with Control Center 17.1 and later)
 - **mysql-connector-odbc-8.0.21-win32.msi** (to be used with earlier versions of Control Center)
3. Ensure that Control Center PCs and all client PCs, which will access IndigoReports using a web browser, have network connectivity to the IndigoReports server.

Installing the server component of IndigoReports

Follow these steps to install the server component of IndigoReports.

1. Copy the installation files to the server where you intend to install IndigoReports.
2. Run the installer file **Setup.IndigoReports-10.1.x.exe**.
3. Review and agree to the license terms.
4. Choose components to install, and click **Next**.
Recommended installer settings: the default options.
5. Choose install location, and click **Next**.
Recommended location: **C:\Program Files\IndigoVision\IndigoReports**
6. Choose memory options, and click **Next**.
Recommended memory settings: 8 GB.
7. Choose the location of the folder where IndigoReports will store reporting data, and click **Next**.
Recommended location: **C:\Program Files\IndigoVision\IndigoReports\data**.
8. Choose to create desktop icons, and click **Next**.



The installation process creates one desktop shortcut to this documentation.

9. Choose Start Menu Folder.
Recommended option: **IndigoReports**.
10. Click **Install**.
11. After installation is complete, IndigoReports generates a password for the built-in administrator account.
A pop-up window with the password displays.
12. Copy the password to your clipboard and paste it in a password manager or another secure location.



Figure 2: IndigoReports installation: administrator password created



After you click **OK** in the password pop-up window, you can not recover the password.

13. To exit the installer, click **Close**.

If you want to use IndigoReports for Control Center Audit Logging, you need to set up IndigoReports appropriately.

► see "Preparing IndigoReports for Control Center Audit Logging" on page 13

Troubleshooting installation errors

If errors occur during installation, you can save the installation logs as described below:

1. Right-click on the installation window.
2. To copy the installation logs, click **Copy Details to Clipboard**.
3. Paste the installation logs into a document.
4. If you need further assistance, send the document to the Technical Support.

Notice Installation logs contain all messages displayed to the user during installation, including the admin password. IndigoVision recommends handling the log with care: remove the password before sharing, and change the password as soon as possible.

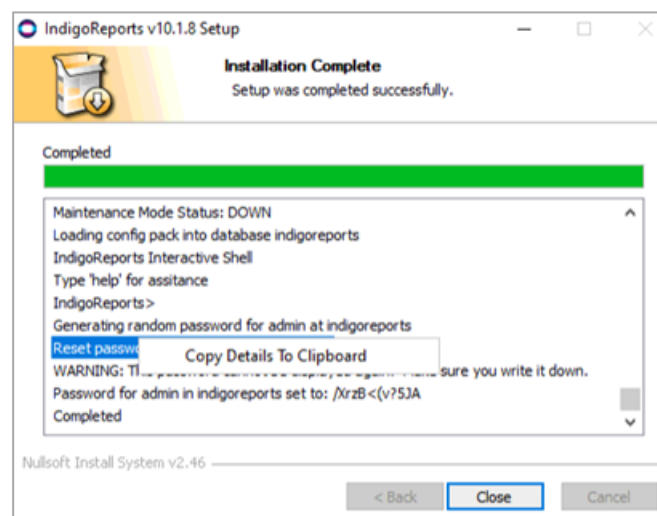


Figure 3: Copying the IndigoReports installation logs to clipboard

Preparing IndigoReports for Control Center Audit Logging

Before you start using IndigoReports for Control Center Audit Logging, you need to set up IndigoReports as follows:

1. Navigate to the IndigoReports program directory, for example, **C:\Program Files\IndigoVision\IndigoReports**.
2. Right-click on **IndigoReports.Shell** and select **Run as administrator**.. This launches the IndigoReports Command Shell.
3. Type command `indigoreports auditcreds`
4. IndigoReports generates ODBC credentials to be configured in Control Center for Audit Logging.

The ODBC username and password are displayed.

5. Highlight the username and password and copy to your clipboard.
6. Paste your password into a password manager or another secure location.



After you close the IndigoReports Command Shell, you can't recover the password.

Notice

If you lose your credentials, you can generate new credentials. The old credentials are automatically disabled.

IndigoReports is now configured for Control Center Audit Logging, and will listen for incoming connections from Control Center on port 4396.

7. Configure Control Center audit logging to the IndigoReports server using the credentials generated in step 4.
- For more information, see "IndigoVision Audit Log Reference Guide"

Prepare IndigoReports for compatibility with earlier versions of Control Center

After installation, IndigoReports is pre-configured for compatibility with Control Center version 17 or later.

If IndigoReports is to be used with an earlier version of Control Center, it must be re-configured for compatibility with versions earlier than version 17. To do this, follow these steps:

1. Navigate to the IndigoReports program directory, for example, **C:\Program Files\IndigoVision\IndigoReports**
2. Right-click on **IndigoReports.Shell** and select **Run as administrator**.
This starts the IndigoReports command shell.
3. Type command `service stop`
4. Edit **overrides.js** located in the IndigoReports data directory, for example, **C:\Program Files\IndigoVision\IndigoReports\data**, or **D:\data**
5. Change `ivexport` version from '17' to '16'.

```
// Package config value overrides (if any)
//
// You can provide new values for anything in the config section
// of the package
// by creating properly named and pathed values here.
//
// Specifically you can change the servers.ivexport.version to
// 16 or 17 depending
// on your control center version. Use 16 for control center
// v16 and lower and
// use 17 for control center version 17 and higher. The default
// is 17.
//
// Any changes made in this file will not be applied until a
// service stop, configure
// and start are done using the shell.
exports.Overrides = {
  servers: {
    ivexport: {
      version: '17'
    }
  }
}
```

6. Save your changes.
7. Type command `service configure`
8. Type command `service start`

If IndigoReports is deployed with a Control Center version earlier than version 17, and Control Center is later upgraded to version 17 or later, step 5 in the above process can be modified so the `ivexport` version is changed from '16' to '17'. After changing the version, continue with the process to complete the Control Center upgrade and to configure IndigoReports for compatibility with version 17 or later.

4 INITIAL SETUP

This section guides you through the initial setup of IndigoReports.

Accessing IndigoReports and logging in for the first time

After installing IndigoReports, you can access the Web interface securely using HTTPS.

Access IndigoReports from another computer

In a supported browser, open the page: `https://your_server_IP_address_or_host_name:4398`



To provide encrypted communications between your browser and IndigoReports by default, a self-signed HTTPS certificate is generated during installation using the server's host name. Most web browsers do not trust self-signed certificates, and display a warning message before allowing you to proceed to the IndigoReports login page. Therefore, IndigoVision recommends installing a trusted certificate provided by a trusted certificate authority or the customer's IT organization.

► For more information, see "HTTPS Certificates" on page 35

After installation, IndigoReports is unlicensed. In such a case, you can log in using the built-in administrator account only.

Access IndigoReports on the IndigoReports server

In a supported browser, open the page: `https://localhost:4398`

Log in to IndigoReports

On the login screen, enter the following credentials:

- Username: `admin`
 - Password: your password generated during the IndigoReports installation.
- The **Licensing Information** page opens.

Licensing

From the **Licensing Information** page, you can choose one of the three options:

- **Auto**: requests a license from the IndigoReports license service.
- **Manual**: used for offline licensing or for new installation.

- **Extend**: used for extending demo licenses.

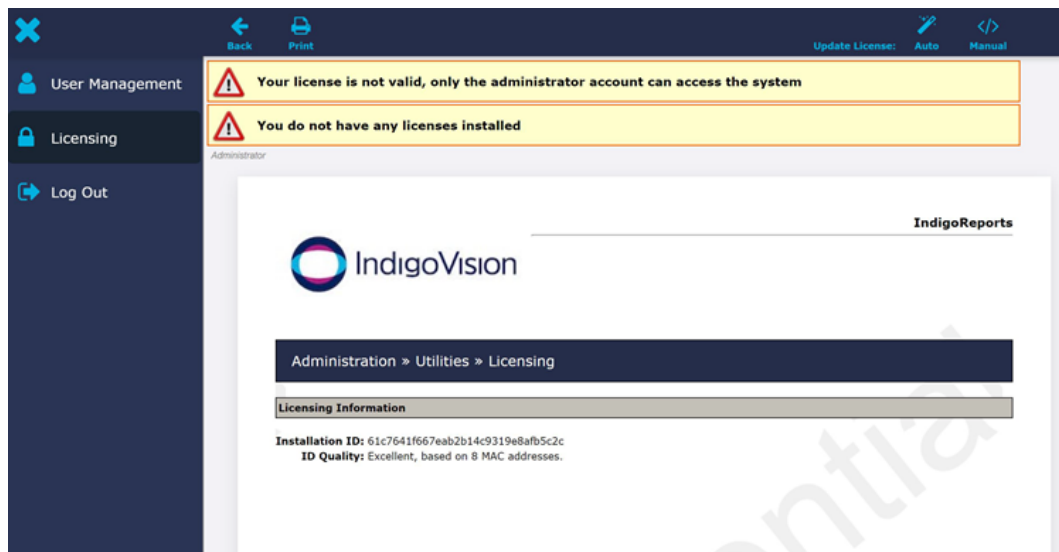


Figure 4: IndigoReports Licensing Information page overview

Auto

Use the **Auto** licensing procedure to request a license from the IndigoReports license service. To obtain a license from the IndigoReports license service, you need to connect over the Internet.

Notice *The Auto licensing procedure is designed for automatically re-licensing IndigoReports when re-installed on existing hardware. For new installations, follow the manual process.*

1. On the **Licensing Information** page, choose **Auto**.

A warning pop-up window displays.

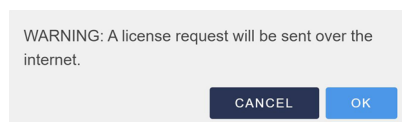


Figure 5: A warning about the Internet connection

2. Click **OK**.
A connection to an IndigoVision server is established.
3. If IndigoReports has been licensed on the same hardware, it will automatically obtain a license.
4. If IndigoReports has never been licensed, or is installed on new hardware, the following message indicates that you need to contact IndigoVision order management team to place a license request:

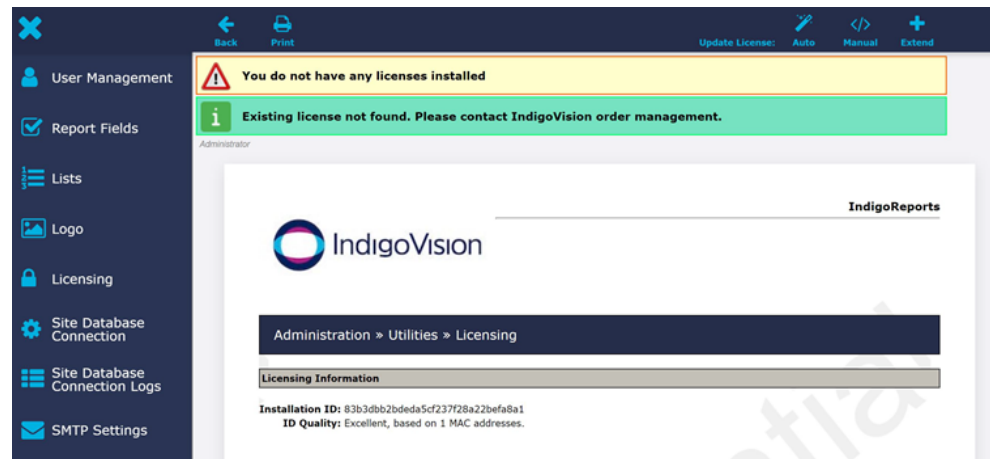


Figure 6: A message warning that no existing license was found

Manual

Use the **Manual** licensing procedure for offline licensing or for new installation.

1. From the **Licensing Information** page, copy the installation ID, displayed below the **Licensing Information** pane.
2. Send the installation ID with your company name and/or purchase order to IndigoVision Order Management.
3. IndigoVision Order Management activates the license and replies with a license key.
4. Click the **Manual** button and enter the license in the text box.

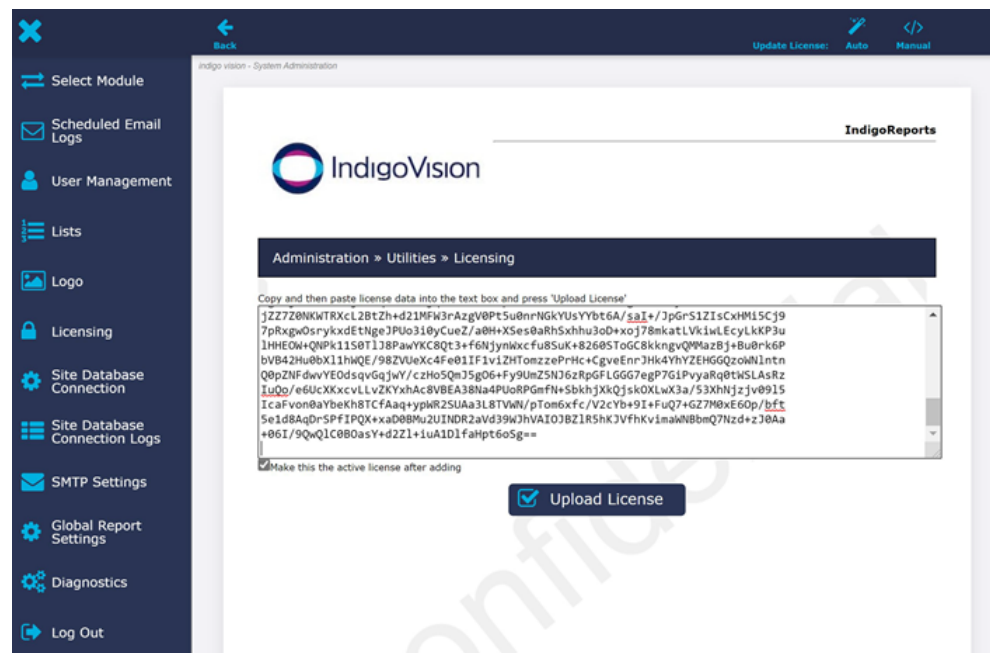


Figure 7: Entering the IndigoReports license manually

5. Select **Make this the active license after adding**.
6. Click **Upload License**.

The license is activated and the messages indicating invalid license disappear.



*The other license details listed in the **Administration > Utilities > Licensing > Current Active License** section are not relevant to the customer and can be ignored.*

Extend

The **Extend** button is only used for extending the duration of IndigoReports demo licenses. For more information on demo licenses, contact your IndigoVision Regional Sales Manager.

Creating a user account

After you have licensed and logged in as an administrator, you can create a new user account to use reporting features.

Notice *The `admin` account can't use reporting features.*

To create a new user account

To create a new user account, follow these steps:

1. In the left navigation menu, click **User Management**.
2. At the top-right of the window, click **Add New User**.
3. Complete the form.
The username must be unique. Completing first name, last name, and password is recommended. Badge ID is optional.
4. Optionally, you can grant the user several roles.
► For more information on user roles, see *"User roles" on page 31*
5. Click **Save**.

After you have created the new user account, you can sign in with this account to access the system.

Connecting IndigoReports to the Control Center site database

After creating a user account, you need to connect IndigoReports to the Control Center site database.

To connect IndigoReports to the Control Center site database

To connect to the Control Center site database, follow these steps:

1. Log out of the built-in **admin** account.
2. Log back in as a user with the **System Administration** role.
3. In the left navigation menu, click **Select Module**.
4. Click **System Administration**.
5. Click **Site Database Connection**.

6. Complete the form.
 - For more information, see "Site database connection" on page 32
7. Click **Save**.

The page reloads and displays the Site Database Connection logs.


To troubleshoot the IndigoReports connection to the Control Center site database


If the connection process was not completed successfully, follow these steps to analyze the problem:

1. In the left navigation menu, click **Site Database Connection Logs**.

The latest entry indicates either a success, or an error and the reason for failure.
2. In case of an error, go back to the step 3 of the previous procedure.

Notice *A user account called **Data Import** is automatically created during installation. The IndigoReports server uses this account to import data from the Control Center site database. This account's credentials are managed by the IndigoReports server, and its activity is tracked in the audit logs.*

 *After initial configuration, a success message may take up to 45 seconds to appear in the site database connection logs. If no logs are shown, wait at least 45 seconds and click the **Refresh** button at the top-right.*

 *After IndigoReports is successfully connected to the site database, it can take up to 30 minutes for some reports to populate with Control Center site data, depending on the server's performance.*

5

USING INDIGOREPORTS

This section describes how to use IndigoReports. To use IndigoReports, you need to sign in with a user account.

Navigating the IndigoReports interface

The navigation menu on the left side of the screen contains icons and buttons that allow you to access all features available within an IndigoReports module.

When using a mobile device, you can tap the icon at the top left of the screen to display the menu icons only.

Available modules

All IndigoReports installations contain the following modules:

- **VMS Reporting** (for audit, health, inventory, and CyberVigilant reports)
- **System Administration** (for system configuration)
- **Data Management** (provides direct access to raw data for troubleshooting)

Additionally, if licensed, the **Incident Reporting** module will be available for creating security incident reports.

To change modules

To change modules, follow these steps:

1. In the left navigation menu, click **Select Module**.
A module selection window opens.
2. Select the module you want to use.

Global reporting features

These features are available across reports and modules.

Filtering reports and searches

You can filter most reports and searches.

1. At the top-right of the screen, click the **Filter** button.
The pop-up window with all available filters opens.
2. Select the filters you want to use to filter the current view.

Some VMS Reporting features can't be filtered, because their reports use information from different sources that don't share the same data structure. The following reports can't use filtering:

- **Health Summary**
- **Inventory**
- **CyberVigilant**

To use the filter feature on the above reports, you need to drill down on individual report elements first. For example, the **Inventory** report can't be filtered. But if you drill down on the **Cameras by Site** graph to display all cameras in a given site, you can filter the resulting view.

Sending reports by email

You can send reports by email as PDF documents. To send an email from IndigoReports, at the top of the screen click the **Email** button.

Downloading reports

To download a report:

1. At the top of the screen, click the **Download** button.
2. Select the file type from the following options:
 - **PDF**
 - **Word**
 - **PPT**
 - **Excel**

VMS Reporting module

The **VMS Reporting** module contains the following reports:

- **Audit**
- **Health**
- **Inventory**
- **Detector**
- **CyberVigilant**
- **Recording**
- **Alarm Events**

To access each of the reports, on the left navigation menu click the corresponding button.



IndigoReports reports are not refreshed in real time - they are a snapshot to document status at the time the report was generated. The date and time of report generation is listed at the top left of the screen. To refresh a report, click on a report feature on the left navigation menu or apply a filter.

My Reports

You can save a filtered report to run at a later time, using the same filter criteria as before.

1. At the top right of a filtered report page, click **Save**.
2. Enter a name for your saved report.
3. Modify criteria as necessary.
4. If you want this report to be e-mailed on a schedule, complete the fields in the **Scheduled Email Configuration** section. This can be modified later by accessing the report in **My Reports**.
5. Click **Save**.

You can now run, modify, or delete your saved reports.

To access your saved reports, do the following:

1. On the left navigation menu, click **My Reports**.
2. In the popup window, select **My Reports**.
3. Select a report from the list.
4. Select one of the following options:
 - **Run**
 - **Modify**
 - **Delete**

Canned Reports

In addition to reports which can be saved by the user, a collection of canned reports are provided. These reports are built with commonly-used criteria and will be enhanced over time through product updates.

To access Canned Reports, follow these steps:


1. On the left navigation menu, click **My Reports**.
2. Select **Canned Reports**.
3. Choose a search that you want to view.

After you have selected a Canned Report, you can either run the report or configure scheduled emails for the report.

Audit Report

IndigoReports provides a unified audit capability by combining Control Center audit logs with IndigoReports audit logs in the IndigoReports Audit feature.

The Audit Report summarizes the audit logs with the following report elements:

| Element name | Description |
|------------------------------------|---|
| Audit Log Connection Status | A table that shows at a glance if all Control Center PCs are writing to the audit logs. The table lists each client PC by host name, and displays its last audit log record. If a given PC has not generated an audit log record within the last 24 hours, the Last record field turns red. |
| |  <i>An entry called IndigoReports always displays to indicate that the IndigoReports server is generating audit logs. This will be the only entry after installation, until Control Center PCs begin connecting to IndigoReports.</i> |


| Element name | Description |
|--|---|
| User Login Activity | A table that shows at a glance which users are currently logged in to Control Center. When a user logs in, their username, Control Center PC's host name, and the time of their last activity are listed below Logged In . When a user logs out, their username is listed in the table below Logged Out when the report is generated. |
| Denied Events Over Time | <p>A graph that indicates trends in Denied events at a glance. Denied events are generated when an action is denied or unauthorized activity is detected. A square box is displayed on the graph below the count of a given day's events. You can click on that box to drill down to a filtered report listing that day's denied events. Events which meet this criteria include:</p> <ul style="list-style-type: none"> • Log Out Denied • Protected Object Access Denied • View Recorded Video Denied • Warning: Insufficient access permissions • Error: Unauthorized to clear alarm • Login: Bad username • Login: Bad password |
| Admin Logins Over Time | A graph that indicates trends in administrator account logins at a glance. A square box is displayed on the graph below the count of a given day's events. You can click on that box to drill down to a filtered report listing that day's denied events. |
| Exports Over Time | A graph that indicates trends in Control Center video exports at a glance. A square box is displayed on the graph below the count of a given day's events. You can click on that box to drill down to a filtered report listing that day's denied events. |
| Account Management Activities | A graph that shows a breakdown of recent account management activities. Examples of account management activities include adding, modifying, or deleting user accounts or their permissions. The bar graph shows the total count of activities by activity type. Activity types are detailed in the legend below the graph. You can click on any of the bars on the graph to drill down to a filtered report listing that activity type's events. |
| Protected Zones and Recordings | A graph that shows a breakdown of recent activities affecting sensitive Control Center objects, like protected zones or protected recordings. Examples of these activities include access to protected objects, or protect and unprotect actions. The bar graph shows the total count of activities by activity type. Activity types are detailed in the legend below the graph. You can click on any of the bars on the graph to drill down to a filtered report listing that activity type's events. |
| Recording and Alarm Management Activities | A graph that shows a breakdown of recent activities affecting video recording or involving the handling of alarms. Examples of these activities include isolating and restoring detectors, setting and unsetting zones, adding bookmarks, or acknowledging and clearing alarms. The bar graph shows the total count of activities by activity type. Activity types are detailed in the legend below the graph. You can click on any of the bars on the graph to drill down to a filtered report listing that activity type's events. |
| Live, Playback, and Export Activities | A graph that shows a breakdown of recent activities involving the review or export of recorded video. Examples of these activities include starting and stopping video streaming or playback, or starting a video export job. The bar graph shows the total count of activities by activity type. Activity types are detailed in the legend below the graph. You can click on any of the bars on the graph to drill down to a filtered report listing that activity type's events. |
| Audit Logs | A section that allows the user to quickly search recent audit log records by entering search criteria in the text box. The records are hidden by default and you can click Show to view them. By default, the most recent 200 records are shown, but this can be changed in Report Preferences for each user. |

Health Report

IndigoReports provides a Health Report that helps customers keep their Control Center systems running at their full capacity.

This report summarizes the operating status of all cameras and NVRs within the Control Center system, and helps the customer understand if they have configured fault detector alarms for complete system coverage.

This report summarizes the Control Center systems health and status with the following report elements:

| Element name | Description |
|--|---|
| License Server Fault Detector Configured | Information if a fault detector has been configured to monitor the system License Server. The value can be Yes or No . |
| Site Database Connection status | This feature indicates the time of the last update of the Control Center site database, and turns red if no update has been received within 24 hours. |
| Audit Log Connection Status | <p>A table that shows at a glance if all Control Center PCs are writing to the audit logs. The table lists each client PC by host name, and displays its last audit log record. If a given PC has not generated an audit log record within the last 24 hours, the Last record field turns red.</p> <div>  <p><i>An entry called IndigoReports always displays to indicate that the IndigoReports server is generating audit logs. This will be the only entry after installation, until Control Center PCs begin connecting to IndigoReports.</i></p> </div> |
| NVR Monitoring Coverage | A pie chart that shows if all configured NVRs are monitored by a fault detector. A legend at the bottom of the chart maps a color to a status indicating either NVR Fault Detector Configured or NVR Fault Detector Not Configured . You can click on colored sections of the pie chart to drill down to a list of the indicated NVRs. |
| Global Recording Jobs Status | A pie chart that shows if all configured recording jobs (including all configured NVRs) are currently recording video. A legend at the bottom of the chart maps a color to a status indicating either Recording or Not Recording . You can click on colored sections of the pie chart to drill down to a list of the indicated recording jobs. |
| Camera Monitoring Coverage | A pie chart that shows if all configured cameras are monitored by a fault detector. A legend at the bottom of the chart maps a color to a status indicating either Camera Fault Detector Configured or Camera Fault Detector Not Configured . You can click on colored sections of the pie chart to drill down to a list of the indicated cameras. |
| Global Recording Jobs Status Distribution | A graph that shows the operational status of all configured recording jobs. A legend at the bottom of the chart maps a color to recording job statuses including Recording , Recording time corrected by NVR , Not recording , camera cannot be contacted , or Disabled . You can click on the bars on the graph to drill down to a list of recording jobs with the indicated status. |
| Recording Jobs with Time Correction | A pie chart that shows if all recording jobs have time synchronization between the camera and the NVR. A legend at the bottom of the chart maps a color to a status indicating either Recording Time Synchronized or Recording Jobs with Time Correction . You can click on colored sections of the pie chart to drill down to a list of the recording jobs. |
| Cameras with NTP Server Configured | A pie chart that shows if all cameras have been enabled to obtain date and time from an NTP (Network Time Protocol) server. A legend at the bottom of the chart maps a color to a status indicating either Enabled or Disabled . You can click on colored sections of the pie chart to drill down to a list of the indicated cameras. |

Inventory Report

IndigoReports provides an Inventory Report that helps customers keep track of cameras and NVRs, keep their firmware up-to-date, and view configuration details without needing to

directly access the devices.

To simplify camera configuration or troubleshooting, if cameras are accessible via network from a user's PC, they can click on camera IP addresses or URLs directly on the report and their browser will be redirected to the camera's web interface.

The Inventory Report summarizes customer's hardware and firmware status with the following report elements:

| Element name | Description |
|--|---|
| NVRs by Site | A graph that shows the total number of NVRs in the Control Center system, and organizes them by site. A legend at the bottom of the graph maps a color to a site. You can click on the bars on the graph to drill down to a list of NVRs in that site. |
| Cameras by Site | A graph that shows the total number of cameras in the Control Center system, and organizes them by site. A legend at the bottom of the graph maps a color to a site. You can click on the bars on the graph to drill down to a list of cameras in that site. |
| Firmware Versions by Model | A table that groups cameras by model to quickly ensure cameras have matching firmware, or to identify cameras with out-of-date firmware. The table is hidden by default and you can click Show to view it. Within each camera model group, cameras are grouped by firmware version and listed by name and IP address. Clicking on a camera's IP address will redirect your browser to the camera web interface. |
| Camera Count Over Time | A graph that indicates trends in the total camera count of a Control Center system. A square box is displayed on the graph below the total camera count on a given day. |
| Cameras added in the last 30 days | A table that lists cameras that have been added to the Control Center system within the last 30 days. Camera listings include their name and IP address. Click on a camera's IP address to redirect your browser to the camera web interface. This list is limited to the last 10 cameras added within 30 days by default, but this can be changed in Report Preferences for each user. |
| Cameras removed in the last 30 days | A table that lists cameras that have been removed from the Control Center system within the last 30 days. Camera listings include their name and IP address. Clicking on a camera's IP address will redirect your browser to the camera web interface. This list is limited to the last 10 cameras removed within 30 days by default, but the limit can be changed within user-specific Report Preferences. |
| Cameras | A section that allows the user to quickly search for cameras by entering a camera name in the text box. The records are hidden by default and you can click Show to view them. 200 cameras are listed by default, but this can be changed in Report Preferences for each user. To view a list of all cameras in the Control Center system, click Show All . |
| NVRs | A section that allows the user to quickly search for NVRs by entering an NVR name in the text box. The records are hidden by default and you can click Show to view them. 200 NVRs are listed by default, but this can be changed in Report Preferences for each user. To view a list of all NVRs in the Control Center system, click Show All . |
| Alarm Servers | A section that allows the user to quickly search for Alarm Servers by entering an Alarm Server name in the text box. The records are hidden by default and you can click Show to view them. 200 Alarm Servers are listed by default, but this can be changed in Report Preferences for each user. To view a list of all Alarm Servers in the Control Center system, click Show All . |

Detector Report

IndigoReports provides a detector report designed to help customers quickly spot system trouble or security issues by analyzing detector activation activity.

This report summarizes the historical detector activations as well as current detector status with the following report elements:


| Element name | Description |
|-------------------------------------|--|
| Most Active Detectors | <p>A graph that shows at-a-glance the most active detectors during a given time period. The default time period is 7 days, but this can be configured in user-specific Report Preferences. Any detectors that have activated during the given time period are listed by name and total activation count during the time period.</p> <p>Click the bar representing a given detector lets you drill-down to a listing of that detector's activation events during the given time period.</p> |
| Activations by Detector Type | <p>A graph that shows at-a-glance the most active detector types during a given time period. The default time period is 7 days, but this can be configured in user-specific Report Preferences. Each detector type is listed along with a total count indicating the total number of detector activations for that detector type.</p> <p>Click on the bar representing a given detector type lets you drill-down to a listing of all detector activations during the time period where the detector's type matches the bar selected.</p> |
| Detector Status Distribution | <p>A pie that shows at-a-glance the most recent status (as indicated by the timestamp at the top of the report) of all configured detectors. A legend at the bottom of the chart maps a color to each detector status including Triggered, Restored (Enabled), and Isolated (Disabled).</p> <p>Click on colored parts of the pie, which represents a given detector status, lets you drill-down to a listing of all detectors which match that status.</p> |
| Detectors | <p>A section that lets you search for detectors by name by entering search criteria in the text box. The records are hidden by default.</p> <p>Click Show to view the records.</p> <p>When detectors are shown, each detector listing includes its status as well as a listing of that detector's activations if any occurred during the report's selected time period.</p> |

CyberVigilant Report

IndigoReports provides a CyberVigilant report which combines data from CyberVigilant sensor appliances, CyberVigilant in Camera, and Control Center audit logs to help spot potential attacks or breaches.

This report summarizes the Control Center system's cyber security events with the following report elements:

| Element name | Description |
|---|---|
| CyberVigilant IoC (Indicators of Compromise) dashboard | <p>A green / red indication as to whether any potential indicators of compromise (IoCs) have been detected during the report's time period. The default time period is 24 hours, but this can be changed in user-specific Report Preferences.</p> <p>Each of the seven IoCs are listed and show a green checkmark if associated events have not occurred during the report's time period. If events associated with a given IoC have been detected during the report's time period, that IoC's title will turn red. Additionally, the associated event types will be listed underneath the IoC title. Each event type will be listed with a total count of associated events during the report's time period. You can click on an event type to drill-down to a listing of each individual matching event.</p> <p>The following IoCs are shown on the IoC Dashboard:</p> <ul style="list-style-type: none"> • Suspicious User Activity - unauthorized user access or actions from Control Center audit logs • Blocked Activity - unauthorized network traffic which has been blocked by a configured camera's CyberVigilant in Camera firewall • DoS (Denial of Service) - potential denial-of-service events detected by CyberVigilant • Honey pot activity - network traffic to or from a honeypot device which has been configured on a CyberVigilant sensor appliance • Network protocol anomaly - network traffic which deviates from the standard protocols used by Control Center. • Recon - scans and other events which may indicate network reconnaissance activity |

| Element name | Description |
|---|---|
| | <ul style="list-style-type: none"> Remote device access - unauthorized remote access to monitored cameras or NVRs within the Control Center system Unauthorized activity - network traffic between unauthorized devices and monitored cameras or NVRs within the Control Center system |
| CyberVigilant Events by Type | <p>A graph that summarizes cyber-security events detected within the report's time period. The default time period is 7 days, but this can be changed in user-specific Report Preferences. Each event type is listed by name along with a total count of events matching that event type during the report's time period.</p> <p>Click on an event type's bar on the graph to drill-down to a listing of individual events which match that event type.</p> |
| Last 10 CyberVigilant Events | <p>A table that summarizes recent cyber security events. 10 events are listed by default, but this can be changed in user-specific Report Preferences. Events are listed by the name of the detector which captured them. Each event listing includes a description of the event and a timestamp.</p> <div>  <div> <p><i>There will always be an entry called IndigoReports to indicate that the IndigoReports server itself is generating audit logs.</i></p> <p><i>This will be the only entry after installation until Control Center PCs begin connecting to IndigoReports.</i></p> </div> </div> |
| CyberVigilant in Camera Events (by camera) | <p>A pie chart that indicates at-a-glance which cameras are generating cyber security events. The chart includes all CyberVigilant in Camera events from configured cameras within the report's time period. The default time period is seven days, but this can be changed in user-specific Report Preferences. A legend at the bottom of the chart maps a color to a camera. Each camera's colored piece of the pie chart includes a count totalling all of its CyberVigilant in Camera events during the report's time period.</p> <p>You can click on a camera's piece of the pie chart to drill-down to a listing of that camera's CyberVigilant in Camera events.</p> |
| CyberVigilant Events Over Time | <p>A graph that indicates trends in cyber security events at-a-glance. A square box is displayed on the graph underneath the count of a given day's events.</p> <p>You can click on that square box to drill-down to a filtered report listing that day's cyber security events.</p> |

Recording Report

IndigoReports provides a recording report designed to help customers make sure all of their cameras are being recorded.

This report summarizes the status of all configured recording jobs in the Control Center system, and helps the customer quickly identify cameras and NVRs which may need attention.

The Recording report includes the following report elements:

| Element name | Description |
|-------------------------------|--|
| Current Recording Jobs | A comparison showing the total number of successful recording jobs compared to the total number of configured recording jobs across the Control Center system. |

| Element name | Description |
|-------------------------------------|---|
| Global Recording Jobs Status | <p>A pie chart that indicates at-a-glance whether or not all configured recording jobs, including all configured NVRs, that are currently recording video.</p> <p>A legend at the bottom of the chart maps a color to a status indicating either Recording or Not Recording.</p> <p>You can click on colored sections of the pie chart to drill-down to a list of the indicated recording jobs.</p> |
| Status: All Recording Jobs | <p>A graph that indicates the operational status of all configured recording jobs. A legend at the bottom of the chart maps a color to recording job statuses including Recording, Recording time corrected by NVR, Not recording, camera cannot be contacted, or Disabled.</p> <p>You can click on the bars on the graph to drill-down to a list of recording jobs with the indicated status.</p> |
| Recording Jobs by NVR | <p>A table that summarizes all configured recording jobs and groups them by NVR. Recording jobs can be searched by entering criteria, for example, a camera name, in the search box.</p> <p>The table is hidden by default. Click Show to view the table.</p> <p>When shown, each NVR is listed with a comparison of total successful recording jobs compared with its total configured recording jobs, and each recording job is listed with detailed information and status.</p> |

System Administration module

The System Administration module contains the following features:

- User Management - shown only to users assigned to this role
- Lists - custom field lists for Incident Reports
- Logo - allows upload of a 280x70 JPG image which will be shown at the top-left of all reports.
- Licensing
- Site Database Connection - configuration for connection to Control Center's site database.
- Site Database Connection Logs
- SMTP Settings
- Scheduled E-mail Logs
- Global Report Settings - settings for report headers and scheduled report e-mails
- Diagnostics - only used by technical support

User roles

When new user accounts are created, no roles are assigned by default. Roles control a given user's access to modules within IndigoReports. One or more roles may be assigned to a user when creating or modifying a user account:

- **Report Preferences** - this role allows users to customize user-specific report parameters (for example, how many records to show per page) and schedule e-mails for saved reports
- **System Administration** - this role allows access to the 'System Administration' module
- **User Management** - this role allows the creation or modification of user accounts, including password resets. This role implies the System Administration role
- **Data Management** - this role is designed for administrator users and is only intended for troubleshooting. The Data Management module allows users view 'raw' data

generated by some IndigoReports back-end processes, or data imported into IndigoReports from Control Center. This module includes views of the following data:

- **Alarm Events** - event records including zone alarms, detector activations, and data records from configured alarm servers within the Control Center system
- **Site Database Imports** - lists of Control Center site objects like cameras, NVRs, alarm servers, zones, detectors, and more, as well as raw XML-formatted ONVIF configuration data fetched from cameras configured in the Control Center system
- **Advanced Search** - an advanced search feature allowing granular searches of raw data within IndigoReports. This includes audit log records as well as Alarm Events and Control Center site objects from Site Database Imports
- **VMS Reporting** - this role allows access to the 'VMS Reporting' module

Lists

Custom lists can be configured for the following fields in the Incident Reporting module:

- Locations
- Incident Types

Site database connection

The following fields must be completed after installation to connect IndigoReports with the Control Center site database:

- **File path** - the path where the Control Center site database files can be found (e.g. C:\IndigoSiteDB or \\192.168.1.1\IndigoSiteDB)
- **Username** - username of a Control Center user (we recommend a dedicated 'service account' user) assigned with the 'Administrator' or 'Restricted Administrator' role
- **Password** - the Control Center user's password
- **Import Alarm History Backfill Seconds** - when IndigoReports connects to Control Center, it will request historical alarm records from configured alarm servers this many seconds in the past
- **ONVIF polling interval** - interval (in seconds) which IndigoReports will connect to configured cameras to obtain updated ONVIF details
- **Site Database Polling interval** - interval (in seconds) which IndigoReports will check the Control Center site database for updates
- **Audit Log Reaping** - retention period (in days) for audit log records stored in IndigoReports
- **Alarm Log Reaping** - retention period (in days) for alarm and data records stored in IndigoReports (this is configured independently of the period configured on the Alarm Server storing the original records)
- **SMB Username** - if the Control Center site database is located in an SMB share, an SMB username should be provided for IndigoReports to use when connecting to the site database (optional - only required if SMB authentication is required)
- **SMB Password** - password for the SMB user
- **SDS Address** - IP Address or Hostname of the machine that is running the SDS
- **SDS Token** - a service authentication token is needed for use by applications connecting to the SDS. Please refer to page 27 of the SDS Admin guide on how to generate a Service Authentication Token
- **SDS Port** - enter the port that the SDS is configured to respond on. Default is 8135
- **Allow untrusted SDS certificates** - this option should be enabled if the Site Database Server certificate is Untrusted

SMTP Settings

Customers can provide SMTP server connection parameters for use when sending e-mailed reports.

A HTTPS CERTIFICATES

HTTPS is a secure communications protocol used between clients, for example web browsers, and web servers, for example, IndigoReports. HTTPS provides security in two ways:

- **Encryption** - communications are encrypted to maintain confidentiality so they cannot be intercepted by 3rd parties.
- **Authenticity** - HTTPS certificates are used so each party (the client and the server) can verify the other's identity before communicating. Additionally, the parties typically require a trusted certificate authority (CA) to assert (or sign) the validity of the certificates.

To enable secure-by-default communications and for convenience, IndigoReports generates a self-signed certificate using the server's host name during installation. Most web browsers do not trust self-signed certificates, and will display a warning message before allowing you to proceed to the IndigoReports login page.



The self-signed certificate generated during installation is associated with the server's host name. This certificate will be invalidated and will need to be regenerated if the server's host name is changed.

Installing a trusted certificate (recommended)

Installing a certificate signed by a trusted certificate authority is recommended.

On corporate networks, the customer's IT organization may be able to sign certificates on their Windows domain, or may use a 3rd party trusted certificate authority, for example, DigiCert.

Before a certificate can be signed, a certificate signing request (CSR) must be generated by the IndigoReports server. The CSR must then be provided to the certificate authority. The certificate authority will provide a signed certificate, which can then be installed in the IndigoReports server.

This documentation provides a general overview of the certificate signing process, but some steps may vary depending on your certificate authority. Contact your IT organization or certificate authority if further detail or assistance is required.

Generate the CSR

To generate a CST, follow these steps:

1. Navigate to the IndigoReports program directory (the default path is C:\Program Files\IndigoVision\IndigoReports)
2. Right-click on **IndigoReports.Shell** and select **Run as administrator** to launch the IndigoReports Command Shell.
3. Type the following command and press enter: `cert create csr`
4. Click-and-drag to highlight the CSR.

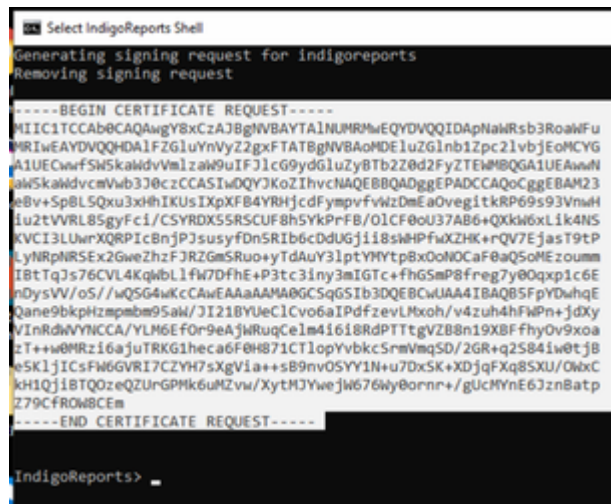


Figure 8: Selection of CSR

5. Right click and copy the CSR to your clipboard
6. Paste the CSR into a text file or e-mail so that you can provide the CSR to the certificate authority.

Install the signed certificate

After the certificate authority has signed the certificate, they will provide a new certificate to be installed on the IndigoReports the server. The following steps are recommended to be completed on the IndigoReports server.

1. Open the certificate file provided by the certificate authority in a text editor, for example Notepad.
2. Select all the text and copy.
3. Navigate to the IndigoReports program directory (the default path is C:\Program Files\IndigoVision\IndigoReports)
4. Right-click on **IndigoReports.Shell** and select **Run as administrator** to launch the IndigoReports Command Shell.
5. Type the following command and press enter: `service stop`
6. Type the following command and press enter: `cert install server`
A message is shown asking you to paste the certificate text.
7. Select an empty space below the message, right-click and paste the certificate text.
8. Select CTRL+D
9. Type the following command and press enter: `service start`

Trusting the IndigoReports server's built-in certificate authority

If you do not have access to an IT organization or trusted certificate authority, or if IndigoReports is installed on an isolated network without a domain, you may wish to trust the IndigoReports server's built-in certificate authority.

To do this, the built-in certificate authority's certificate must be installed as a **Trusted Root Certificate Authority** on each PC used to access IndigoReports. After the built-in certificate authority's certificate is obtained, consult your web browser's documentation for instructions on installing the certificate as a **Trusted Root Certificate Authority**.

Obtain the built-in certificate authority's HTTPS certificate

To obtain the built-in certificate authority's HTTPS certificate, follow these steps:

1. Navigate to the IndigoReports program directory (the default path is C:\Program Files\IndigoVision\IndigoReports)
2. Right-click on **IndigoReports.Shell** and select **Run as administrator** to launch the IndigoReports Command Shell.
3. Type the following command and press enter: `cert show ca`
4. Select the certificate text. Ensure you select the `BEGIN` and `END` certificate text comments.
5. Right-click and copy the text.
6. Paste the text into your text editor, for example Notepad.
7. Save the file using the file extension `.crt`, for example, save the file as **indigoreportsca.crt**.
8. Consult your web browser's documentation for instructions on installing this certificate as a **Trusted Root Certificate Authority**.

Generating a new certificate if your server's host name changes

To generate a new certificate, if your server's host name changes, follow these steps:

1. Navigate to the IndigoReports program directory (the default path is C:\Program Files\IndigoVision\IndigoReports)
2. Right-click on **IndigoReports.Shell** and select **Run as administrator** to launch the IndigoReports Command Shell.
3. Type the following command and press enter: `stop service`
4. Type the following command and press enter: `cert create server hostname`
Where `hostname` is the server's hostname
5. Type the following command and press enter: `start service`
6. If you were using a certificate signed by a trusted certificate authority, this new certificate must be signed and installed.

After these steps have been completed, follow the instructions on generating a CSR and installing a certificate.

► For more information, see *"Generate the CSR" on page 35*