IndigoVision

Integra

User Guide

IndigoVision

THIS MANUAL WAS CREATED ON TUESDAY, APRIL 23, 2019.

DOCUMENT ID: IU-CAP-MAN001-4

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

Contact address

IndigoVision Limited

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

Dell Software License Agreement

BEFORE USING YOUR INTEGRA VIEW SYSTEM, READ THE DELL SOFTWARE LICENSE AGREEMENT THAT CAME WITH YOUR SYSTEM. YOU MUST CONSIDER ANY MEDIA OF DELL-INSTALLED SOFTWARE AS BACKUP COPIES OF THE SOFTWARE INSTALLED ON YOUR SYSTEM'S HARD DRIVE. IF YOU DO NOT ACCEPT THE TERMS OF THE AGREEMENT, CALL THE CUSTOMER ASSISTANCE TELEPHONE NUMBER.

FOR CUSTOMERS IN THE UNITED STATES, CALL 800-WWW-DELL (800-999-3355).

FOR CUSTOMERS OUTSIDE THE UNITED STATES, VISIT **SUPPORT.DELL.COM** AND SELECT YOUR COUNTRY OR REGION FROM THE TOP OF THE PAGE.

Windows License Terms

THE OPERATING SYSTEM ON THE DEVICE IS NOT LICENSED AS GENERAL PURPOSE SERVER SOFTWARE. AS SUCH, YOU ARE PROHIBITED FROM INSTALLING AND USING ANY OTHER SOFTWARE ON THAT SERVER (UNLESS SUPPLIED BY INDIGOVISION); AND ACCESSING OR USING DESKTOP FUNCTIONS ON THE SERVER OTHER THAN AS NECESSARY FOR OPERATING THE NVR-AS SOFTWARE.

TABLE OF CONTENTS

1 ABOUT THIS GUIDE

This guide is written for users of IndigoVision's Integra and provides an overview of the Integra as well as installation and configuration information.

Safety notices

This guide uses the following formats for safety notices:

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

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

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

Additional information relating to the current section.

2 OVERVIEW

IndigoVision's Integra takes the strain out of setting up a control room.

With the Integra, you can combine products including Control Center, Control Center Web, License Server and the NVR into one compact, rack-mountable appliance.

Each Integra appliance provides everything you need to record, playback, view live video and manage alarms at a site with up to 24 cameras.

IndigoVision Integra provides the following features:

- Integrated PoE+ switch: Connect up to 8, 16 or 24 IP cameras on each Integra 8, Integra 16 or Integra 24
- Record video to integrated storage
- Use extendable distributed architecture
- View live and recorded video from IndigoVision cameras and supported third party cameras
- Use advanced alarm management
- Configure automatic actions for recording, PTZ movement, email alerts and more.
- View video and manage alarms on the move with IndigoVision Control Center Mobile
- Control Center can be accessed and controlled remotely using IndigoVision VPN

All Integra Appliances come pre-installed with the following IndigoVision products:

- **Control Center front-end application**

  The user interface for the Control Center suite.

  You can use this to configure and manage Integra installations, view live video, manage recorded video and handle alarms. Configuration data is stored in the Control Center site database.
- **Network Video Recorder / Alarm Server (NVR-AS)**

  Server software which combines video recording and playback with advanced alarm management capabilities.
- **License Server**

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

  A service that you can enable to allow live video and alarm management on mobile devices using the IndigoVision Control Center Mobile app.
- **IndigoVision VPN**

  A service that provides a secure network connection to the Integra so that operators can monitor video and recordings remotely using IndigoVision Control Center.

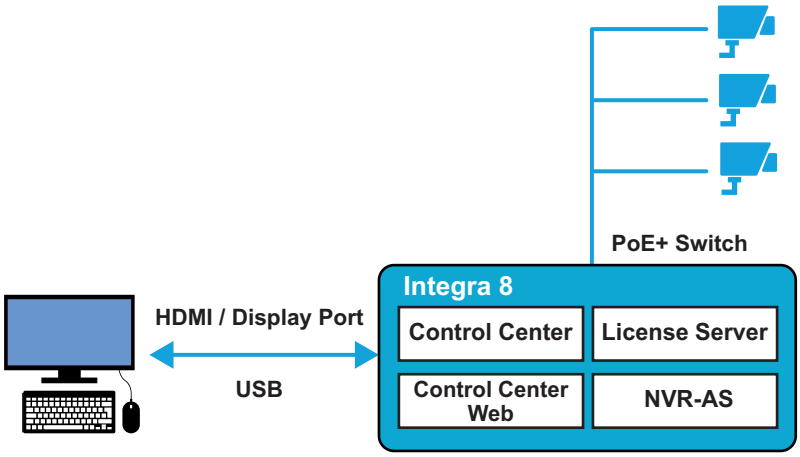

Figure 1: Standalone Integra system

You can create a larger distributed video security system with more than 24 cameras by combining multiple Integra appliances.

To do this, you must use an IndigoVision Integra View Workstation and License Federation. The IndigoVision Integra View Workstation also provides a powerful Control Center workstation for operators and administrators.

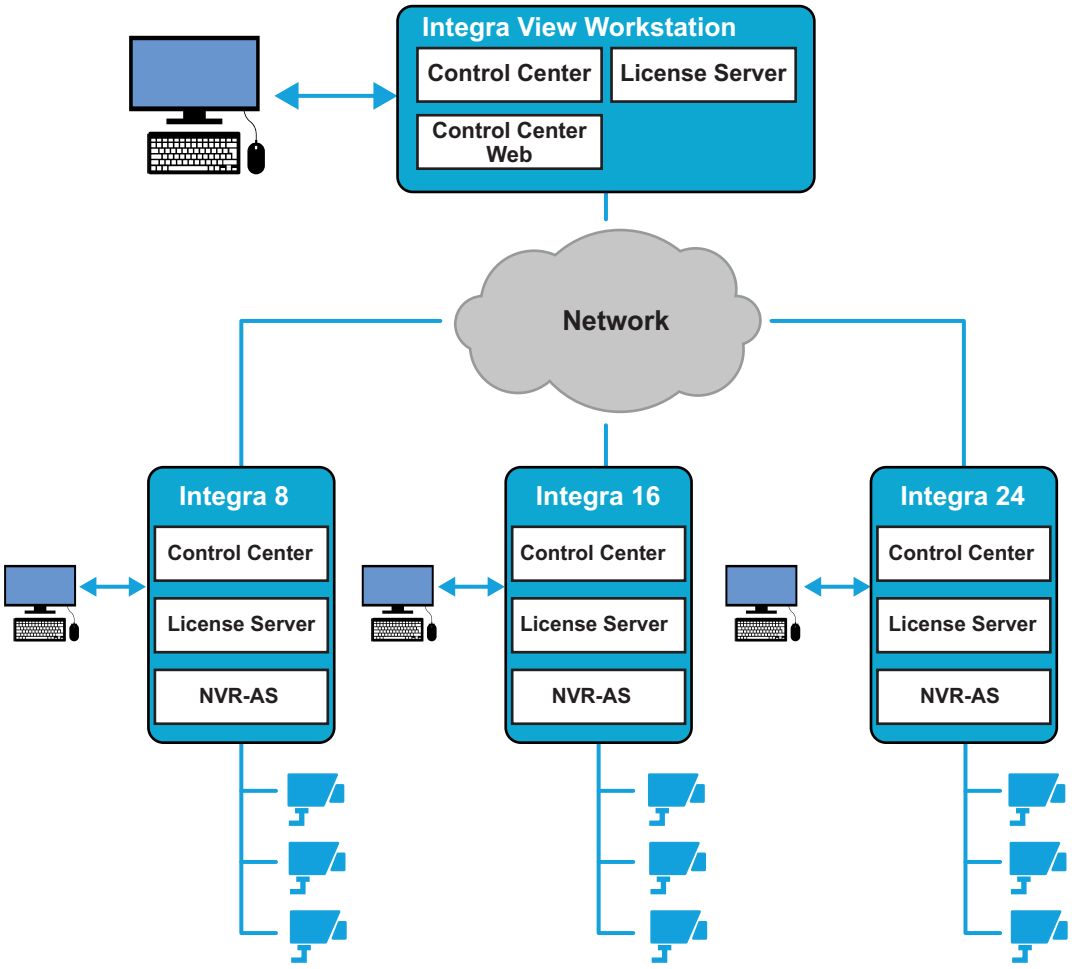

Figure 2: Federated Integra system

Federation of licenses allows multiple License Servers, each with their own license, to be combined into a single system. When License Servers are combined in this way their Camera & NVR license counts are accumulated.

A federated licensing system consists of a single Central License Server running on an Integra View Workstation and multiple Edge License Servers running on Integra Appliances.

In a federated system using an Integra View Mini Workstation the maximum federated Camera count that can be accumulated is 24. Once this limit has been reached adding additional Edge License Servers to the federation will not increase the count unless the Central License Server is replaced.

Table 1: Camera limits at different bands

Type	Max Camera Count
Integra View Mini	24
Integra View Mid	Unlimited

3 HARDWARE

The IndigoVision Integra range consists of the following products:

- Integra 8
- Integra 16
- Integra 24
- Integra View Mini Workstation
- Integra View Mid Workstation

Integra 8

The Integra 8 has the smallest physical form factor of all the appliances. It provides 8 PoE+ ports for IP cameras.

The Integra 8 contains the following:

- An internal hard disk for the operating system and application software.
- A separate hard disk for video storage.

The Integra 8 supports up to 2 monitors.

Integra 8 rear panel connections

The Integra 8 has the following rear panel connections:

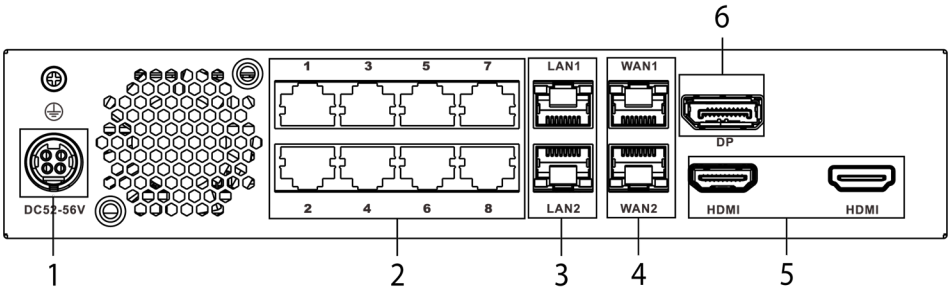

Figure 3: Integra 8 rear panel connections

Table 2: Integra 8 rear panel connections

No.	Connection	Description
1	Power Jack (DC 52-56V)	Connect the power adapter and the power cord shipped with the Integra. Do not use any other power supply.
2	PoE/PoE+ Switch	The PoE/PoE+ switch provides connection to 8 PoE/PoE+ devices
3	LAN (RJ-45) 10/100/1000Mbps	Network connection port used for connecting the switch to a network

No.	Connection	Description
4	WAN (RJ-45) 10/100/1000Mbps	Network connection port used for connecting the PC to the internet
5	2 x HDMI Monitors	Allows you to connect to a monitor through HDMI
6	DisplayPort	Allows you to connect to a monitor through DisplayPort

Integra 16 and Integra 24

The Integra 16 and Integra 24 are larger than the Integra 8 variant, but still fit in a 1U rack space.

The Integra 16 provides 16 PoE+ ports. The Integra 24 provides 24 PoE+ ports.

The Integra 16 and Integra 24 contain the following:

- An internal hard disk for the operating system and application software.
- A separate, four disk RAID5 array for video storage.

The Integra 16 and Integra 24 support up to 2 monitors.

Integra 16 and Integra 24 rear panel connections

The Integra 16 and Integra 24 have the following rear panel connections:

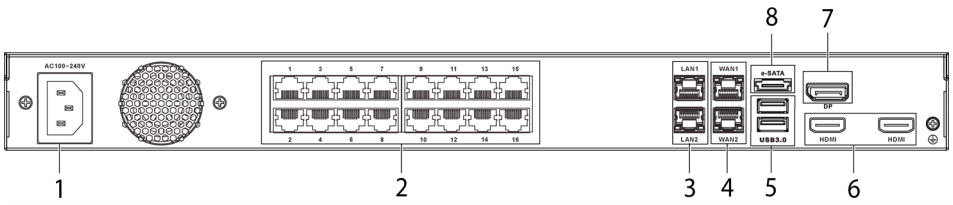

Figure 4: Integra 16 and 24 rear panel connections

Table 3: Integra 16 and 24 rear panel connections

No.	Connection	Description
1	Power socket (AC 100-240V)	Connect the power cable shipped with the Integra. Do not use any other power supply.
2	PoE/PoE+ Switch	The PoE/PoE+ switch provides connection to 16 or 24 PoE/PoE+ devices
3	LAN (RJ-45) 10/100/1000Mbps	Network connection port used for connecting the switch to a network
4	WAN (RJ-45) 10/100/1000Mbps	Network connection port used for connecting the PC to the internet
5	2 x USB 3.0 Ports	Allows you to connect to external USB devices
6	2 x HDMI Monitors	Allows you to connect to a monitor through HDMI
7	DisplayPort	Allows you to connect to a monitor through DisplayPort
8	e-SATA	(Not currently supported)

Integra View Mini Workstation

The Integra View Mini Workstation is a small but powerful workstation that is perfect for those small spaces in a Control Room. It supports up to two monitors.

Integra View Mid Workstation

The Integra View Mid Workstation is a more powerful workstation in a tower PC form factor designed for larger Integra systems.

The Integra View Mid Workstation supports up to four monitors.

Either an Integra View Mini Workstation or an Integra View Mid Workstation must be used in any Integra system with more than one Integra appliance.

4 GETTING STARTED

Integra 8, Integra 16 and Integra 24

This chapter describes the initial steps required to start using an Integra appliance.

Server Installation

Follow the instructions provided in the Quick Start Guide to safely install the server.

Before installing the Integra, review the safety instructions and guides provided with the system.

Never remove the power cord from an Integra device without first shutting down the server. Shut down the server from within Windows, or by pressing the power button on the front panel.

Complete the operating system setup

When you power up an Integra device for the first time, Windows performs initial configuration.

During the initial configuration, you must do the following:

- Specify the location settings
- Read and accept the Windows license agreement
- Optionally disable all of the automatic windows services for customer experience improvement by selecting ***Customize*** on the **Get going fast** page
- Create a local Windows user account

If the Integra is connected to an existing network before it is powered on, the **Choose how you'll connect** page may be displayed. In this page, select ***Join a local Active Directory domain***. This does not require an Active Directory domain on your network.

During the operating system setup, Windows may reboot a number of times.

After Windows configuration is complete and you login for the first time, the system is ready for configuration.

Change Control Center Administrator Password

By default, the Control Center site database is configured with a single administrator user. To protect your security system, you must update this account with a secure password.

Notice *To avoid unauthorized access, IndigoVision strongly recommend that you change the default password for Control Center.*

1. On the desktop, open Control Center with the default credentials:
   Username: `administrator`
   Password: `administrator`
2. In Control Center, select ***File > Change Password***.
   The **Change password** dialog opens.
3. Enter the following fields:
   Current password: `administrator`.
   New password: Enter the password which you want to use.
   Confirm new password: Enter the password which you want to use.
4. Select ***OK***.
   The Control Center Administrator password is changed.

Change Switch Password

IndigoVision Integra appliances contain an integrated PoE/PoE+ switch.

You can manage the switch through the web configuration page from the Integra appliance's Windows desktop.

Notice *To avoid unauthorized access, IndigoVision strongly recommend that you change the default username and password for the web configuration page.*

1. To access the web configuration page, in the Integra launch Internet Explorer and navigate to the IP address `10.5.1.1`.
2. When prompted, enter the default credentials:
   Username: `admin`
   Password: `admin`
3. From the Web Management interface select ***System > Account / Password***
   The **Account / Password** page opens.
4. Change the switch username and password, then select ***Apply***.
   The switch username and password is changed.

After you have configured these settings, you can start adding cameras to the system.

- ► For more information about adding cameras, *see "Add a camera" on page 33*
- ► For more information about other configuration tasks, *see "Additional Configuration" on page 19*

If you are using this appliance to extend an existing Integra system, there are further configuration requirements.

- ► For more information, *see "Expanding an Integra system" on page 34*

Integra View Workstation

This chapter describes the initial steps required to start using an Integra View Mini Workstation or Integra View Mid Workstation.

Complete the operating system setup

When you power up an Integra device for the first time, Windows performs initial configuration.

During the initial configuration, you must do the following:

- Specify the location settings
- Read and accept the Windows license agreement
- Optionally disable all of the automatic windows services for customer experience improvement by selecting ***Customize*** on the **Get going fast** page
- Create a local Windows user account

If the Integra is connected to an existing network before it is powered on, the **Choose how you'll connect** page may be displayed. In this page, select ***Join a local Active Directory domain***. This does not require an Active Directory domain on your network.

During the operating system setup, Windows may reboot a number of times.

After Windows configuration is complete and you login for the first time, the system is ready for configuration.

Change Control Center Administrator Password

By default, the Control Center site database is configured with a single administrator user. To protect your security system, you must update this account with a secure password.

Notice *To avoid unauthorized access, IndigoVision strongly recommend that you change the default password for Control Center.*

1. On the desktop, open Control Center with the default credentials:
   Username: `administrator`
   Password: `administrator`
2. In Control Center, select ***File > Change Password***.
   The **Change password** dialog opens.
3. Enter the following fields:
   Current password: `administrator`.
   New password: Enter the password which you want to use.
   Confirm new password: Enter the password which you want to use.
4. Select ***OK***.
   The Control Center Administrator password is changed.

When you have changed the password, you can use the Integra View Workstation to expand an existing Integra system.

► For more information, *see "Expanding an Integra system" on page 34*

5 ADDITIONAL CONFIGURATION

If your Integra device is part of a larger Integra system, or if you want to use some of the Integra system's more advanced features, then you must make further changes to the configuration.

Switch Configuration

IndigoVision Integra appliances contain an integrated PoE/PoE+ switch.

You can manage the switch through the web configuration page from the Integra appliance's Windows desktop.

To access the web configuration page, launch Internet Explorer and navigate to the switch address, for example `http://10.5.1.1`.

When prompted, enter the username and password.

► For more information, *see "Change Switch Password" on page 16*

From this interface, you can configure the network settings for the switch. By default the switch has the following configuration:

Table 4: Default internal switch IP properties

IP Address	10.5.1.1
Subnet Mask	255.0.0.0
Default Gateway	10.0.0.1
Username	admin
Password	admin
DHCP Server	Enabled
DHCP Address Range Start	10.5.1.101

Before you add cameras to the Integra device or connect the Integra device to the network, you may wish to change the network settings on the switch to reflect your network environment.

You can use an Integra in the following network environments:

- **Isolated network**

  The Integra is not connected to a wider local area network.

  By default, the Integra's switch runs a DHCP server that dynamically allocates IP addresses to any connected IP cameras.

  No further configuration is required.
- **Existing network with a DHCP server**

  The Integra is connected to a wider local area network with an existing DHCP server.

IP cameras connected to the Integra device can use the connected external DHCP server.

- **Existing network using static address scheme**

  The Integra is connected to a wider local area network with a static IP allocation policy.

  If this fits your deployment then you will need to select IP addresses and a netmask that you wish to use for your Integra device and set the integrated switch DHCP address range.

Isolated network

The default switch settings are designed for an isolated network deployment. No additional configuration of the switch is necessary.

The IP cameras can be configured in the following ways:

- Configure the IP cameras to use DHCP

  The DHCP address is allocated by using the PoE/PoE+ port number as the last two digits of the address. For example:

  PoE/PoE+ port **1**: 10.5.1.1**01**

  PoE/PoE+ port **2**: 10.5.1.1**02**
- Configure the IP cameras with an unused static address in the 10.0.0.1-10.255.255.255 range

To inspect or change the DHCP server settings, open the web configuration page and select ***Advanced Features > DHCP Server***.

Existing network with a DHCP server

To configure the IP cameras to use a DHCP server that is running on your local area network, rather than on the Integra switch itself, you must disable the DHCP server on the integrated switch.

1. Login to the switch web configuration page using a web browser.
2. Select ***Advanced Features > DHCP Server***.
3. Change the status to ***Disable*** then select ***Apply***.

You must change the default IP address and netmask to something that fits in your existing network:

4. Navigate to the switch web configuration page.
5. Select ***System > IP Configuration > IPv4***.
6. Change the static IP address from `10.5.1.1` to a valid IP address for your network.
7. Select ***Apply***.

Before you update the IP address in the network settings, ensure that the IP address which you intend to use instead of the default is a valid IP address for your network environment.

Caution

The configuration pages for the switch will only be available on the network settings you submit to this form.

If you change the IP address in the network settings, you will not be able to access the web configuration page using the default IP address.

After you have disabled the DHCP server on the integrated switch, connect the switch to the existing network via the LAN1 or LAN2 ports.

To add cameras, ensure they are configured to use DHCP and connect them to the Integra switch ports.

► For more information, *see "Add a camera" on page 33*

Notice *The network configuration for the Integra server defaults to a static address. You must adjust these settings when connecting the Integra server to an existing network.*

► For more information, *see "Connect the Integra appliance to an existing network" on page 22*

Existing network using static address scheme

To connect the Integra appliance to an existing network that does not have a DHCP server, you can use a static address scheme.

To do this, you must configure the integrated DHCP server address range to allocate IP addresses to the ports, and configure the switch with a valid IP address for your network.

Determine a valid IP range for cameras connected to the Integra device, then reconfigure the DHCP server.

1. Login to the switch web configuration page using a web browser.
2. Select ***Advanced Features > DHCP Server***.
3. In the ***IP start from*** field, enter the IP address which you want to assign to port 1.

   The range extends from this start address by the number of ports on the switch. For example, the default range for an Integra 16 is `10.5.1.101` to `10.5.1.116`.

Notice *You must ensure the address range used by the Integra device for the connected IP cameras will not overlap with any other DHCP server's address pool on your network.*

4. Select ***Apply***.

You must change the default IP address and netmask to something that fits in your existing network:

5. Navigate to the switch web configuration page.
6. Select ***System > IP Configuration > IPv4***.
7. Enter the static IP address settings which you want the switch to use.
8. Select ***Apply***.

Caution *Before you update the IP address in the network settings, ensure that the IP address which you intend to use instead of the default is a valid IP address for your network environment.*

Caution *The configuration pages for the switch will only be available on the network settings you submit to this form.*
If you change the IP address in the network settings, you will not be able to access the web configuration page using the default IP address.

After you have configured the switch, connect the switch to the existing network through the LAN1 or LAN2 ports.

Notice *The DHCP server on the Integra appliance's integrated switch does not respond to requests from devices connected through LAN1 or LAN2.*

To add cameras, ensure they are configured to use DHCP, or assign a static IP address outside the DHCP server range.

► For more information, *see "Add a camera" on page 33*

Notice *The network configuration for the Integra server defaults to a static address. You must adjust these settings when connecting the Integra server to an existing network.*

► For more information, *see "Connect the Integra appliance to an existing network" on page 22*

Network Settings

The Integra View Workstation and Integra appliances have different networking configurations.

Connect the Integra appliance to an existing network

To connect an Integra appliance to an existing network, you must carry out additional configuration of the Integra appliance.

Configure the network settings on the switch

You must change the network settings from the default static IP settings to a configuration that fits your Local Area Network.

► For more information, *see "Switch Configuration" on page 19*

Connect the Integra device to the network using the appropriate physical ports

If you want to make the cameras available on other Integra devices as part of a federated system of Integra appliances and Integra View Workstations all connected on the same local area network, then connect the Integra appliance to the network using the LAN1 or LAN2 ports.

If you want to enable remote desktop access to the Integra, or provide remote access using Control Center Web or IndigoVision VPN, while also keeping the IP cameras isolated from the rest of your network, then connect the Integra appliance to the network using the WAN1 or WAN2 ports.

Table 5: Default Integra network configuration

vEthernet (External Switch) Address	10.5.1.2
vEthernet (External Switch) Netmask	255.0.0.0
vEthernet (External Switch) Gateway	10.0.0.1
WAN1	DHCP
WAN2	DHCP

Configure the Windows network interfaces

Configure the network interfaces within Windows on the Integra device.

1. Open the web configuration page, and select ***Network and Sharing Center > Change adapter settings***.
2. Locate the appropriate adapters:
   - LAN ports: use the ***vEthernet*** (External Switch) adapter
   - WAN ports: use the individual adapter

Notice *Do not edit the adapters labelled **Switch1 – Do Not Edit** or **Switch2 – Do not edit**.*

3. Right-click the adapter and select ***Properties***.
4. Select ***Internet Protocol Version 4 (TCP/IPv4) > Properties***.
5. Review and modify the settings as required.

Notice *In order for an Integra Appliance to be part of a License Federation, it must have an IP address that does not change over time. This can be achieved with a static address configured on the host or a static allocation made by the DHCP server.*

6. Select ***OK***.
   The dialog closes. Your changes are applied to the configuration.

Connect an Integra View Workstation to an existing network

The Integra View Workstation has a single 1Gbps Ethernet adapter. By default, this adapter is configured to use DHCP.

Configure the IP settings on the Integra device.

1. Open the web configuration page, and select ***Network and Sharing Center > Change adapter settings***.
2. Right-click the adapter and select ***Properties***.
3. Select ***Internet Protocol Version 4 (TCP/IPv4) > Properties***.
4. Review and modify the settings as required.

Notice *An Integra View Workstation must have an IP address that does not change over time. This can be achieved with a static address configured on the host or a static allocation made by the DHCP server.*

5. Select ***OK***.
   The dialog closes. Your changes are applied to the configuration.

Date and time settings

Caution *All devices in the IndigoVision system, including the Integra, must be time synchronized using the same NTP hierachy. If they are not, warnings are issued, and certain functionality may not behave correctly, including aspects of video playback.*

Adding upstream time servers

1. From the Start screen select ***Edit NTP Configuration***. A configuration file opens.
2. Delete the default Internet time servers hosted at `pool.ntp.org`.
   By default, the Integra View Workstation is configured to use Internet time servers. If you are adding an upstream time server on your own network, you should first remove the servers hosted at `pool.ntp.org`.
3. Add the upstream NTP server following the format in the configuration file.
   For example to add an NTP server with IP address 192.168.1.1, add the following line:
   ```
   server 192.168.1.1 iburst
   ```
4. Add further server configuration lines for any additional upstream NTP servers.
5. Save and close the configuration file.
6. Restart the NTP service by selecting ***Restart NTP Service*** from the Start screen.

Removing upstream time servers

1. From the Start screen select ***Edit NTP Configuration***. A configuration file opens. See for an example configuration file.
2. Remove the line containing the IP address of the server you wish to remove.
3. Save and close the configuration file.
4. Restart the NTP service by selecting ***Restart NTP Service*** from the Start screen.

Master time server

If this Integra will act as a master time source for a local area network when the configured NTP servers are not available, then the stratum value for the local clock should be changed in

the configuration file.

For other Integra appliances, this setting should be left at the default of a stratum value of 12.

1. From the Start screen select ***Edit NTP Configuration***. A configuration file opens.
2. Find the following line in the configuration file:
   ```
   fudge 127.127.1.0 stratum 12
   ```
3. Change this line to the following:
   ```
   fudge 127.127.1.0 stratum 5
   ```
4. Save and close the configuration file.
5. Restart the NTP service by selecting ***Restart NTP Service*** from the Start screen.

For full documentation on the NTP configuration file format refer to www.ntp.org.

Time zone

Review the time zone setting of the device and change it if necessary.

1. Open the Control Panel.
2. Select ***Set the time and date***.
3. Adjust the time zone setting as required.

Remote desktop configuration

Remote desktop is disabled by default. Enabling remote desktop updates the firewall rules to allow remote desktop connections.

1. Open the Control Panel.
2. Select ***System and Security > System > Remote settings***. The **System Properties** dialog opens.
3. Select the required **Remote Desktop** option.
   If ***Remote Desktop*** connections are allowed, a dialog opens to warn you of the firewall implications.
4. Click ***OK*** to confirm the additional firewall exception.
5. Click ***OK*** to close the **System Properties** dialog.

Windows Update

IndigoVision recommends that all Integra devices have Windows Update enabled and that updates are applied as soon as practicable after release.

The operating system must be regularly updated to ensure optimal security and performance level.

Remote Access

The Integra can be used remotely over the Internet using either Control Center Web or IndigoVision VPN.

Control Center Web is designed to provide quick and easy monitoring on the move. It allows users to access the Integra using the Control Center Mobile app from iOS or Android devices,

or using a web browser. Operators can view live video, monitor alarms and playback video from the time of an alarm.

IndigoVision VPN allows operators to run IndigoVision Control Center from a separate Windows PC connected through the Internet in a secure manner. All of the standard Control Center functionality is available including full playback of recordings, export and site administration.

Control Center Web is ideal for users who need to monitor live videos while away from site or to respond to alarms when they are triggered. For greater system control and configuration it is recommended to use IndigoVision VPN with Control Center.

IndigoVision VPN

IndigoVision VPN creates a secure network connection across an untrusted network such as the Internet, enabling remote access from IndigoVision Control Center anywhere in the world.

IndigoVision VPN provides:

- Simplified installation and configuration of a software VPN
- Encryption of all traffic between devices in the VPN
- Streamlined deployment of Integra and Integra View devices on the Internet
- An easy-to-use configuration interface
- A VPN hosted on existing hardware with no additional cloud service costs
- A scalable solution to your remote access problems
- Powered by OpenVPN, an industry approved open source VPN solution

IndigoVision VPN is pre-installed on IndigoVision Integra and Integra View devices. Before it can be used it must be configured. Refer to the IndigoVision VPN Administrator's Guide for further details. You can find this in the Start Menu of the Integra device.

Control Center Web

Control Center Web encompasses the server side component of IndigoVision's Control Center Mobile and it is required to use the mobile application. Control Center Web also allows you to access live video from the Integra device through a web browser.

Control Center Web provides the following:

- Access to low latency live video from any supported ONVIF camera
- Active alarm management
- Recorded video and audio from the time of an alarm
- Access to a Control Center site securely over the Internet
- Ability to control access through the Control Center site database

Control Center Web does not require plugins or other software to be installed in the web browser.

Components

Control Center Web consists of the following components:

- **Control Center Web application server**

  A web service that runs in IIS to provide the business logic for Control Center Web. It also serves the client application to users.

You must configure the Control Center Web application server with a site database and media server in order to operate.

- **Control Center Web media server**

  A virtual machine that provides services to adapt video streams from cameras within the IndigoVision system, to allow the streams to be viewed using a standard web browser or mobile application.

- **Control Center Mobile**

  A native mobile app that runs on Apple iOS or Android, and can access Control Center Web without requiring a separate web browser.

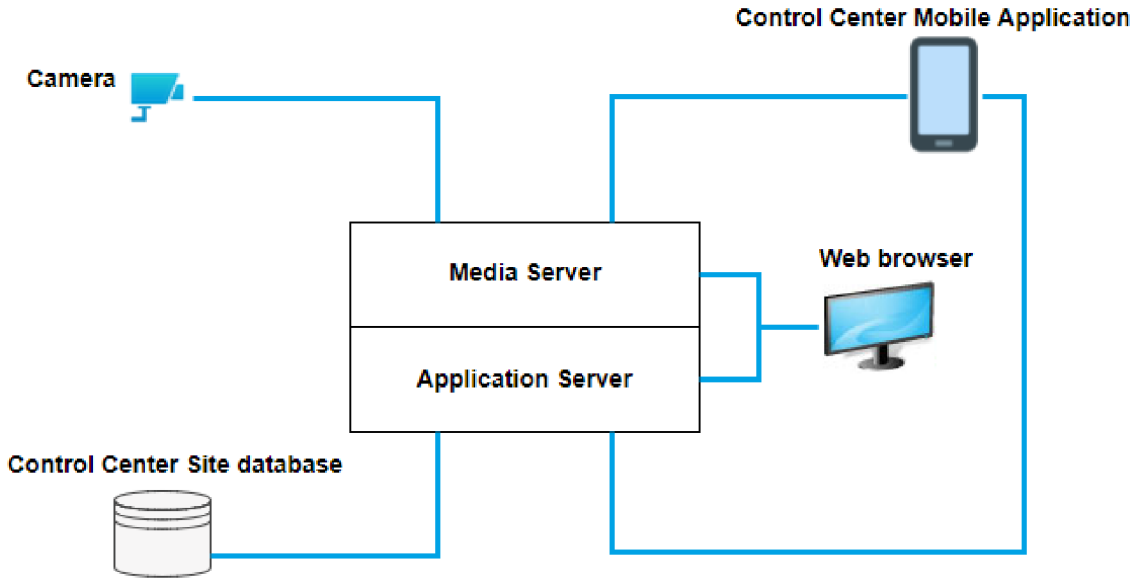

Figure 5: Control Center Web components

Browser compatibility

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

- Mozilla Firefox 54.0 or later
- Google Chrome™ 60.0 or later

Configure Control Center Web on Integra

The Control Center Web media server is already installed on your Integra device.

To use the Control Center Mobile app or web browser, you must configure the media server and install the application server.

Certificates

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

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

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

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

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

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

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

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

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

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

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

- **Use a self-signed certificate**

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

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

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

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

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

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

Enable the media server

To start the media server, do the following:

1. From the start menu, open the Hyper-V Manager tool.
2. In the pane on the left of the screen, ensure that the local PC is selected.
3. Right-click the media server virtual machine, and select ***Start***.

   The media server is now running.

Notice *If you want to stream live video using Control Center Web, you must leave the media server running at all times.*

Configure the media server to start automatically

To ensure that the media server always starts when the Integra restarts, right-click the media server virtual machine, then select ***Settings... > Automatic Start Action > Always start this virtual machine automatically***.

Change the media server password

The media server is installed with a default password. IndigoVision recommend you change this password to something more secure at the earliest opportunity.

1. Open the Hyper-V Manager tool.
2. In the pane on the left of the screen, ensure that the local PC is selected.
3. Right-click the media server virtual machine, and select ***Connect...***.
4. When prompted, login to the media server with the following details:
   - Username: `msuser`
   - Default password: `1234`
5. Enter the following command:
   ```
   passwd
   ```
6. Follow the prompts to change the password for the ***msuser*** user.
7. When prompted, exit the login prompt by entering the following command:
   ```
   exit
   ```
   The media server password has been changed.

Media server network settings

The media server is installed with the following default network settings:

Table 6: Default media server network settings

IP Address	10.5.1.3
Subnet Mask	255.0.0.0
Default Gateway	10.0.0.1
DNS	None

If you are connecting the Integra device to a wider local area network, you may have to change these network settings.

Change the media server network settings

You can change the media server network settings after installation.

1. Open the Hyper-V Manager tool.
2. In the pane on the left of the screen, ensure that the local PC is selected.
3. Right-click the media server virtual machine, and select ***Connect...***.
4. When prompted, login to the media server with the following details:

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

IndigoVision recommends that you change the default password after installation.

► For more information, *see "Change the media server password" on page 29*

5. Run the following command:
   ```
   sudo nano /etc/network/interfaces
   ```
6. When prompted for the sudo password, enter the media server password with which you logged in.
7. In the configuration file, navigate to one of the following sections, depending on the your configuration:
   - Static IP configuration (the default after installation)
     ```
     iface eth0 inet static
           address <STATIC_IP>
           netmask <NETMASK>
           network <NETWORK>
           broadcast <BROADCAST>
           gateway <GATEWAY>
           dns-nameservers <DNS_SERVER>
     ```
   - DHCP configuration
     ```
     iface eth0 inet dhcp
     ```
8. If required, edit the configuration file:
   - To switch between static IP and DHCP configurations, replace the configuration file content with the desired format from step 4.
   - To change an existing static IP configuration, edit the appropriate fields.
9. To save your changes to the file, press ***Ctrl + X*** and follow any prompts.
10. Reboot the virtual machine, using the following command:
    ```
    sudo reboot
    ```
    The media server IP configuration is updated.

Install the application server

Install the application server component after the media server.

1. In Windows Explorer, navigate to ***C:\Control Center Web*** and double-click the ***ControlCenterWeb.exe*** file.
   The **End-User License Agreement** dialog opens.
2. Read the agreement, select the check box to accept the agreement, and click ***Install***.
   The Control Center Web Setup Wizard opens.
3. Click ***Next***.
   The **Configuration Options** dialog opens.
4. Update the following fields:
   - **Install IndigoVision Control Center Web to:**
     Enter the location to which you want to install the Control Center Web.
   - **Select the Control Center Site Database location:**
     Enter the location of your Control Center site database. By default, this is installed at ***C:\IndigoSiteDB***.
   - **Specify the Media Server URL:**

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

You must replace SET_MEDIA_SERVER_HOST_HERE with the hostname or IP address of your media server.

► For more information, *see "Media server network settings" on page 29*

IndigoVision recommends that you use a UNC path for remote site databases, instead of mapped drives.

If access to the site database is restricted, the user account installing the application must have access to this location for installation to complete.

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

For more information on SSL/TLS certificates, see "Certificates" on page 27

Choose from the following options:

- **Supply a certificate file**
  If you have an existing certificate, do the following:
  a. Select the ***Supply an Existing certificate file (.pfx)*** radio button.
  b. Click ***Select***, and select the desired file.
  c. Enter the password for the certificate.
  d. Click ***Next***.
- ***Automatically generate a self-signed certificate***
  Control Center Web can automatically generate and install a self-signed certificate. These do not provide as much security as signed certificates but allow installations to be set up quickly and easily. To configure:
  a. Select the ***Generate an untrusted self-signed certificate*** radio button and click ***Next***.
  b. A warning message will be displayed to highlight the security issues associated with this type of certificate. Read the information provided and click ***Confirm*** to proceed.
- **Continue without installing a certificate**
  If you wish to configure a certificate later, you can skip this step. However, Control Center Web will not operate until a valid certificate is correctly installed. To continue:
  a. Select the ***Configure later*** radio button and click next.
  b. A warning will appear highlighting that a certificate is required for Control Center Web to operate. Click ***Next*** to proceed.

7. Click ***Install***.
   The application server installation begins.
8. If prompted to restart the PC, enter `Y`.
   When your PC restarts, the installer automatically starts again when you log back in.

9. When the installation is finished, click ***Close***.
10. If you wish to configure a TLS/SSL certificate after the installation completes, do one of the following:
    - Request a certificate from a Certificate Authority (CA)
    - Use an existing certificate
    - ► For more information, see the Control Center Web Administrator's Guide

Configure NTP on the media server

On Integra appliances, by default the media server is configured to synchronize with the NTP server running on Windows. On Integra View Workstations, the media server is configured to synchronize with Internet time servers.

To ensure that the media server and the rest of the Control Center system are correctly synchronized, configure the media server to use the same time servers as the Windows NTP software on the Integra appliances.

► For more information, *see "Configure NTP on the media server" on page 42*

The installation is complete.

You can login to Control Center Web using a compatible browser.

► For more information, *see "Browser compatibility" on page 27*

You must login using the login details of a valid user in the configured Control Center site database.

For more information on administration of Control Center Web, including troubleshooting and installation of Control Center Mobile, refer to the Control Center Web Administrator's Guide. You can find this in the start menu of the Integra device.

---

6 OPERATIONS

This chapter describes common tasks required for the operation of the Integra device.

Add a camera

Before adding IP cameras to an Integra system, consider how you wish to allocate IP addresses. By default the integrated PoE/PoE+ switch uses an integrated DHCP server.

► For more information, *see "Switch Configuration" on page 19*

To add an IndigoVision camera, refer to the camera's Quick Start Guide to find the default network settings for the device.

Notice *Most IndigoVision cameras default to a static IP address of 10.5.1.10.*
To avoid IP conflicts, only add one such device at a time and reconfigure the network settings as appropriate.

To add a camera to the Integra system, do the following:

1. Connect the camera to an unused numbered port at the rear of the Integra device.
   ► For more information, *see "Integra 8 rear panel connections" on page 11*
   ► For more information, *see "Integra 16 and Integra 24 rear panel connections" on page 12*
2. To reconfigure the camera's network settings, do one of the following:
   - For an IndigoVision camera, use the camera's web configuration page.
   - For a third party camera, use the ONVIF Config Utility.
3. To configure the camera's NTP settings to use the NTP server integrated on the Integra appliance, specify the IP address of the Integra server.
4. Change the default credentials for the device to a more secure configuration.

Notice *The default username and password supplied with IP cameras are for initial configuration only. IndigoVision recommend that you update all devices, including cameras, with secure username and passwords.*

5. From the desktop, open Control Center.
6. Login as an Administrator user.
7. Make sure you are in Setup view.
8. Click ***Visible Devices*** in the Video explorer.
9. Select the required devices from the list in the main window. Shift-click or Control-click to select more than one device at a time.

10. Drag the device you want to add to the site from the list and drop it over the site name. The device is displayed in the Video explorer, below the site.

    Press and hold CTRL while dragging the device to the site to create a device that can then be cloned.

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

Expanding an Integra system

Depending upon the variant, a single Integra appliance can support a number of IP cameras:

- Integra 8: up to 8 IP cameras
- Integra 16: up to 16 IP cameras
- Integra 24: up to 24 IP cameras

To support more cameras, you can expand the system by purchasing additional Integra appliances. For example, a system with an Integra 8 and an Integra 24 can support up to 32 cameras in total.

If you do not use at least one Integra View Workstation to your system, then each Integra appliance operates as a standalone system without access to cameras on other Integra appliances.

► For more information, see Figure 2

Add an Integra View Workstation to an Integra system

Notice *The following information refers to expanding an Integra system across a local area network. For system expansion across a wide area network, refer to the IndigoVision VPN Administrator's Guide.*

To add an Integra View Workstation to an existing Integra system, configure it as the License Server and site database file server for all Integra appliances.

1. Install the workstation.
   ► For more information, *see "Getting Started" on page 15*
2. If you have a Windows domain on your network, add the Integra Workstation to the domain.

Notice *Active Directory is not included with Integra and this guide assumes you do not have access to such infrastructure.*

For improved security and scalability, IndigoVision recommend that you connect Integra appliances to a Windows domain, create Control Center users using Windows authentication only, and manage Windows user accounts using Active Directory.

For more information, refer to the Control Center Security Hardening Guide.

3. If you do not have an existing Windows domain, create or connect to a Windows workgroup instead.
   ► For more information, *see "Add an Integra device to a Windows Workgroup" on page 40*
4. Update the site database on the Integra View Workstation:
   a. From the Start screen, select ***Control Center Site Database Setup***.

b. Select ***Modify an existing site database*** and click ***Next***.
c. Select the site database and click ***Next***. By default, this is installed at ***C:\IndigoSiteDB***.
d. Change the License Server IP to the IP of the Integra View Workstation and click ***Next***.
e. Click ***Next > Finish***.

5. Share the site database on the Integra View Workstation using a Windows network share:
   a. Ensure that the site database is accessible on the remote Integra appliances in your system.
   b. Choose or create a Windows user to access the site database remotely from each Integra appliance or workstation.
      Ensure that this user is able to login on each of the Integra appliances as well as the workstation.

Notice *IndigoVision recommend that you create a new account without Windows Local Administrator privileges.*

6. In Windows Explorer, navigate to the Control Center site database. By default, this is installed at ***C:\IndigoSiteDB***.
7. Right-click the database folder, then click ***Sharing > Share***.
8. Configure the list of users who you wish to allow access to the site database.
   - To allow users to make changes to the site database, add Read/Write permission.
   - To allow users to be operators only, and not make changes to the site database, add Read permission.

Notice *IndigoVision recommend that you keep permissions for network shares as limited as possible to reduce the risk of unauthorized access.*

9. Click ***Share***.
10. Re-add each existing Integra appliance to your system.
    ► For more information, *see "Add an Integra Appliance to an existing Integra system" on page 36*

You can now discover and add cameras, NVRs and Alarm Servers from existing Integra appliances to the site database.

► For more information about adding devices to the site database, refer to the Control Center Help

If you were using Control Center Web on one of your Integra appliances, you should uninstall it from the Integra appliance and run it on the Integra View Workstation.

► For more information about uninstalling Control Center Web, *see "Uninstall Control Center Web" on page 42*
► For more information about setting up Control Center Web, *see "Control Center Web" on page 26*

Add an Integra Appliance to an existing Integra system

Notice *The following information refers to expanding an Integra system across a local area network.*

► For more information on system expansion across a wide area network, *see "IndigoVision VPN" on page 26*.

Before adding an Integra appliance to an existing Integra system, do the following:

- Ensure that an Integra View Workstation is hosting the site database and License Server.
- If the total camera count is greater than 24, ensure that it is an Integra View Mid Workstation that is hosting the License Server.

To add an Integra Appliance to an existing Integra system, do the following:

1. Install the server.
   ► For more information, *see "Getting Started" on page 15*
2. If you have a Windows domain on your network, add the Integra appliance to the domain.
3. If you do not have an existing Windows domain, create or connect to a Windows workgroup instead.
   ► For more information, *see "Add an Integra device to a Windows Workgroup" on page 40*
4. Add the Integra Appliance to the License Federation:
   a. From the Start screen on the Integra View Workstation, select ***License Server Administrator***.
   b. Enter the IP address of the Integra Appliance.
      Alternatively, click ***Discover...*** and select the Integra Appliance from the list.
   c. Click ***Add***.
   d. Click ***OK*** to apply the change.
5. From the Start screen on the Integra Appliance, select ***Control Center Site Database Setup***.
6. Select ***Use an existing site database*** and click ***Next***.
7. Enter the path to the mapped network drive for the site database.
   For example: `\\myIntegraworkstation\SiteDB`
8. Click ***Next > Finish***.
   The Control Center Site Database Setup dialog closes.
9. From the Start screen, select ***NVR-AS Administrator***, and click ***Next*** until you reach the License Server Details page.
10. Change the License Server to the IP address of the Integra View Workstation hosting your Integra View license.
11. Click ***Next > Finish***.
    The NVR-AS Administrator dialog closes.

*IndigoVision recommends that **site database caching** is enabled for all users that connect to a remote site database across the Internet.*

► For more information, *see "Site Database Caching" on page 43*.

You can now add cameras to the Integra Appliance, and they will be available on the local appliance and through Control Center on each of the other Integra devices in your system.

► For more information, *see "Add a camera" on page 33*

Configuring language settings

To change the language Control Center uses, do the following:

1. Start Control Center.
2. In Control Center, select ***Tools > Change Language***.
3. Select your required language from the drop-down list, then click ***OK***.

Notice *Your Operating System may require changes made in this dialog to be authorized.*

4. Shut down and restart Control Center.

Control Center now uses the language which you selected.

Replacing a failed disk on an Integra 8

The Integra 8 has a single video storage disk, with no RAID array. If a disk fails, you should replace it as soon as possible.

Contact IndigoVision Technical Support to supply you with a replacement disk.

When you receive the replacement disk, replace the failed disk by doing the following:

1. Remove the disk caddy containing the failed disk.
2. Remove the failed disk from the disk caddy, and replace it with a disk of the same capacity.
3. Insert the disk caddy back into the Integra appliance.
4. From the Start screen, select ***Computer Management utility > Disk Management***.
5. If the **Initialize Disk** wizard opens, select ***GPT partitioning*** and complete the wizard.
6. Right-click on the unallocated space in the newly added disk and select ***New Simple Volume...***
7. Use the following settings:
   - Set volume size to the maximum size
   - Use the drive letter D
   - Set Allocation Unit Size to `64K`
   - Name the volume appropriately, for example: Video Library

   Leave other settings at their default
8. Select ***Finish***.
   The partition is created.

RAID Management

To manage the video storage disks, you can use the Marvel Tray disk management software installed on the following appliances:

- Integra 16
- Integra 24

To access the disk management interface, do the following:

1. From the desktop, select ***Marvell Tray***.
   The Marvell Storage Utility application opens.
2. When prompted, enter the Windows username and password for the Integra appliance.
   The disk management interface opens.

Using the disk management interface, you can do the following:

- Check the status of the array
- Configure email alerts
  - ► For more information, *see "Receive email alerts for storage faults on Integra 16 and Integra 24" on page 40*
- Replace missing disks

Replacing a failed disk on an Integra 16 or Integra 24

The RAID5 array on the Integra 16 and Integra 24 devices can tolerate a single disk failure without any data loss.

If a disk fails, you should replace it as soon as possible to maintain array redundancy.

Caution *If you remove the disk while the Integra appliance is in operation, the system considers the disk as failed. Do not remove disks while the device is in operation unless they have failed.*

Contact IndigoVision Technical Support to supply you with a replacement disk.

When you receive the replacement disk, replace the failed disk by doing the following:

1. Remove the disk caddy containing the failed disk.
2. Remove the failed disk from the disk caddy, and replace it with a disk of the same capacity.
3. Insert the disk caddy back into the Integra appliance.
4. In the Marvell Storage Utility application, confirm that the disk is incorporated into the array and has started rebuilding.

Notice *The Integra 16 and Integra 24 appliances emit an audible alarm when a RAID array is degraded.*

► For more information, *see "How do I silence the audible alarm from an Integra 16 or Integra 24?" on page 46*

Recreating the RAID5 array on an Integra 16 or Integra 24

If two disks fail at the same time in the video storage array on an Integra device, you must recreate the RAID5 array.

Before you recreate the RAID5 array, ensure that there are four functional disks of the same capacity inserted into the drive bays.

To recreate the RAID5 array, do the following:

1. From the desktop, select ***Marvell Tray***.
   The Marvell Storage Utility application opens.

2. From the device tree, select ***Adapter 0***.
3. Select ***Operation > Create Array***.
4. Include each of the four physical disks in the array.
5. Use the following settings:
   - RAID5
   - ***Disk Cache***: `Enable`
   - ***Stripe Size***: `64K`
6. Select ***Submit*** to create the array.
   The new RAID5 array is created.
7. From the device tree, select the new array.
8. Select ***Create VD***.
9. Use the following settings:
   - ***Cache Mode***: `On`
   - ***Initialize***: `Fast Initialization`
   - ***RAID Size***: Use the maximum size
   - ***Stripe Size***: `64K`
   - ***Gigabyte Rounding***: `None`
10. Select ***Submit*** to create the virtual disk.
    The new virtual disk is created.
11. From the Start screen, select ***Computer Management utility > Disk Management***.
12. If the **Initialize Disk** wizard opens, select ***GPT partitioning*** and complete the wizard.
13. Right-click on the unallocated space in the newly added disk and select ***New Simple Volume...***
14. Use the following settings:
    - Set volume size to the maximum size
    - Use the drive letter D
    - Set Allocation Unit Size to `64K`
    - Name the volume appropriately, for example: Video Library

    Leave other settings at their default
15. Select ***Finish***.
    The partition is created.

Deploy Control Center Web on the Internet

You can deploy Control Center Web for remote access over the Internet, including allowing the use of data connections from mobile service providers.

Deploying any service over the Internet increases your system's exposure to potential malicious activity.

To deploy Control Center Web over the Internet, follow the steps in chapter 5 of the Control Center Web Administrator's guide. You can find this in the start menu of the Integra device.

Add an Integra device to a Windows Workgroup

To add an Integra device to a Windows Workgroup, or create a new Workgroup for Integra devices, do the following:

1. Right-click the ***Start*** icon and select ***System***.
   The System screen opens.
2. In ***Computer name, domain, and workgroup settings*** select ***Change Settings***.
3. In ***Computer Name*** select ***Change...***.
4. Go to ***Member of*** and specify the workgroup.
   This should be a unique string for your network.
5. Click ***OK***.
   The System screen closes.
6. When prompted, reboot the device.

Receive email alerts for storage faults on Integra 16 and Integra 24

You can configure the Integra 16 and Integra 24 appliances to send email notifications when a disk failure occurs on the RAID array used for video storage.

For more information, *see "RAID Management" on page 37*

To configure email notifications, do the following

1. From the desktop, select ***Marvell Tray***.
   The Marvell Storage Utility application opens.
2. From the left-hand pane, select ***Email Notify Settings***.
3. Enter the details of your SMTP server for sending emails.
4. Select ***Test Settings*** to check your settings.
   If the settings are correctly configured, an email is sent to the address you entered in the ***username*** field on this page.
5. Select ***Submit*** to save the settings.
6. From the left-hand pane, select ***Account Management***.
7. Change the email address to the address that you want to receive notifications.
8. Select the types of notification that you want to receive.
   If you want to be notified when a single disk failure occurs and when the array is degraded, select both ***Error*** and ***Warning***.
9. Select ***Submit*** to save the settings.

Request a certificate from a Certificate Authority

You can use a certificate from either a public or private Certificate Authority (CA) with the Integra appliance. The process for requesting a certificate from your Certificate Authority will differ depending on the type of CA you are using.

► For more information, *see "Certificates" on page 27*

Many public CA services will use an online web portal to request the certificate.

Create a certificate request:

1. In the IIS Manager tool, click on the local server in the Connections pane.
2. Select ***Server Certificates***.
3. Select ***Create Certificate Request...*** from the Actions pane.
4. Populate the request with your server details:
   a. ***Common Name***
      This should be the fully qualified domain name (FQDN) that clients will use to access your server, for example `myserver.mydomain.com` or for wildcard certificates `*.mydomain.com`.
   b. ***Organization***
      Your company name.
   c. ***Company Unit***
      Your department within your company.
   d. Enter the address details for your company:
      - ***City/Locality***
      - ***State/Province***
      - ***Country/Region***

   Once entered, click ***Next***.

Notice *Some browsers require a **Subject Alternate Name** field in SSL/TLS certificates before they are considered secure. IIS Manager does not populate this field. You can populate this field using the Certificate Enrollment Wizard.*

► For more information refer to "How to Request a Certificate with a Custom Subject Alternative Name" at https://technet.microsoft.com/en-us/library/ff625722(v=ws.10).aspx

5. In **Cryptographic Service Provider Properties**, select a bit length of at least 2048, and click ***Next***.
6. Specify the location of the request file to save
7. Click ***Finish***.
   The dialog closes.

Process the certificate request on the CA server:

- The exact steps depend on the type of CA you are using.
- At the end of the process, you have a certificate from the CA server for your Integra server .

The Certificate Authority may provide different formats of signed certificate, for example .pfx, .pem, .crt, .cer, .ca-bundle etc. When installing the certificate through IIS, it should be provided in `.cer` format. Alternatively, a `.pfx` format certificate can be installed during Control Center Web installation.

Import the certificate:

1. In the IIS Manager tool, click ***Complete Certificate Request...*** in the action pane.
2. Browse for the certificate file.
3. Rename the certificate file, using a name which you will find easy to remember.
4. Click ***OK***.

You can now use the certificate with Integra.

► For more information, *see "Manually install an existing certificate" on page 42*

Manually install an existing certificate

You can use an existing certificate with the Integra appliance and use it to secure HTTPS connections.

1. In the IIS Manager tool, open the Integra site.
2. Within the main Features View, open the Server Certificates tool.
3. In the Actions pane, select ***Bindings...***.
   The **Site Bindings** dialog opens.
4. In the ***Bindings*** dropdown list, Select ***https***.
5. Click ***Edit***.
6. In the ***SSL/TLS Certificate*** dropdown list, select the certificate you want to use.
7. Click ***OK***.
8. Click ***Close***.

Configure NTP on the media server

IndigoVision recommends that you synchronize time settings on the cameras and the media server using NTP.

Configure the media server to use your site's NTP server.

1. Open the Hyper-V Manager tool.
2. In the pane on the left of the screen, ensure that the local PC is selected.
3. Right-click the media server virtual machine, and select ***Connect...***.
4. When prompted, login to the media server with the following details:
   - Username: `msuser`
   - Default password: `1234`
5. Run the following command:
   ```
   sudo nano /etc/ntp.conf
   ```
6. When prompted for the sudo password, enter the media server password with which you logged in.
7. In the configuration file, remove any existing lines configuring upstream servers, for example:
   ```
   server 10.5.1.2 iburst
   ```
8. In the configuration file, add the following line:
   ```
   server <SERVER> iburst
   ```
   where `<SERVER>` is the name or the IP address of your site's NTP server.
   If you have multiple servers in a pool, add a line for each server in the pool.
9. To save your changes to the file, press ***Ctrl + X*** and follow any prompts.
10. Restart the NTP service, using the following command:
    ```
    sudo systemctl restart ntp
    ```
    NTP is configured on the media server.

Uninstall Control Center Web

To uninstall Control Center Web from an Integra appliance, do the following:

1. From the Start menu, select ***Add or Remove Programs > IndigoVision Control Center Web > Uninstall***.

1. Open the Hyper-V Manager tool.
2. In the pane on the left of the screen, ensure that the local PC is selected.
3. Right-click the media server virtual machine, and select ***Delete***.

Site Database Caching

Site database caching allows operators to use Control Center, even if the remote site database is unavailable due to a network outage. After a remote site database is accessed, Control Center stores a local read-only copy of the database for a specific user or group. If connectivity is lost the local copy is used, allowing that user or group to log in until connectivity is restored.

IndigoVision recommends that site database caching is enabled for all users that connect to a remote site database across the Internet.

To enable caching, follow these steps:

1. Open Control Center and log in.
2. In the **Users Explorer**, right-click the user or group that requires site database caching and select **Properties**.
3. Select the **Settings** tab
4. Select **Cache primary site database**.
5. Click **OK** to close the window.

7 TROUBLESHOOTING

This chapter provides troubleshooting information to resolve common issues.

Camera not displayed in Control Center visible devices

A camera attached to the Integra appliance's integrated switch may not be displayed in the Control Center visible devices pane for the following reasons:

1. There is a problem with either the camera hardware or the network cable.

   In the web configuration page, observe the diagram of the switch ports at the top of the page.

   If the port to which the camera is connected is not displayed as green, then there is a problem with the camera hardware or the network cable.
2. There is not enough power available for all of the connected cameras.

   Check the integrated PoE+ switch can supply enough power for the connected cameras:

   Table 7: Integra PoE+ power

Variant	Maximum PoE+ Power	Warning LED illuminated
Integra8	120W	110W
Integra16	240W	230W
Integra24	360W	350W

3. The camera's IP address and netmask is not compatible with the Integra network configuration.

   Control Center will not be able to discover a camera that is not on the same subnet.

   When adding cameras to an Integra appliance, change the IP settings to use DHCP, or a unique address that is valid for your network. You can do this in the camera's web configuration page.

If the camera is not displayed in the Control Center visible devices pane, but you can access it through the IP address, you can add the camera manually to Control Center.

► For more information, see "Add devices manually" in the Control Center Help.

A camera is displayed as unlicensed in Control Center

Control Center uses a grey icon with red key to display an unlicensed camera.

A camera may be displayed as unlicensed for the following reasons:

1. You are trying to use a camera which is not directly connected to the Integra appliance's integrated switch.

The Integra appliances are only licensed for use with cameras directly connected to the integrated switch.

2. You have recently expanded an Integra system to have more than 24 cameras and an Integra View Mini Workstation is hosting the License Server. That is more cameras than an Integra View Mini Workstation allows and it will need to be replaced by an Integra View Mid Workstation.

How do I silence the audible alarm from an Integra 16 or Integra 24?

The Integra 16 and Integra 24 raise an audible alarm when they detect a degraded RAID array.

You can silence this alarm through the RAID management software.

1. From the desktop, select ***Marvell Tray***.
   The Marvell Storage Utility application opens.
2. When prompted, enter the Windows username and password for the Integra appliance.
3. From the device tree, select ***Adapter 0***.
4. Select ***Mute Alarm***.
   The alarm is silenced.

Notice *To avoid loss of data, degraded RAID arrays should be repaired by replacing the failed disk as soon as possible.*

► For more information, *see "Replacing a failed disk on an Integra 16 or Integra 24" on page 38*

Monitor recordings

To monitor jobs that are currently recording, use IndigoVision's Control Center application.

Control Center allows you to monitor all jobs on your NVR-AS. It allows you to set up recording jobs on NVRs on a visible network. You can also use it to view any existing jobs and their current state (enabled, disabled, recording, etc).

If a transmitter shows ***Trying to record*** in Control Center's recording schedule this indicates a problem with the transmitter. You should check the network connections and that the device is switched on. You should then try to access the device's Web Configuration pages.

NVR Alerts

You should pay particular attention to the following alerts in Control Center:

- **Disk Full**
  Disk full alerts indicate that the Integra disk is full, and that the NVR cannot delete any recordings, for example, because they are protected. Use Control Center to check for recordings marked as Protected and unprotect these recordings.
- **Maximum Recordings**
  These indicate that the maximum number of recordings has been exceeded. This may be because there are too many short recordings.

Recording failure alerts

Recording failure alerts indicate that one or more cameras are not recording correctly.

- Check the network connection between the camera and the Integra.
- Ensure that the maximum number of licensed streams has not been exceeded.

Problems configuring License Federation

License Federation can only be configured if the License Server is version 15.3 or later and the Integra View license is enabled for federation. Integra View Workstations which were delivered with License Server 15.2 will not have the necessary license unless they have been upgraded by contacting IndigoVision Sales Orders.

If you are shown the following error message when opening the License Server Administrator: "Cannot setup federation on a Central License Server with a version 15.2 Integra View license", contact IndigoVision Sales Orders to update your Integra View license by sending a fingerprint file.

Create and send a fingerprint file

Create a fingerprint file using the ***License Manager*** tool.

1. In the **License Manager**, select ***Request a new or updated IndigoVision license*** and click ***Next***.
2. Select where you want the **License Manager** to save a fingerprint file, and click ***Next***.

   The **License Manager** displays the following:
   - The location of the new fingerprint file
   - The contact details for IndigoVision Sales Orders
3. Send the fingerprint file to IndigoVision Sales Order with your IndigoVision order acknowledgment number.

IndigoVision then provides a license file.

Apply a license file

Use the ***License Manager*** tool to apply your IndigoVision license file to the License Server.

1. In the **License Manager**, select ***Apply a new or updated IndigoVision license*** and click ***Next***.
2. Select the IndigoVision license file, and click ***Next***.

   The **License Manager** displays a confirmation notification.
3. Click ***Finish***.

   The new license is applied.