IndigoVision

IndigoVision VPN

Administrator's Guide

IndigoVision

This manual was created on Wednesday, March 27, 2019.

Document ID: IU-CAP-MAN004-2

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

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

1 ABOUT THIS GUIDE

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

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

References

- IndigoVision website: https://www.indigovision.com/
- IndigoVision Integra User Guide: https://www.indigovision.com/download/integra-user-guide
- Control Center Help
- OpenVPN: https://openvpn.net/
- IndigoVision Control Center Installation Guide – Available from the Control Center CD or the support section of the IndigoVision website

Safety notices

This guide uses the following formats for safety notices:

⚠ **Warning**

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

⚠ **Caution**

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

Notice

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

💡

Additional information relating to the current section.

2 OVERVIEW

A Virtual Private Network (VPN) is a technology that creates a secure connection over a less secure network, such as the Internet. The IndigoVision VPN allows administrators to install and configure a VPN hosted on existing IndigoVision hardware, enabling secure remote access from IndigoVision Control Center.

The 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 and Integra

The IndigoVision VPN works in partnership with IndigoVision Integra to support remote access over the Internet.

IndigoVision Integra is an all-in-one appliance that is easy to install and ideal for small deployments in remote locations. It is often desirable to manage such security systems from a central control room or from an unsecured Internet connection when the operator is not at the site.

Remote users can connect using the Internet and access all of the same functionality from anywhere in the world. All the remote user requires is a compatible Windows PC with IndigoVision Control Center and the IndigoVision VPN client installed.

IndigoVision VPN and Integra View

An IndigoVision Integra View can be used to manage multiple Integra devices in a federated system. The IndigoVision VPN can be installed on an Integra View to allow remote Integras to connect securely to the Integra View over the Internet.

The Integra View hosts a License Server, the Control Center Site Database and the IndigoVision VPN server. The Integra appliances connect to the Integra View and use the Site Database hosted on the Integra View. The appliances still run Control Center for local operators but all live and recorded video, as well as alarms, can be viewed from the Integra View as well.

Examples of IndigoVisionVPN with Integra and IndigoVision VPN with Integra View systems are provided.

► For more information, *see "Example system configurations" on page 8*

Operating System Compatibility

The IndigoVision VPN is compatible with IndigoVision Integra and Integra View Workstation products. In addition it can be used to configure other Windows PCs to act as VPN clients.

The IndigoVision VPN software is compatible with the following operating systems:

Table 1: Supported operating systems

Operating system	Supported
Windows 10 64-bit (1607 and later)	Y (recommended)
Windows 8.1 64-bit April 2014 Update	Y
Other	N

Notice *IndigoVision recommend that any PC connected to the Internet is kept up to date with automatic operating system updates, even if the connection is made with a secure VPN.*

3 EXAMPLE SYSTEM CONFIGURATIONS

IndigoVision VPN can be set up in a variety of configurations depending on the system requirements and number of sites involved. Below are a number of sample configurations that may provide guidance when specifying or installing an Integra security system. The IP addresses used are not to be adhered to rigidly but are instead used to demonstrate the IP ranges and subnets involved.

Single Integra with remote access

The following example represents a site with a single Integra device and a remote client connecting using IndigoVisionVPN. This configuration might apply to scenarios such as an office with an Integra security system that users will monitor from a remote location. Remote users can create a secure connection temporarily or have a permanent connection. The remote machine must have both IndigoVision Control Center installed and IndigoVision VPN installed and configured as a VPN Client.

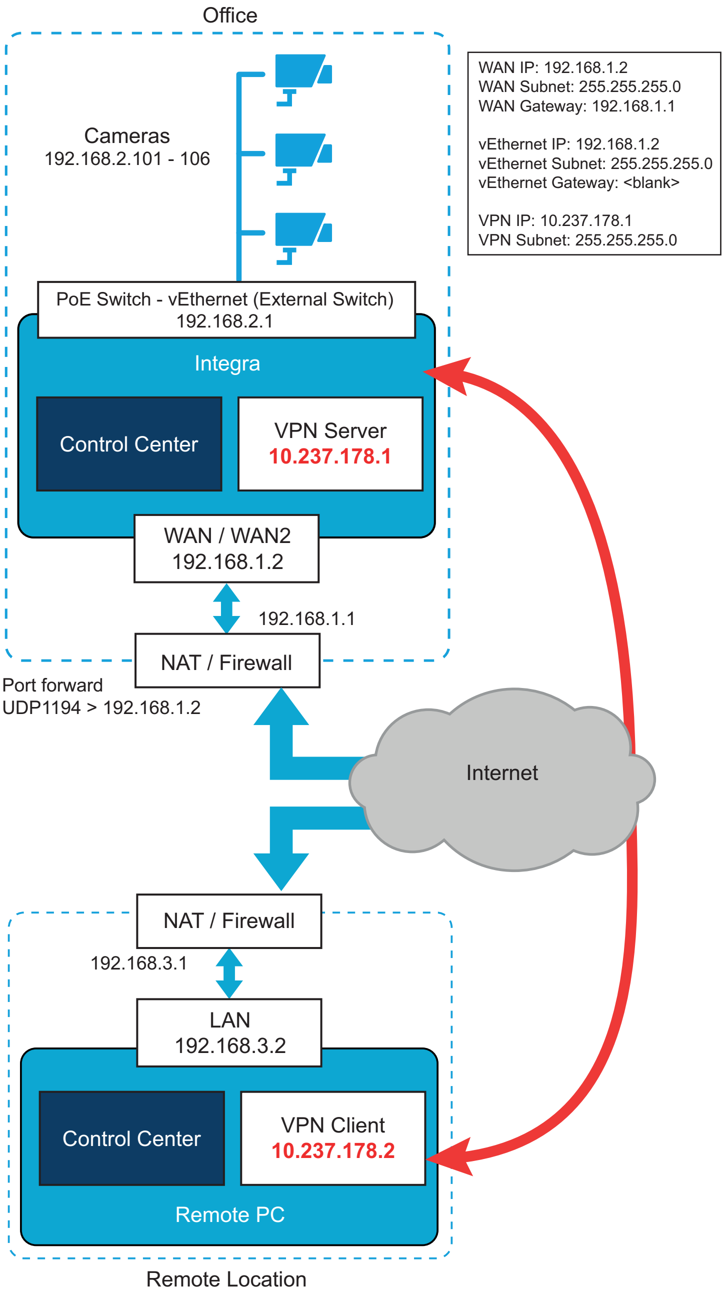


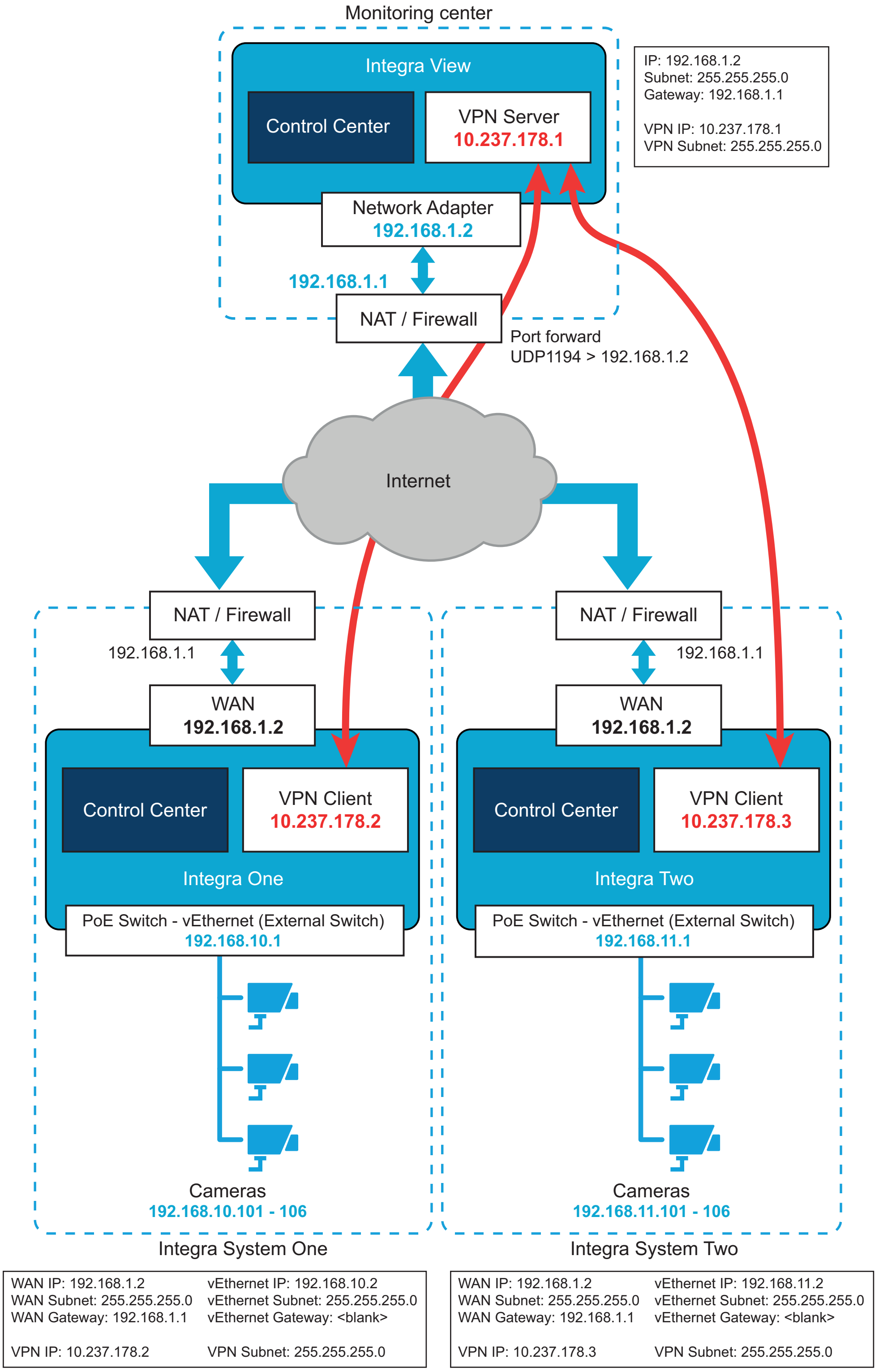
Figure 1: Single Integra with remote access

- The cameras are connected directly to the Integra. The cameras operate on a different subnet to the rest of the Local Area Network.
- Port Forwarding/Mapping must be set up on the Office Router/Firewall to allow access to UDP port 1194 of the Integra.
- The IP address range of the remote client (ie 192.168.3.X in the above diagram) must not conflict with the IP address range of the vEthernet (External Switch) adapter (in this case 192.168.2.X). Additionally, neither may conflict with the VPN address range (10.237.178.X).

Integra View and multiple Integras

The following example is representative of a multi-site Integra security system with an Integra View being used to remotely manage all sites. One such example would be a store chain with a single monitoring center providing surveillance and evidence gathering across multiple stores.

Each store would have its own Integra and cameras recording video locally, with an Integra View located at the monitoring center. The VPN is permanently connected between all sites. Operators at the monitoring center can view live feeds from cameras at any of the sites and search through recordings as if they were accessing locally.



IP: 192.168.1.2
Subnet: 255.255.255.0
Gateway: 192.168.1.1

VPN IP: 10.237.178.1
VPN Subnet: 255.255.255.0

WAN IP: 192.168.1.2	vEthernet IP: 192.168.10.2
WAN Subnet: 255.255.255.0	vEthernet Subnet: 255.255.255.0
WAN Gateway: 192.168.1.1	vEthernet Gateway: <blank>
VPN IP: 10.237.178.2	VPN Subnet: 255.255.255.0

WAN IP: 192.168.1.2	vEthernet IP: 192.168.11.2
WAN Subnet: 255.255.255.0	vEthernet Subnet: 255.255.255.0
WAN Gateway: 192.168.1.1	vEthernet Gateway: <blank>
VPN IP: 10.237.178.3	VPN Subnet: 255.255.255.0

Figure 2: Integra View with multiple Integras

- The cameras on each site are connected directly to the Integra. The cameras operate on a different address scheme to the rest of the Local Area Network.
- Port Forwarding/Mapping must be set up on the monitoring center's Router/Firewall to allow access to UDP port 1194 of the Integra View.
- The IP address range of each of the Integra's vEthernet networks must not conflict with the IP address range of the Integra View. In addition the network range of each

Integra must not conflict with each other. Finally, the IP address ranges must not conflict with the VPN address range. In the above example, the four respective networks in the example above are 192.168.1.X, 192.168.10.X and 192.168.11.X and 10.237.178.X.

- Operators at one store can access camera feeds and recordings from another store if needed.

4 ALLOW REMOTE ACCESS TO A SINGLE INDIGOVISION INTEGRA APPLIANCE

If you have a single IndigoVision Integra 8, 16 or 24 appliance that you wish to make available to authorized remote clients, follow these steps:

1. Configure the network on the Integra
2. Install IndigoVision VPN on the Integra appliance and configure the Integra as a VPN server using the IndigoVision VPN Configuration Tool
3. Configure your router and firewall to allow incoming connections to the VPN server on your public Internet connection used by the Integra appliance.
4. Configure the Control Center Site Database so as the License Server is available to connecting clients.
5. Then for each client configure the follow items:
   - IndigoVision VPN to connect to the VPN
   - Control Center Site Database
   - Date and time settings

Configure the integrated switch network

In order to use an IndigoVision Integra remotely, it must be connected to a network with Internet access. IndigoVision recommend that the WAN1 or WAN2 port is used for this connection to separate the devices attached to the Integra switch from the rest of the local area network.

The Integra’s integrated switch network must also be configured so as the cameras attached to the switch can communicate using the VPN.

Table 2: Default Integra switch network configuration

Switch IP Address	10.5.1.1
Switch subnet mask	255.0.0.0
Default Gateway	10.0.0.1
DHCP Address Range Start	10.5.1.101
Integra PC address – vEthernet (External Switch)	10.5.1.2

For use with a VPN, IndigoVision recommend that a smaller subnet is chosen for the switch to minimize the chance of a network overlap. This is essential for systems with multiple Integra appliances and an Integra View Workstation, where there must be no overlap between the different switch networks.

For the following example, we will assume that we want to change the configuration to the following:

Table 3: Example reconfigured network

Switch IP Address	192.168.20.1
Switch subnet mask	255.255.255.0
Switch default gateway	192.168.20.2
vEthernet (External Switch) IP address	192.168.20.2
vEthernet (External Switch) subnet mask	255.255.255.0
vEthernet (External Switch) default gateway	<blank>
DHCP range start	192.16.20.101

IndigoVision recommend a subnet mask of 255.255.255.0 or higher to keep the subnet small. Both the switch IP address and Integra's vEthernet IP address must be on the same subnet.

1. Any cameras that are configured with a static IP address will no longer be accessible after the following steps. These cameras should be reconfigured to a new address or configured to use DHCP before commencing.
2. From the Desktop of the Integra, double-click the **Switch configuration** shortcut on the desktop to login to the switch web configuration page using a web browser. Alternatively, use Internet Explorer with the default switch IP address of http://10.5.1.1. By default, the username and password are `admin`.
3. Select ***System > IP Configuration > IPv4*** from the left hand pane.
4. Enter the new IP address and subnet mask of the switch into the respective fields. Enter the new IP address of the ***vEthernet (External Switch)*** in the Default Gateway field. For the above example:

   IPv4 Address: 192.168.20.1

   Subnet Mask: 255.255.255.0

   Default Gateway: 192.168.20.2
5. Click ***Apply***, then read and accept the warning message to apply the changes.

Warning

As the IP address has been changed, the web configuration page will now be unreachable until steps 6-9 are completed. Additionally, any loss in power before step 15 is completed will erase any changes made to the switch configuration.

6. From the Start Menu on the Integra open **Network and Sharing Center**.
7. Click on ***Change adapter settings***.
8. Right-click on the ***vEthernet (External Switch)*** adapter and select ***Properties***
9. Change the IP configuration to the desired address. Note that since the Default Gateway for the Integra is configured on another network interface (WAN1/WAN2), it should be left blank here. For the above example:

   IPv4 Address: 192.168.20.2

   Subnet Mask: 255.255.255.0

   Default Gateway: <blank>
10. In Internet Explorer, browse to the new address for the switch.
11. Select ***Advanced Features > DHCP Server***.
12. 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 the above example, enter `192.168.20.101`.

13. Select ***Apply***.
14. Reboot all cameras that use DHCP to dynamically assign their IP addresses.

    This will give each a new address compatible with the switch's new network configuration.
15. At the top-left of the window, click ***Save Running Configuration*** to store the switch configuration permanently.
16. Close the success dialog box that appears.
17. From the Desktop on the Integra, right-click the ***Switch configuration*** shortcut and select ***Properties***.
18. In the URL field, update the address with the new switch IP address (http://192.168.20.1).
19. Click ***OK*** to close the window.

Install IndigoVision VPN

To install the IndigoVision VPN software, follow these steps:

1. Download the IndigoVision VPN installer from the Support page on the IndigoVision website or extract it from the Control Center installation media.

   ► For more information, *see "References" on page 5*
2. Double-click the ***setup.exe*** to start the installation process.
3. Click ***Next***.

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

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

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

   The IndigoVision VPN Installation begins. Accept any security dialogs that open during installation.
7. Click ***Finish*** to close the installer.

   A window may open indicating that the PC needs restarted to complete the installation.

   You must restart the PC before running the IndigoVision VPN Configuration Tool.

   The installation is complete.

Configure the Integra as a VPN server

To configure an IndigoVision Integra as a VPN server, perform the following steps on the Integra appliance:

1. If the **IndigoVision VPN Configuration Tool** is not already open, select

   Start Menu > IndigoVision > IndigoVision VPN Configuration Tool
2. Click ***Next*** to begin the configuration.

   The **Installation Mode** page is shown.
3. Select ***Install IndigoVision VPN as a new server*** and click ***Next***.

If the IndigoVision VPN has been configured as a server previously, a dialog will be displayed stating that the existing configuration will be overwritten. Select ***Overwrite*** to continue with the configuration.

The ***VPN Network*** page is shown.

If local area network used by the Integra running the VPN server or client PCs will conflict with the default VPN network displayed on this page, then the VPN network will need to be changed.

The VPN network must be a subnet within one of the standard IPv4 private network ranges (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16).

Notice *If the VPN network is changed, the server IP address on the VPN will also change. Take note of the server IP address listed on this page. This will be needed to complete the configuration later.*

4. Click ***Next***.

   The **Authentication** page is shown.

5. Choose a username and password for this server.

   Clients using the VPN will need to provide these details in order to connect.

   The username and password is used by client PCs to connect to the VPN and access the Control Center Site Database.

   The password must be entered twice to confirm it has been entered correctly.

   An indication of your password’s strength is displayed to assist in password selection.

6. Click ***Next***.

   If the **Password strength warning** is shown:

   - Click ***Yes*** to continue.
   - Click ***No*** to go back and choose a more secure password.

Notice *This username and password protects your IndigoVision security system from access by unauthorized parties. It is essential that a unique username and strong password are chosen to keep your system safe. IndigoVision recommends that you pay attention to the password strength warnings and choose passwords that:*

- Are over 11 characters long
- Avoid common surveillance device passwords, for example `Admin1234`
- Use a mixture of alpha-numeric characters and symbols
- Contain multiple uncommon words
- Avoid repeated words and characters

Notice *Consider changing the VPN password on a regular basis to keep the system secure.*

► For more information, *see "Change the VPN password or other server settings" on page 34*

If the **User account warning** is shown:

- Click ***Yes*** to continue.
- Click ***No*** to go back and pick a different username.

IndigoVision VPN will create or modify an existing Windows user based on the specified username in order to make the Control Center Site Database available through a network share.

The **Integra Switch Network** page is shown.

7. Enter the IP address and subnet mask of the integrated switch and vEthernet adapter on this Integra, and the camera DHCP start address.

   This must match the details from the configured network for the Integra.

   ► For more information, *see "Configure the integrated switch network" on page 14*

8. Click ***Next***.

   The **Integra WAN Network** page is shown. Enter the WAN IP address and subnet mask. This must match the details from the Integra's WAN1/WAN2 network interface.

9. Click **Next**.

   The **Configuring VPN Server** page is shown.

10. Wait for the configuration to complete then click ***Next***.

    The **Generate Client Configuration** page is shown.

11. Enter the public-facing address and port that VPN clients will use to connect to this VPN server.

    The address should be either a fully qualified domain name or a static IP address for your public facing Internet connection.

Notice *If you do not have a static IP for your Internet connection, then you could use a dynamic DNS service.*

► For more information, *see "Configure Dynamic DNS for the IndigoVision VPN Server" on page 33*

The port specified here is the port that you will open on your router and firewall so as connecting clients are forwarded to the VPN server.

Notice *For increased security, IndigoVision recommend that you choose a random port above 8000 to hide the VPN technology being used from potential attackers.*

12. Click ***Browse…*** and choose a location to save the client configuration file.

13. Click ***Next***.

    The **Server Configuration Complete** page is shown.

14. Click ***Finish***.

The configuration tool may request that the Integra is restarted. Either click ***Restart Now*** to allow the PC to restart, or ***Restart Later*** if you intend to manually restart the PC at later time.

⚠ Warning *If a restart is requested, connecting VPN clients may not be able to access the cameras attached to the Integra until the Integra is restarted.*

The VPN software is now configured and the IndigoVision VPN Configuration Tool closes.

Configure the router and firewall

So that external devices on the Internet, running the IndigoVision VPN client software can connect to the Integra appliance, the router and firewall (see) for the Local Area Network (LAN) must open a port that redirects to the Integra.

► For more information, *see "Configure a router and firewall to expose the IndigoVision VPN" on page 32*

Configure the Site Database on the VPN server

In order that connecting VPN clients can verify the IndigoVision Integra license, the Control Center Site Database must list the IndigoVision License Server on the VPN IP address used by the Integra that hosts the VPN.

To reconfigure the Site Database follow these steps:

1. Open the Control Center Site Database Setup Utility.

   Start Menu > IndigoVision > Control Center Site Database Setup
2. Select **Modify an existing Site Database** and click ***Next***.

   The **Modify Existing Site Database** dialog is shown.
3. Click ***Next***.

   The **License Server Details** dialog is shown.
4. Enter the IP address of the Integra on the IndigoVision VPN; default: 10.237.178.1.

   There is no need to make any other changes.
5. Click ***Next*** then click ***Finish***.

   The Site Database has been configured.

The IndigoVision Integra has now been configured as a VPN server such that authorized clients can connect and use Control Center remotely.

Configure IndigoVision VPN on each client

After the VPN server has been configured, the IndigoVision VPN can be installed and configured on the client PCs. Before starting to configure a client, ensure the following is available:

- The username and password for the VPN server
- The ***IndigoVision VPN – Client Config.zip*** file created by the IndigoVision VPN Configuration Tool on the VPN server
- The IndigoVision VPN installation files

To configure the client PC follow these steps:

1. Install the IndigoVision VPN client on the client PC.

   ► For more information, *see "Install IndigoVision VPN" on page 16*
2. If the **IndigoVision VPN Configuration Tool** is not already open, Select ***Start Menu > IndigoVision > IndigoVision VPN Configuration Tool***
3. Click ***Next*** to being configuration.

   The **Installation Mode** page is shown.
4. Choose between two different client configuration modes:

5. Select either **Install IndigoVision VPN as an on-demand client for occasional use** or **Install IndigoVision VPN as a permanent client** and click ***Next*** then follow the appropriate steps.

On-Demand client: In this mode, the tool will setup the **OpenVPN GUI** tool to allow the user to choose when to connect or disconnect to the VPN.

Permanent client: In this mode, the tool will setup OpenVPN to run as a Windows service in the background. It will connect when the PC is started and reconnect automatically if the VPN connection is lost for any reason.

Notice *If the IndigoVision VPN has been configured as a server previously, a dialog will be displayed stating that the existing configuration will be overwritten. Select* ***Overwrite*** *to continue with the configuration.*

On-Demand client configuration

If you chose to install the on-demand client, follow these steps:

1. Locate the ***IndigoVision VPN – Client Config.zip*** file generated by the server.
2. Enter the username and password for the VPN server.
3. Choose an available drive letter to mount the remote Control Center Site Database.

   If there are existing mounted network drives on your PC, the letter may still appear in the list of available drive letters. Take care to choose a letter that is not already allocated. If the remote Control Center Site Database is already mounted then its drive letter will already be selected, in this case it is safe to keep the same drive letter.
4. Click ***Next***.

   The **Configuring VPN Client** page is shown.

   You will be prompted to connect to the VPN.
5. Use the OpenVPN GUI from the system tray to connect to the VPN server when prompted.
   - ► For more information on using the OpenVPN GUI, *see "Use the OpenVPN GUI to connect or disconnect to the VPN" on page 32*
6. Click ***OK*** after the VPN is connected.

   The Control Center Site Database network share will be mounted using the selected drive letter.

   The **Client Configuration Complete** page is shown.
7. Click ***Next*** after the configuration completes.
8. Click ***Finish*** to exit.

Permanent client configuration

If you choose to install the permanent client, follow these steps:

1. Locate the ***IndigoVision VPN – Client Config.zip*** file generated on the server.
2. Enter the username and password for the VPN server.
3. Choose an available drive letter to mount the remote Control Center Site Database.

   If there are existing mounted network drives on your PC, the letter may still appear in the list of available drive letters. Take care to choose a letter that is not already allocated. If the remote Control Center Site Database is already mounted then its drive letter will already be selected, in this case it is safe to keep the same drive letter.

4. Enter the username and password for the VPN server.
5. Click ***Next***.

   The **Configuring VPN Client** page is shown.
6. Click ***Next*** once the configuration completes.

   The **Client Configuration Complete** page is shown.
7. Click ***Finish*** to exit.

The PC is now connected to the IndigoVision VPN server. It will connect automatically when the PC is restarted. If you wish to manually connect or disconnect, the ***OpenVPNService*** can be started or stopped from the Windows Services applet.

Configure the Site Database on the VPN client PC

In order to use Control Center on the client PC, it must be configured to use the remote site database.

1. Open the Control Center Site Database Setup Utility, ***Start Menu > IndigoVision > Control Center Site Database Setup***
2. Select ***Modify*** an existing Site Database and click ***Next***.

   The **Use Existing Site Database** dialog is shown.
3. Enter mapped network drive, for example: ***D:\***
4. Click ***Finish***.

Control Center can now be opened on the client and, as long as the VPN is connected, it should be possible to access all of the video and alarm features available on the Integra.

Date and Time settings

⚠ **Caution**

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

It is important that the remote Integra appliance and the client PCs are synchronized using NTP.

Configure the Integra as an upstream time server for all of the client PCs using its address on the VPN; default 10.237.178.1.

A Windows NTP client and server implementation can be found on the Control Center CD or downloaded from the support section of the IndigoVision website [1]. More information on installing and configuring the NTP server on Windows can be found in the **Control Center Installation Guide**.

► For more information, *see "References" on page 5*

5 USE AN INDIGOVISION INTEGRA VIEW WITH REMOTE INTEGRAS

If you have multiple IndigoVision Integra appliances that you wish to connect together using an unsecured network, such as the Internet, follow these steps:

1. Choose a network configuration on each of the Integra appliances.
2. Install IndigoVision VPN on the Integra View and configure the Integra View as a VPN server using the IndigoVision VPN Configuration Tool.
3. Configure your router and firewall to allow incoming connections to the VPN server on your public Internet connection used by the Integra View.
4. Configure the Control Center Site Database so that the License Server is available to connecting clients.
5. For each Integra appliance configure the following items:
   - IndigoVision VPN to connect to the VPN
   - NVR and Control Center Site Database
   - Date and time settings
6. Add the Integra appliances to the License Federation on the Integra View.
7. Add the cameras, NVRs and Alarm Servers to the Site Database on the Integra View.

Choose a network configuration

When connecting multiple remote sites together, care must be taken to assign network addressing schemes for all Integra appliances that will be compatible once they are connected directly in the VPN.

Before setting up an IndigoVision VPN, consider the network configuration of all of the Integra appliances and the Integra View and change their configuration so that:

- Each Integra appliance uses a unique switch subnet that does not overlap with any of the other Integra appliance switches.
- Each Integra appliance uses a switch subnet that has a small IP range to make future expansion easier.
- Neither the Integra appliances nor the Integra View uses a network that overlaps with the VPN network; default 10.237.178.0/255.255.255.0.

To change the IP configuration for the integrated switch on each Integra appliance, follow the steps used to configure the integrated switch network.

Install IndigoVision VPN

To install the IndigoVision VPN software, follow these steps:

1. Download the IndigoVision VPN installer from the Support page on the IndigoVision website or extract it from the Control Center installation media.

   ► For more information, *see "References" on page 5*
2. Double-click the ***setup.exe*** to start the installation process.
3. Click ***Next***.

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

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

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

   The IndigoVision VPN Installation begins. Accept any security dialogs that open during installation.
7. Click ***Finish*** to close the installer.

   A window may open indicating that the PC needs restarted to complete the installation.

   You must restart the PC before running the IndigoVision VPN Configuration Too

Configure the integrated switch network

In order to use an IndigoVision Integra remotely, it must be connected to a network with Internet access. IndigoVision recommend that the WAN1 or WAN2 port is used for this connection to separate the devices attached to the Integra switch from the rest of the local area network.

The Integra's integrated switch network must also be configured so as the cameras attached to the switch can communicate using the VPN.

Table 4: Default Integra switch network configuration

Switch IP Address	10.5.1.1
Switch subnet mask	255.0.0.0
Default Gateway	10.0.0.1
DHCP Address Range Start	10.5.1.101
Integra PC address – vEthernet (External Switch)	10.5.1.2

For use with a VPN, IndigoVision recommend that a smaller subnet is chosen for the switch to minimize the chance of a network overlap. This is essential for systems with multiple Integra appliances and an Integra View Workstation, where there must be no overlap between the different switch networks.

For the following example, we will assume that we want to change the configuration to the following:

Table 5: Example reconfigured network

Switch IP Address	192.168.20.1

Switch subnet mask	255.255.255.0
Switch default gateway	192.168.20.2
vEthernet (External Switch) IP address	192.168.20.2
vEthernet (External Switch) subnet mask	255.255.255.0
vEthernet (External Switch) default gateway	<blank>
DHCP range start	192.16.20.101

IndigoVision recommend a subnet mask of 255.255.255.0 or higher to keep the subnet small. Both the switch IP address and Integra's vEthernet IP address must be on the same subnet.

1. Any cameras that are configured with a static IP address will no longer be accessible after the following steps. These cameras should be reconfigured to a new address or configured to use DHCP before commencing.
2. From the Desktop of the Integra, double-click the **Switch configuration** shortcut on the desktop to login to the switch web configuration page using a web browser. Alternatively, use Internet Explorer with the default switch IP address of http://10.5.1.1. By default, the username and password are `admin`.
3. Select ***System > IP Configuration > IPv4*** from the left hand pane.
4. Enter the new IP address and subnet mask of the switch into the respective fields. Enter the new IP address of the ***vEthernet (External Switch)*** in the Default Gateway field. For the above example:

   IPv4 Address: 192.168.20.1

   Subnet Mask: 255.255.255.0

   Default Gateway: 192.168.20.2
5. Click ***Apply***, then read and accept the warning message to apply the changes.

⚠ **Warning**

As the IP address has been changed, the web configuration page will now be unreachable until steps 6-9 are completed. Additionally, any loss in power before step 15 is completed will erase any changes made to the switch configuration.

6. From the Start Menu on the Integra open **Network and Sharing Center**.
7. Click ***Change adapter settings***.
8. Right-click the ***vEthernet (External Switch)*** adapter and select ***Properties***
9. Change the IP configuration to the desired address. Note that since the Default Gateway for the Integra is configured on another network interface (WAN1/WAN2), it should be left blank here. For the above example:

   IPv4 Address: 192.168.20.2

   Subnet Mask: 255.255.255.0

   Default Gateway: <blank>
10. In Internet Explorer, browse to the new address for the switch.
11. Select ***Advanced Features > DHCP Server***.
12. 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 the above example, enter 192.168.20.101.
13. Select ***Apply***.

14. Reboot all cameras that use DHCP to dynamically assign their IP addresses. This will give each a new address compatible with the switch’s new network configuration.
15. At the top-left of the window, click ***Save Running Configuration*** to store the switch configuration permanently. Close the success dialog box that appears.
16. From the Desktop on the Integra, right-click the ***Switch configuration*** shortcut and select ***Properties***.
17. In the URL field, update the address with the new switch IP address (http://192.168.20.1).
18. Click ***OK*** to close the window.

Configure the Integra View as a VPN Server

To configure an IndigoVision Integra View as a VPN server, perform the following steps:

1. Install the IndigoVision VPN software.

   ► For more information, *see "Install IndigoVision VPN" on page 16*
2. If the IndigoVision VPN Configuration Tool is not already open, it can be started from the Start menu, select ***Start Menu > IndigoVision > IndigoVision VPN Configuration Tool***
3. Click ***Next*** to begin configuration.

   The **Installation Mode** page is shown.
4. Select ***Install IndigoVision VPN as a new server*** and click ***Next***.

   If the IndigoVision VPN has been configured as a server previously, a dialog is displayed stating that the existing configuration will be overwritten. Select ***Overwrite*** to continue with the configuration.

   The ***VPN Network*** page is shown.

   If local area network used by the Integra running the VPN server or client PCs will conflict with the default VPN network displayed on this page, then the VPN network will need to be changed.

   The VPN network must be a subnet within one of the standard IPv4 private network ranges (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16).

Notice *If the VPN network is changed, the server IP address on the VPN will also change. Take note of the server IP address listed on this page. This will be needed to complete the configuration later.*

5. Click ***Next***.

   The **Authentication** page is shown.
6. Choose a username and password for this server.

Notice *The password will be used in conjunction with the Integra Device Name (configured later) to connect to the VPN. The username and password will also be used to access the Control Center Site Database through the VPN and by any non-Integra client that connects to the VPN.*

   The password must be entered twice to confirm it has been entered correctly.

   An indication of your password’s strength is displayed to assist in password selection.

7. Click ***Next***.

If the **Password strength warning** is shown.

- Click ***Yes*** to continue.
- Click ***No*** to go back and pick a more secure password.

Notice *This username and password protects your IndigoVision security system from access by unauthorized parties. It is essential that a unique username and strong password are chosen to keep your system safe. IndigoVision recommends that you pay attention to the password strength warnings and choose passwords that:*

- Are over 11 characters long
- Avoid common surveillance device passwords, for example `Admin1234`
- Use a mixture of alpha-numeric characters and symbols
- Contain multiple uncommon words
- Avoid repeated words and characters

Notice *Consider changing the VPN password on a regular basis to keep the system secure.*

► For more information,*see "Change the VPN password or other server settings" on page 34*

If the **User account warning** is shown:

- Click ***Yes*** to continue
- Click ***No*** to go back and pick a different username

Notice *IndigoVision VPN will create or modify an existing Windows user based on the specified username in order to make the Control Center Site Database available through a network share.*

The **Integra VPN Clients** page is shown.

8. For each Integra appliance that will be connected to the VPN:
   a. Click ***Add***.
      The **Add New Integra Device** page is shown.
   b. Specify a name for this Integra.
      This name identifies the Integra appliance to the VPN server and must be unique among all other appliances.
   c. Select the Integra model from the list.
   d. Enter the IP address and subnet mask of the **vEthernet** network connection on this Integra appliance.
   e. Enter the IP address and subnet mask of the **WAN** network connection on this Integra appliance.
   f. Enter the **camera DHCP start address** on this Integra appliance.
   g. Click ***Add***.
      The **Add New Integra Device** page is closed and the Integra is added to the **Integra VPN Clients** page.
9. Click ***Next***.
   The **Configuring VPN Server** page is shown.
10. Wait for the configuration to complete then click ***Next***.
    The **Generate Client Configuration** page is shown.

11. Enter the public-facing address and port that VPN clients will use to connect to this VPN server.

The address should be either a fully qualified domain name or a static IP address for your public facing Internet connection.

Notice *If you do not have a static IP for your Internet connection, then you could use a dynamic DNS service.*

► For information, *see "Configure Dynamic DNS for the IndigoVision VPN Server" on page 33*

The port specified here is the port that you will open on your and firewall so as connecting clients are forwarded to the VPN server.

Notice *For increased security, IndigoVision recommend that you choose a random port above 8000 to hide the VPN technology being used from potential attackers.*

12. Click ***Browse…*** and choose a location to save the client configuration file.
13. Click ***Next***.

    The **Server Configuration Complete** page is shown.
14. Click ***Finish***.

The VPN software is now configured and the IndigoVision VPN Configuration Tool will close. It is now time to configure the router and firewall to allow external connections to the VPN server.

Configure the router and firewall Integra View

In order that the Integra appliances running the IndigoVision VPN client software can connect to the IndigoVision VPN using the Internet, the router and firewall (see Figure 2) for the Local Area Network (LAN) must open a port that redirects to the Integra View.

► For more information, *see "Configure the router and firewall" on page 19*

Configure IndigoVision VPN on each Integra appliance

Now that the Integra View is configured to accept incoming VPN client connections, the IndigoVision VPN can be installed on the remote Integra appliances.

Before starting to configure an Integra as a client, ensure the following is available:

- The Integra name and password that was configured on the VPN server
- The ***IndigoVision VPN – Client Config.zip*** file created by the IndigoVision VPN Configuration Tool on the VPN server
- The IndigoVision VPN installation files

For each Integra appliance, follow these steps:

1. Install the IndigoVision VPN software.

   ► For more information, *see "Install IndigoVision VPN" on page 16*

2. If the IndigoVision VPN Configuration Tool is not already open, it can be started from the Start menu, select ***Start Menu > IndigoVision > IndigoVision VPN Configuration Tool***
3. Click ***Next*** to being configuration.

   The **Installation Mode** page is shown.
4. Select ***Install IndigoVision VPN as a permanent client*** and click ***Next***.

Notice *If the IndigoVision VPN has been configured previously as a server, a dialog will be displayed stating that the existing configuration will be overwritten. Select* ***Overwrite*** *to continue with the configuration.*

The **Client Configuration** page is shown.

5. Browse for the ***IndigoVision VPN – Client Config.zip*** file generated on the server.
6. Choose an available drive letter to mount the remote Control Center Site Database.

   If there are existing mapped network drives on your PC, take care to choose a letter that is not allocated.
7. Enter the Integra name and password for the VPN server.

   The **Integra name** is the unique identifier specified on the IndigoVision VPN server when this Integra appliance's switch IP and subnet mask were entered. The matching Integra name must be used here, or the VPN will not be able to access the devices on this Integra's switch.
8. Click ***Next***.

   The **Configuring VPN Client** page is shown.
9. Click ***Next*** once the configuration completes.

   The **Client Configuration Complete** page is shown.
10. Click ***Finish***.

The Integra appliance is now connected to the VPN, providing a secure network connection between the Integra View and this Integra. This connection will automatically be made whenever the system is restarted.

NVR Configuration

The NVR on the Integra must be configured to use the vEthernet network interface and to use the License Server on the Integra View:

1. From the Start menu, select ***NVR-AS Administrator***, and click ***Next*** until you reach the **License Server Details** page.
2. Change the License Server to the IP address of the Integra View Workstation on the VPN; default: 10.237.178.1.

   This is the fixed IP address of the Integra View Workstation on the IndigoVision VPN.
3. Click ***Next*** until you reach the **Network Settings** page.
4. On the **Network Address** drop-down menu, select the address of the vEthernet adapter; default: 10.5.1.2.
5. Click ***Next > Finish***.

   The **NVR-AS Administrator** dialog closes.

Site Database Configuration

In order to use Control Center on the Integra appliance, it must be configured to use the remote site database.

1. Open the Control Center Site Database Setup Utility, select ***Start Menu > IndigoVision > Control Center Site Database Setup***
2. Select ***Modify an existing Site Database*** and click ***Next***.

   The **Use Existing Site Database** dialog is shown.
3. Enter the mapped network drive letter chosen when configuring the VPN client, for example: ***D:\***
4. Click ***Finish***.

Before Control Center can be used with additional cameras, the License Federation must be established.

Date and Time settings

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

It is important that the remote Integra appliances and the Integra View are synchronized using NTP.

Configure the Integra View Workstation as an upstream time server for all of the Integra appliances using its address on the VPN; default: 10.237.178.1.

For more information on configuring the NTP settings on an Integra or Integra View Workstation, refer to **Date and Time Settings** in the Integra User Guide

► For more information, *see "References" on page 5*

Add the Integra appliances to the License Federation

In order that the Integra View can add all of the remote cameras to its Site Database, it must be given access to the License Servers running on the remote Integra appliances.

On the Integra View:

1. From the Start screen on the Integra View Workstation, select ***License Server Administrator***.
2. For each Integra appliance, enter the IP address of the Integra appliance’s ***vEthernet (External Switch)*** Adapter and click ***Add***.
3. After all the Integras have been added, click ***OK*** to apply the changes.

Add the cameras, NVRs and Alarm Servers to the Site Database

Now that the Integra appliances and Integra View are connected, the Site Database is available on all connected devices, and the License Server on the Integra View has been configured, the cameras and NVRs from the remote Integra appliances can be added to the Site Database.

To populate the Site Database:

1. Log into Control Center as an Administrator on any of the connected Integra appliances or the Integra View.
2. For each camera that is directly connected to the current Integra, add it using device discovery in the Setup view of Control Center in the normal manner.
3. For each camera connected to a remote Integra through the VPN either:
   a. Login into Control Center on that remote Integra and add the cameras to the Site Database with the aid of device discovery.
   b. Or add the device to the Site Database manually through the Setup view.

      For more information on adding devices manually refer to **Add devices manually** in the Control Center Help.

      ► For more information, *see "References" on page 5*

Notice *IndigoVision Camera Gateway or VSM cameras cannot be added manually. Such cameras must be added to the site database using Control Center on the Integra with a direct LAN connection to the service.*

The network of distributed Integra appliances is now configured to work securely across the Internet.

6 OPERATIONS

Configure a router and firewall to expose the IndigoVision VPN

In order that external devices on the Internet running the IndigoVision VPN client software can connect to the IndigoVision VPN server, the router and firewall for the Local Area Network (LAN) must open a port that redirects to the Integra.

The incoming port that the router exposes must match the value entered in the IndigoVision VPN configuration tool on the **Generate Client Configuration** page. The router must forward all UDP protocol traffic on this public-facing port to 1194 on the VPN server.

For details on how to configure port forwards on the router contact your IT department or refer to the router’s user documentation.

Table 6: Firewall rules for IndigoVision VPN

Service	Protocol	Destination Port	Dir	Comments
OpenVPN Server	UDP	1194	IN	Connections from remote VPN clients

Use the OpenVPN GUI to connect or disconnect to the VPN

The OpenVPN GUI can be used to control the connection on a client PC to the IndigoVision VPN. It is enabled by the IndigoVision VPN Configuration Tool if you select ***Install IndigoVision VPN as an on-demand client for occasional use*** when configuring the client.

When enabled, the tool is visible in the Windows system tray.

To connect to the IndigoVision VPN, follow these steps:

1. Right-click on the OpenVPN GUI icon and click on ***Connect***.

   The **OpenVPN Connection** dialog is shown, with a prompt to provide the username and password.
2. Enter the username and password for this IndigoVision VPN server.

   Optionally check the ***Save password*** box to avoid having to enter the credentials the next time you connect.
3. Click ***OK***.

   After a short while the connection is established and the **OpenVPN Connection** dialog closes.

► If there is a problem establishing a connection to the VPN server, *see "The IndigoVision VPN client cannot connect to the VPN server" on page 38*.

To disconnect from the IndigoVision VPN:

1. Right-click on the OpenVPN GUI icon.
2. Click on ***Disconnect***.

   The connection to the VPN server will be closed immediately.

Configure Dynamic DNS for the IndigoVision VPN Server

Domain Name Services (DNS) provide a mapping between a user defined domain name, for example integra.indigovision.com, and an IP address. Dynamic DNS provides a domain name, for an IP address that changes over time.

Many Internet service providers sell connections that provide a dynamic public IP address, rather than a static IP address. In this case it is harder to host any service through the Internet connection, as connecting clients do not know what the address will be. If you do not have a static public IP address, you can use a dynamic DNS service to host an IndigoVision VPN server with a constant public-facing domain name.

IndigoVision do not provide a dynamic DNS service, but there are many dynamic DNS providers available, both premium and free, with each offering a different Service Level Agreement. For the purposes of this guide, we make use of the free service available at www.now-dns.com, though the steps will be common to many providers.

To use the dynamic DNS service on the IndigoVision VPN server, follow these steps:

1. Register with the dynamic DNS provider, on page 33
2. Choose a fully qualified domain name, on page 33
3. Automatically update DNS provider if the IP address changes, on page 34

Register with the dynamic DNS provider

If you are new to the dynamic DNS service, you will need to register a new account.

- Navigate to www.now-dns.com and select ***Register*** from the navigation bar.
- Enter a suitable email address/password and click ***Create account***.

At this point, a confirmation email will be sent to your account. If it is not received promptly, check your spam filter to ensure that it has not been incorrectly marked as spam.

After the email is received, click the enclosed link to activate your account.

Choose a fully qualified domain name

After you have created your account, you can create a dynamic DNS address.

1. While logged into the Now-DNS site, select ***Manage Hostnames*** from the navigation bar.
2. Under ***Hostname Creation***, enter your desired hostname.

   This should be something specific to the site and easy to remember, for example ***my-restaurant*** or ***headoffice*** but should not contain spaces or special characters.
3. Select a domain from the drop-down on the right-hand side and click ***Check availability***.

   The combination of hostname and domain must be unique.

   If the address is available, an IP address field will be presented and automatically filled with your current IP address.
4. Click ***Create now*** to add the domain to your account.

You should now have a dynamic DNS address, for example, ***my-restaurant.dnsdyn.net*** which mirrors your current external IP address. If your external IP address is fixed, you do not need to do anything further. If not, or you are unsure, you will need to set up an update client.

Automatically update DNS provider if the IP address changes

You can download and install the update client using the following procedure. The update client must be installed either on the PC that is running the IndigoVision VPN server, or another PC on the same network.

1. While logged into the Now-DNS site, select ***Automatic Updater Clients*** from the navigation bar.
2. Select the Windows installer ***Download*** link from the center of the page.
3. After the setup file is downloaded, open it and follow the installation instructions.
4. After the installer is complete, the update client opens.
5. Enter the username and password into the client, along with the hostname entered earlier.

Change the VPN password or other server settings

To change the IndigoVision VPN password or other server settings, follow these steps:

1. On the PC running the IndigoVision VPN Server, start the IndigoVision VPN Configuration Tool from the Start Menu, select ***Start Menu > IndigoVision > IndigoVision VPN Configuration Tool***
2. Click ***Next***.

   The Installation Mode page is shown.
3. Select ***Edit the existing IndigoVision VPN server configuration*** and click ***Next***.

Apart from the password (which is not stored for increased security), all of the previously entered settings will be loaded on each of the configuration pages. Settings such as the username or password can be altered in the normal way.

After the password has been changed on the server and the Configuration Tool is closed, each of the existing clients needs to be reconfigured with the new password.

► For more information, *see "Configure IndigoVision VPN on each client" on page 19*

► For more information, *see "Configure IndigoVision VPN on each Integra appliance" on page 27*

Add a new Integra to the VPN on an Integra View

To add a new Integra to the IndigoVision VPN, follow these steps:

1. Carefully consider and change the network configuration on the new Integra appliance to fit within the existing system.

   ► For more information, *see "Choose a network configuration" on page 22*
2. On the Integra View, start the IndigoVision VPN Configuration Tool from the Start Menu, select ***Start Menu > IndigoVision > IndigoVision VPN Configuration Tool***
3. Click ***Next***.

   The Installation Mode page is shown.
4. Select ***Edit the existing IndigoVision VPN server configuration*** and click ***Next***.

Apart from the password (which is not stored for increased security), all of the previously entered settings will be loaded on each of the configuration pages.

5. On the Integra VPN Clients page, click ***Add***.
6. Specify the details of the new Integra and click ***Add***.
7. Complete the rest of the server configuration and close the tool.
8. Configure the new Integra appliance.
   - ► For more information, *see "Configure IndigoVision VPN on each Integra appliance" on page 27*
   - ► For more information, *see "NVR Configuration" on page 28*
   - ► For more information, *see "Site Database Configuration" on page 29*
   - ► For more information, *see "Date and Time settings" on page 21*
9. Add the new Integra to the License Server on the Integra View
   - ► For more information, *see "Add the Integra appliances to the License Federation" on page 29*
10. Now the cameras, NVR and Alarm Server running on the new Integra can be added to the Control Center Site Database.
    - ► For more information, *see "Add the cameras, NVRs and Alarm Servers to the Site Database" on page 30*

Edit an Integra on an Integra View

To edit an Integra on the VPN, follow these steps:

1. On the Integra View, go to ***Start Menu > IndigoVision > IndigoVision VPN Configuration Tool***.
2. Click ***Next***.

   The **Installation Mode** page is shown.
3. Select ***Edit the existing IndigoVision VPN server configuration*** and click ***Next***.

   Apart from the password, which is not stored for security, all of the previously entered settings will be loaded on each of the configuration pages.
4. On the Integra VPN Clients page, double-click the Integra you wish to edit or select the desired Integra and click ***Edit***.

   The **Edit Integra** page is shown.
5. Edit the Integra configuration as required and click ***OK***.
6. Continue to the end of the configuration tool to apply the changes.

Remove an Integra from the VPN on an Integra View

To remove an Integra from the VPN, follow these steps:

1. On the Integra View, start the IndigoVision VPN Configuration Tool from the Start Menu, select ***Start Menu > IndigoVision > IndigoVision VPN Configuration Tool***
2. Click ***Next***.

   The **Installation Mode** page is shown.
3. Select ***Edit the existing IndigoVision VPN server configuration*** and click ***Next***.

   Apart from the password (which is not stored for security), all of the previously entered settings will be loaded on each of the configuration pages.
4. On the **Integra VPN Clients** page, select the Integra that you wish to remove.
5. Once the Integra is selected, click ***Remove***.

6. Continue to the end of the configuration tool to apply the changes.

Connect additional client PCs to an existing IndigoVision VPN

Whether, the IndigoVision VPN is hosted on an Integra View or Integra appliance, it is possible to add additional non-Integra clients to the VPN without changing the configuration of the VPN server.

To add additional client PCs to the VPN if the client PC is not an Integra appliance, you need to allow remote access to a single IndigoVision Integra appliance

► For more information, *see "Configure IndigoVision VPN on each client" on page 19*

7 TROUBLESHOOTING

The IndigoVision VPN client cannot connect to the VPN server

If you are configuring a **permanent VPN client** and the IndigoVision VPN Configuration Tool presents a warning message:

```
Failed to connect to the configured VPN server.
```

```
Click OK to go back to the previous page and review the settings.
```

Check the client log file in the OpenVPN installation folder in ***C:\Program Files\OpenVPN\log\IndigoVision VPN Client.log***

If you are configuring an on-demand VPN client using the OpenVPN GUI tool, check the log file in ***%USERPROFILE%\OpenVPN\log\IndigoVision VPN Client.log***

1. If the log file contains the following line, for example:

   ```
    TLS Error: TLS key negotiation failed to occur within 60
   seconds (check your network connectivity)
   ```

   Then the client could not establish a network connection with the server.

   - Check that you have a working Internet connection on the client PC.
   - Check that there is no firewall on the client PC or its LAN that prevents outgoing connections to the configured server port.

Notice *Some organizations prevent outgoing connections to any port other than 80 or 443. In such cases, the public-facing port of the VPN server may need to be changed to one of these ports.*

   - Check that port is correctly forwarded from the router and firewall on the server's Internet connection
   - Check that the OpenVPNService is running on the IndigoVision VPN server.

2. If the log file contains the following line, for example:

   ```
   AUTH: Received control message: AUTH_FAILED
   ```

   Then the username and password combination are rejected by the server.

   - Check that you are using the correct credentials for this server.

Cannot discover cameras in Control Center on the remote Integra

Device discovery in Control Center will not work for devices that are connected through the VPN. In such cases devices can either be added manually using Control Center on the remote PC, or Control Center can be run on the Integra where the camera is connected where device discovery will operate normally.

► For more information on adding devices in an Integra View system, *see "Add the cameras, NVRs and Alarm Servers to the Site Database" on page 30*

Overlapping network warning when configuring the IndigoVision VPN server

When configuring an Integra View Workstation as a VPN server with multiple Integra appliances, the IndigoVision VPN Configuration Tool may present validation warnings with the messages:

```
IP address range conflict with another Integra
```

This indicates that you are trying to add an Integra with a switch that operates with an IP address range that overlaps, or is contained within, another Integra appliance already configured on the server. The tool will prevent both of these devices being configured as the VPN would not be able to route traffic to both Integras.

Additionally if you try to add an Integra using a switch network that overlaps or is contained within the VPN network the following message is shown:

```
IP address range conflict with VPN network
```

It is not possible to use Integra appliances that conflict with the VPN network address space. By default, this is 10.237.178.0/255.255.255.0

To resolve either of these issues, the switch network on one or more of the Integra appliances must be changed. You will need to choose a better network configuration

► For more information, *see "Choose a network configuration" on page 22*

Video quality issues when streaming over IndigoVision VPN

If the VPN is connected, but there are issues with the quality of the video streams from remote devices connected through the VPN, check the following:

- Check the internet connection between the Control Center workstation and the remote site. The quality of service provided on the public Internet can vary over time.
- Check that the number of video streams being viewed in Control Center is within the recommended levels for your hardware.

Try reducing the number of concurrent streams being viewed or recorded using the VPN connection to check if this is the problem.

Notice *When using the IndigoVision VPN to stream video, the workstation hardware may not be able to display the same amount of video as it can when the streams are all on the local network.*

Cannot add or update user for the Control Center Site Database network share

Occasionally, when Windows users are removed from a PC or from a domain controller used by the PC, orphaned Windows accounts can be left behind. These can cause the configuration tool to fail.

To remove these from Windows, contact your Network Administrator or perform the actions below:

1. From the Start menu, select ***Run***. Enter `lusrmgr.msc` and click ***OK***.
2. In the left hand pane, select ***Users***.
3. In the central pane, check for any unexpected users. These are usually identifiable by a question mark in the user icon or a name beginning with characters, for example, `S-1-5-21`.
4. Right-click the desired user and select ***Delete***.

⚠ **Warning** *Make sure that the user accounts in question are not in active use because after they are deleted, users cannot be recovered.*

A INDIGOVISION VPN FIREWALL CONFIGURATION

The IndigoVision VPN software uses the following ports when acting as a server or client.

Ports required for IndigoVision VPN

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