IndigoVision

CyberVigilant

User Guide

IndigoVision

THIS MANUAL WAS CREATED ON WEDNESDAY, JANUARY 9, 2019.

DOCUMENT ID: IU-NVR-MAN027-7

Legal Considerations

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

Copyright

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 CyberVigilant devices. It provides installation and configuration information for the device, as well as a description of the hardware and specifications.

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

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

Part of the IndigoVision management hardware offering, CyberVigilant helps maintain the security of your Control Center environment by detecting threats as they occur. Alarms are raised within the Control Center system enabling operators to respond immediately to a cyber-attack.

CyberVigilant automatically monitors cameras and NVRs in the Control Center Site Database. Using the CyberVigilant configuration, you need to manually authorize other entities in the Control Center environment that are expected to communicate with these devices, including Control Center workstations and NTP servers.

To detect malicious configuration changes on cameras or NVRs, CyberVigilant has two operating modes, differentiating between normal system operation and system configuration.

System Architecture

CyberVigilant is designed to monitor an attached network segment and detect incoming attacks.

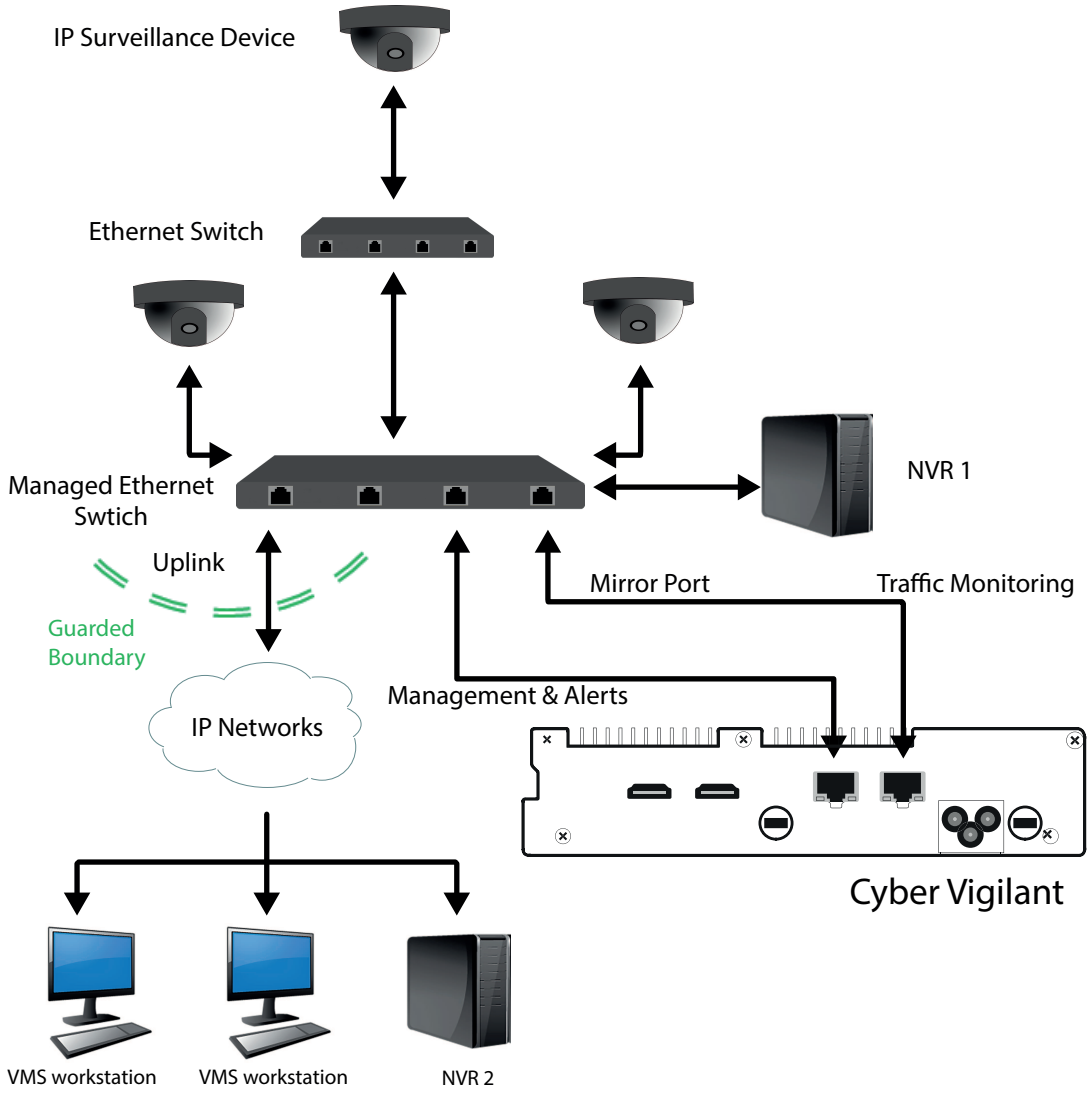

Figure 1: CyberVigilant System Architecture

In this scenario the CyberVigilant device is monitoring the traffic on the uplink port of the switch it is attached to.

Capabilities

CyberVigilant connects to your edge network switch to monitor connected cameras, encoders, NVRs and the CyberVigilant device itself. CyberVigilant can alert Control Center operators and trigger automated actions in response to various situations such as the following:

- Accessing the web pages of cameras/NVRs/CyberVigilant.
- Camera access from outside the expected list of NVRs and Control Center workstations.
- Unknown external entities communicating with cameras/NVRs/CyberVigilant.
- Detecting TCP/UDP network reconnaissance.
- Attempting to access network services that are not supported by the device.
- Shell access when device reconfiguration is not expected or is done using an insecure protocol.

- Unexpected DNS, NTP or SMTP servers being used by monitored surveillance devices.
- Potential denial-of-service attacks.

CyberVigilant is not designed to provide protection against the following:

- Cameras being hooded or disconnected – an Alarm Server is capable of that monitoring and alerting.
- Workstation protection against viruses, malware etc.
- Devices that are already compromised sending one-way data out to unknown external entities.
- Attacks against devices where the network communications do not traverse the switch uplink that CyberVigilant is monitoring. For example:
  - A local NVR recording cameras within the same network segment.
  - Devices that are in the Control Center site but are outwith the network segment that CyberVigilant is attached to.
- Attacks against the CyberVigilant device itself, when the Management Interface is not attached to the switch you are monitoring.

The following setups are not supported:

- Control Center workstations in the edge network.
- NVRs or Alarm Servers in the edge network accessing cameras or NVRs outside its own edge network. That situation would cause false alarms and is not supported.

CyberVigilant is an extension of good security policy and should be used in addition to the guidelines in the IndigoVision Control Center Security Hardening Guide.

3 HARDWARE DESCRIPTION

This chapter details the CyberVigilant device's connections, weight and dimensions.

Metrics

Dimensions

- 190.5 mm (W) x 107 mm (D) x 48.3 mm (H)

Weight

- 1.4 kg

Connections

There are connections on the front, side and rear of the device.

Notice *Not all ports are supported, and not all should have devices connected to them.*

► For more information, See "Package contents" on page 13

Video

- HDMI port 1
- HDMI port 2

Notice *A monitor should only be connected for initial configuration.*

USB

- 4 x USB 3.0 (front)
- 1 x USB 2.0 (front)
- 2 x Micro USB OTG (side) (currently not supported)

Notice *Only USB keyboards are supported for initial network configuration. No other USB devices should be connected to the CyberVigilant device.*

LAN

- 2 x RJ-45 10/100/1000 Mbps adaptive Ethernet interface

Power requirements

The CyberVigilant device is powered using a mains powered internal 50W PSU. The maximum power consumed by the product is 15W.

4 GETTING STARTED

This chapter describes the initial steps required to start using the CyberVigilant device.

Package contents

Before continuing, please check that you have been shipped the items listed for your device.

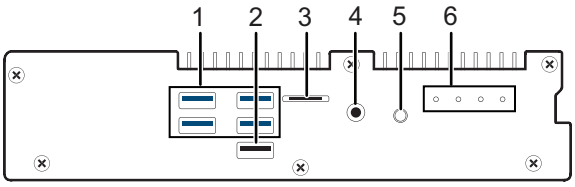

Figure 2: Front connections

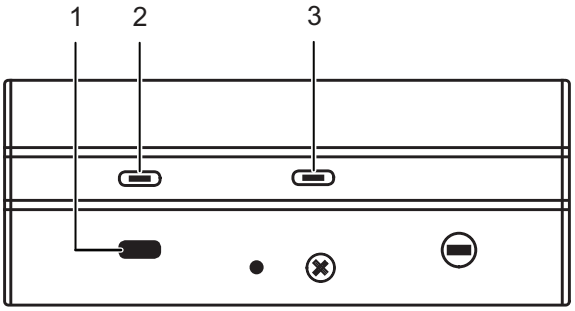

Figure 3: Side connections

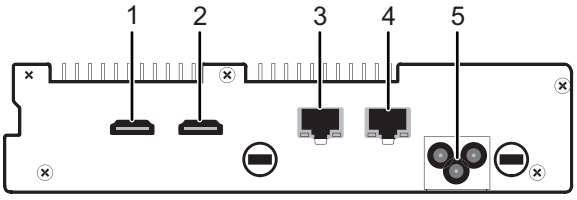

Figure 4: Rear connections

Front connections

1. 4 x USB 3.0 ports
2. USB 2.0 port
3. Micro SD (currently not supported)
4. LINE OUT (currently not supported)
5. Power on/off button
6. Status LED indicators

Side connections

1. Kensington lock
2. Micro USB OTG (currently not supported)
3. Micro USB OTG (currently not supported)

Rear connections

1. HDMI port 1
2. HDMI port 2
3. Network connection 10/100/1000Mbps port (LAN1) - Management Interface
4. Network connection 10/100/1000Mbps port (LAN2) - Monitored Network Interface
5. Mains power inlet (100V to 240V AC)

Additional items

- Regional IEC mains lead

Power

The CyberVigilant device can be powered on and off manually.

Power on

The CyberVigilant device can be powered on by pressing the manual power on/off button.

When power is applied to the CyberVigilant device it will automatically power up. No button press is required.

Power off

The CyberVigilant device can be powered off by briefly pressing the manual power on/off button.

Notice *Continuously holding the button causes the CyberVigilant device to shut down instantly, and can cause data loss.*

After the power button LED has turned off, the mains power can be disconnected.

Notice *Removing the mains power while the power button LED is blue can result in data loss.*

Initial configuration

Initial configuration can be done using one of the following methods:

- Web configuration using the default IP address
- Monitor and keyboard connected directly to the device

After initial configuration is complete, further device configuration and setup is completed using the Web Configuration pages.

When using the Web Configuration pages for the first time you will be prompted to set a password for the device. The password must contain between 8 and 32 printable ASCII (7-bit US-ASCII) characters. Enter the password again to confirm it.

A warning message may be produced if the password is thought to be weak or insecure. After you have logged in with this password you will be able to set a different or stronger password at any point.

Notice *The web access password must be configured before the NVR is capable of performing any authenticated network services, including recording.*

► For more information, *see "Configuration" on page 25*

Web configuration

The CyberVigilant device comes configured with the following settings:

Table 1: Default network settings

Default IP Address	10.5.1.10
Default Subnet Mask	255.0.0.0

When the CyberVigilant device is connected to a suitable network, you can use these details to configure the device using the Web Configuration pages.

When using the Web Configuration pages for the first time, you will be prompted to set a password for the device before you can log in.

Using a monitor and keyboard

The CyberVigilant device can be configured by connecting a monitor to the HDMI port and a keyboard to one of the USB ports.

1. Connect the keyboard and monitor to the device and press ***Enter***.
   You should see the following prompt:
   ```
   IndigoVision CyberVigilant[CyberVigilant]
   login:
   ```
2. Log in to the device using the username `config` and password `config`.
   The device prompts you to enter the new configuration values.
3. At each prompt, press ***Enter*** to accept the current value.
   - **DHCP** - Enter `Y` or `N` to chose between a DHCP or static IP configuration.
   - **IP Address** — Enter the IP address for the unit's network connection.
   - **Subnet Mask** — Enter the IP network subnet mask for the unit's network connection.
   - **Gateway** — Appropriate default gateway for remote network access: this is only required if the unit is to communicate with devices on a different subnet.
   - **Preferred/Alternate Name Server Address** — Enter the IP address of the DNS server used to convert network names into numerical IP addresses. You only need

to enter a name servers if you wish to specify NTP or other server addresses as names and not as IP addresses.

- **CyberVigilant name** — Enter a name to describe the unit.
- **Location** — Enter a name to describe the location of the unit.
- **Reset network security**

  Enter `Y` to reset all passwords used to access the device, disable IP Access Restrictions, and reset the device to HTTP use only by deleting any HTTPS certificate or certificate request.

You are now ready to attach the device to the network.

The HDMI port goes into sleep mode after a period of inactivity. To bring back out of sleep mode, press any key.

---

5 INSTALLATION

This section details how to install the CyberVigilant device.

Pre-requisites

- Gigabit Managed Ethernet Switch
- Ability to mirror only the ingress traffic on the uplink
- Uplink ingress bandwidth must be less than 45Mbps

Licensing

In order for CyberVigilant to send events to your Alarm Server, your Control Center license must include the CyberVigilant feature.

Use with VLANs

You can use CyberVigilant with networks that are partitioned into VLANs.

CyberVigilant supports untagged and IEEE 802.1Q tagged VLAN traffic. CyberVigilant identifies tagged VLANs by using a VLAN identifier, or VLAN ID.

An example of CyberVigilant working with a VLAN is shown in Figure 5. The two VLANs shown in Figure 5 have VLAN IDs of 101 and 102. The VMS workstations and IP surveillance devices are on VLAN 101.

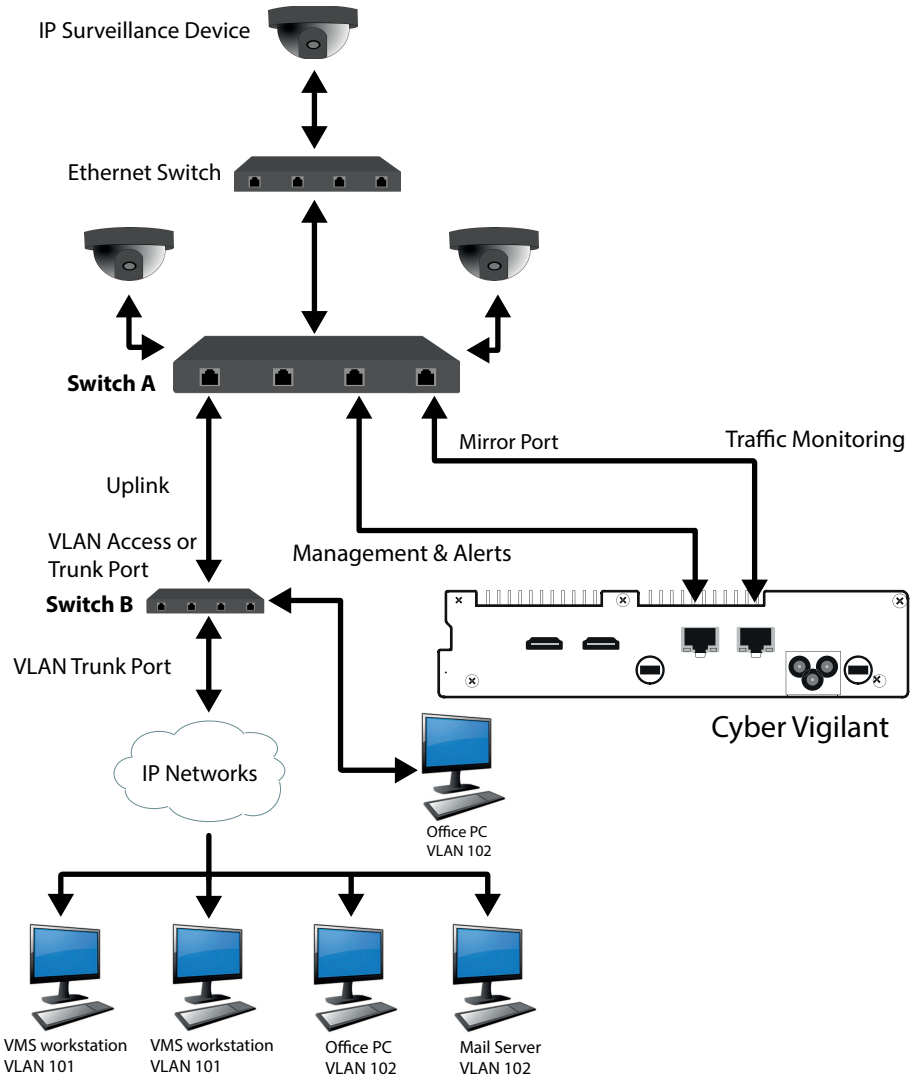

Figure 5: CyberVigilant VLAN architecture

► For more information, *see "VLAN Tagging" on page 20*

Attach the device to the network

Connect the CyberVigilant device to the Ethernet network using two standard Ethernet cables.

- **LAN port 1**: Management Interface

  This port is located on the back of the device and is used for device configuration and communicating alerts to Control Center. You can choose which Ethernet switch this port is attached to:

  - If you want to generate alerts as a result of unauthorized access to the CyberVigilant device itself, then you must connect LAN port 1 to the Ethernet switch you are monitoring. See Figure 1.
  - You can attach LAN port 1 to a completely separate network from the network you are monitoring. See Figure 6.
- **LAN port 2**: Monitored Network Interface

This connection monitors any cameras and NVRs attached to the Ethernet switch, using the Ethernet switch mirroring capability. Connect this port to the mirror port on an Ethernet switch.

After you have connected the LAN ports, you can configure the CyberVigilant device and the connected edge switch.

► For more information, *see "Port mirroring" on page 19*

► For more information, *see "Configuring CyberVigilant for operation" on page 21*

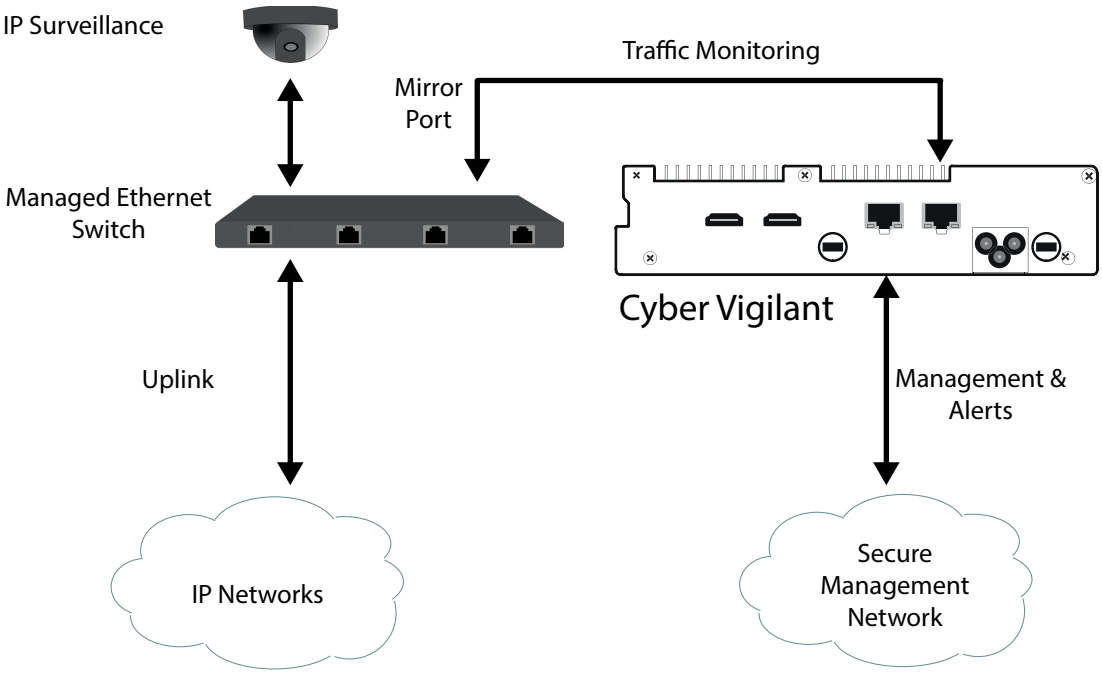

Figure 6: Using separate management network

Switch Configuration

Port mirroring

Using the standard CyberVigilant system architecture, the network switch should be configured so that the uplink port is mirrored to the port that CyberVigilant is attached to.

► For more information, *see "System Architecture" on page 7*

On Cisco switches such as the SG300-10P, carry out the following procedure:

1. Navigate to ***Administration > Diagnostics > Port and VLAN Mirroring***
2. Click ***Add*** to add a port or VLAN to be mirrored.
   Enter the parameters:
   - Destination Port
     Select the port that CyberVigilant is attached to
   - Source Interface
     Select the uplink port from where traffic is to be mirrored.
   - Type
     Select whether incoming, outgoing, or both types of traffic are mirrored to the analyzer port.
     For CyberVigilant select `Rx Only`.

On switches from other manufacturers this option may be referred to as `Ingress` rather than `Rx Only`.

3. Click ***Apply***.
   Port mirroring is now set up.

VLAN Tagging

When using VLANs, you can configure Switch B in Figure 5 to do one of the following:

- Pass traffic for VLAN 101 using a VLAN Access Port:
  This means that CyberVigilant will not process any VLAN 102 traffic.
- Pass IEEE 802.1Q VLAN tagged traffic using a VLAN Trunk Port:
  If you use this configuration, and if the switch preserves the tag when mirroring, then you can configure CyberVigilant to only process data from specified tagged VLANs, instead of all mirrored traffic.
  For example, CyberVigilant can be configured to only process VLAN 101 surveillance data.

For the best performance, IndigoVision recommends that you reduce the amount of data which CyberVigilant processes.

► For more information, *see "Use with VLANs" on page 17*

Other switch vendors may present the configuration options with the terminology Tagged/Untagged.

- **Trunk**: The interface is an untagged member of one VLAN at most, and is a tagged member of zero or more VLANs.
- **Access**: The interface is an untagged member of a single VLAN.

6 OPERATIONS

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

Configuring CyberVigilant for operation

The following configuration steps must be carried out before CyberVigilant is operational:

1. CyberVigilant requires network access to the Control Center Site Database. This may be hosted as part of a domain or as part of a workgroup.

   Using the web configuration for CyberVigilant, specify the Control Center Site Database network path and credentials to access it.
2. Using the web configuration for CyberVigilant, specify the Alarm Server that events should be sent to.
3. In Control Center, create an External System with the IP address of the CyberVigilant device, then create an External Detector on the Alarm Server (that CyberVigilant is configured to use) to allow attack notifications.

   ► For more information, *see "CyberVigilant attack notification" on page 21*
4. In Control Center, create an External Detector on the Alarm Server to allow fault notifications.

   ► For more information, *see "CyberVigilant fault notification" on page 22*
5. To test operation, access the webpage of a device that is being monitored by the CyberVigilant device and is part of the Control Center site using a workstation that is not on the authorized client list. This should cause a Detector Activation and Zone Alarm to be visible in Control Center.

CyberVigilant attack notification

When CyberVigilant detects a possible attack, it sends an event to the configured Alarm Server. You can use this in conjunction with a detector in order to alert operators to the attack:

1. Create a new external detector for the external system in a new or appropriate existing zone.
2. Specify the Activation Input Number as `1000`.
3. Ensure the Dwell Time is `0` seconds and that no Deactivation Event is set to ensure all attacks are logged.

To be informed when CyberVigilant is tracking one or more ongoing and persistent issues:

1. Create another new external detector for the external system in a new or appropriate existing zone.
2. Specify the Activation Input Number as `2000`.

3. Configure this detector with a Deactivation Event of type External and a Deactivation Input Number of `2001` to ensure the state is deactivated when CyberVigilant is no longer tracking any persistent issues.

CyberVigilant fault notification

When CyberVigilant has a fault that may prevent it from operating normally and generating notifications of possible attacks, it will send an event to the configured Alarm Server. This can be used in conjunction with a detector to be able to alert operators to the problem.

Create a new external detector for the external system in a new or appropriate existing zone. Specify the Activation Input Number as `3000`.

To set the state of the detector to reflect whether CyberVigilant has a fault or not, configure the detector with a Deactivation Event of type External, and a Deactivation Input Number as `3001`.

The detector triggers when any of the following faults occur:

- Failure to access the Site Database
- No monitored network interface link
- No monitored network interface traffic
- No valid CyberVigilant license is available

Adding a new device to the system

When a new device (camera, NVR etc) is commissioned and added to the Control Center Site, CyberVigilant will automatically start monitoring communications to that device, subject to those communications traversing the uplink of the network switch that CyberVigilant is receiving traffic from.

► For more information, *see "System Architecture" on page 7*

It takes up to a minute before monitoring begins. Monitoring is stopped within a minute of the device being removed from the Control Center Site.

All NVR and Alarm Server devices in the Control Center Site are automatically recognized by CyberVigilant and will not generate any alerts when interacting with other NVRs and cameras.

Note that if device configuration is carried out after it has been added to the Control Center Site this may cause an alert to be generated by CyberVigilant. Change the Operating Mode to avoid this false alarm.

► For more information, *see "Performing device configuration" on page 22*

Performing device configuration

When you need to reconfigure a surveillance device (camera, NVR-AS, or other device) that is monitored by CyberVigilant, set the CyberVigilant Operating Mode to allow configuration from authorized devices. This prevents triggering alarms when device configuration takes place.

► For more information, *see "Home" on page 25*

The Operation Modes that CyberVigilant supports are the following:

- **Full Protection**: The surveillance system is operational and camera/NVR-AS reconfiguration is not allowed.

- **Allow configuration from authorized devices**: The surveillance system is operational but configuration of cameras/NVRs by explicitly authorized devices is allowed. Configuration by any other device will trigger an alarm.

Notice *After you have configured the camera/NVR-AS, set the CyberVigilant Operating Mode back to **Full Protection**.*

7 CONFIGURATION

This section explains the various configuration options provided by the Web Configuration pages.

Web Configuration pages

To access the Web Configuration pages of the CyberVigilant device, enter the IP address of your device into a web browser.

If a web access password has not been previously defined for the device you will be prompted to set a password.

The password must contain between 8 and 32 printable ASCII (7-bit US-ASCII) characters. Enter the password again to confirm it.

The login page is then displayed. Use the web access password to log in, and the Home page is displayed.

Notice *The web access password must be configured before the NVR is capable of performing any authenticated network services, including recording.*

Notice *IndigoVision devices support Microsoft Internet Explorer (version 8 or higher).*

To access any of the other configuration pages, click the required option in the menu on the left of each page.

To save the changes made on any page, click ***Submit*** before navigating away from that page.

Home

This section is read-only and provides a basic configuration overview of the CyberVigilant device and its operational status.

CyberVigilant requires a compatible Control Center License Server, with a licensed CyberVigilant feature.

CyberVigilant automatically extracts the IP address of the License Server from the configured Control Center Site Database.

Warning

A loopback IP address, such as 127.0.0.1, should not be used when configuring the License Server IP address in Control Center. The License Server IP address defined in the Control Center Site Database must allow access from the CyberVigilant device.

If CyberVigilant loses contact with the License Server, then CyberVigilant continues to work for a limited period of time. CyberVigilant displays the expiry date of this period in the ***Status*** field.

- ***Status*** – If `OK` then CyberVigilant is appropriately configured and licensed. CyberVigilant should provide the expected cyber-attack notifications. If there are one or more of the following faults, they are reported here and you must address them:
  - `Failure to access the Site Database`
  - `No monitored network interface link`
  - `No monitored network interface traffic`
  - `Alarm Server or Remote Logging not configured`
  - `No valid Control Center license available`
  - `CyberVigilant will function normally until...`
- ***Mode*** - Set the required Operating Mode:
  - `Full Protection` - the surveillance system is operational and you should not currently reconfigure the monitored devices.
  - `Allow surveillance device configuration from authorized devices` - the surveillance system is operational but explicitly authorized devices can configure cameras/NVRs. Configuration by any other device triggers an alarm.

Network

Use this page to configure the network settings.

- **CyberVigilant Name** — Enter a name to identify the CyberVigilant device.
- **CyberVigilant Location** — Enter a location to identify the device.
- **Use DHCP** — Check this to enable DHCP for the CyberVigilant device. When this is enabled, the IP address, subnet mask, gateway, and name servers are obtained from the DHCP server on the network. The options for these items are grayed out.

Notice

After switching to DHCP, you need to specify the new IP address of the network device in the web browser. Query the DHCP server to find the assigned IP address, then use this IP address in the web browser to navigate to the device.

The CyberVigilant device chooses the first two DNS servers that the DHCP server specifies.

If at least one NTP server is specified by the DHCP server then the CyberVigilant device will attempt to synchronize with these NTP servers. The Date and Time page will not list these servers and additional NTP servers can still be manually added.

Notice *If the CyberVigilant device fails to receive any configuration settings from a DHCP server on the network, it will not be accessible on the network and you will have to use a keyboard and monitor to set a static IP address.*

► For more information, *see "Initial configuration" on page 14*.

- **IP Address**— Enter the unit's IP address.
- **Subnet Mask** — Enter the unit's IP network subnet mask.
- **Gateway** — Appropriate default gateway for remote network access: this is only required if the unit is to communicate with devices on a different subnet.
- **Broadcast Address** — This value is read-only.
- **Preferred/Alternate Name Server Address** — The IP address of the DNS server used to convert network names into numerical IP addresses. You only need to enter a name server(s) if you need to specify the NTP Server Addresses as a name and not as an IP address or to use a name in the Site Database UNC path.

  The above options are not available for editing if DHCP is enabled.

Date & Time

Use this page to configure the Date and Time settings for the CyberVigilant device.

- **NTP Servers** - This is a list of up to five NTP Servers that the CyberVigilant device will synchronize with.

  Servers can be specified as IP addresses or resolvable hostnames, if at least one name server has been specified.

  Add new servers by entering the server address in the text field and click ***Add***.

  Remove servers by highlighting them in the list and click ***Remove***.

  Changes are applied when you click ***Submit***.
- **Timezone** - Select the timezone for the CyberVigilant device from the list.
- **Master Time Server** – Check this option if the CyberVigilant device is expected to serve as a master time source on a local area network when the configured NTP servers are not available.
- **Hardware Clock** – The date and time for the CyberVigilant device can be directly edited using this form. This should not be required when there is an upstream NTP server.

Network Security

This page allows you to specify a device password to restrict access to the Web Configuration pages. This device password can also be used to access the device using SSH or SFTP, when logging in as ***root***.

- **Configure User**
  - **Change Password** — Enter a password for the unit. This must contain between 8 and 32 printable ASCII (7-bit US-ASCII) characters. Enter the password again to confirm it.

Passwords are automatically verified for security strength, and a warning will be provided if the submitted password is not believed to be secure or could be improved.

Notice *If you forget the password, you will need to connect a keyboard and monitor in order to reset the device's security settings*

► For more information, *see "Using a monitor and keyboard" on page 15*

IP Access Restrictions

- **Enable** — Check this box to restrict CyberVigilant access to the allowed addresses.

Notice *Before enabling the IP Access Restrictions, please make sure that a management PC is included in the Addresses Allowed list. Failure to do so may result in a loss of connectivity, and require physical access to the unit to disable the restrictions.*

► For more information, *see "Reset network security" on page 16.*

- **Addresses Allowed** — Enter the IP addresses of workstations that will be used to administer CyberVigilant.

  To remove an address, select the address and click ***Remove***. Shift-click or Control-click to select more than one address.
- **Add Address** — Enter an IP address and click ***Add***.

  You can also enter an address range, for example `10.5.1.12-20`, or a CIDR address including a netmask, for example `192.168.123.0/24`.

Remote Secure Shell Access

Use these settings to control remote access to the unit using a secure shell (SSH). It is possible to create a separate account with a different password to the unit for diagnostic purposes. This support account has more restricted and secure access to the unit.

Enable - Use this to enable or disable remote access to the unit.

Support User - Use this to enable or disable a remote access account with the user name "support". If enabled, remote access users will be able to login using this user name.

Support Password - Enter a password for the "support" user account. This must contain between 8 and 32 printable ASCII (7-bit US-ASCII) characters. Enter the password again to confirm it.

Passwords are automatically verified for security strength, and a warning will be provided if the submitted password is not believed to be secure or could be improved.

Root Access - Use this option to enable or disable full administrative direct remote access to the unit with the user name "root".

For best security it is recommended to ensure that remote access is disabled after unit configuration. If remote access is required for diagnostic purposes it is recommended to enable a support user account with a different password to the device password and disable root access.

HTTPS Configuration

Use these settings to configure the HTTPS settings. However, you can only install Signed Certificates when HTTPS is disabled. Disable HTTPS before changing these settings.

Mode — Select to enable device configuration using HTTP and HTTPS. You must select at least one option.

The device must have a valid HTTPS certificate to enable HTTPS. Use the options in this section to create and apply a certificate.

Private Key (Regenerate) - Use this option to regenerate your private key. Using this option invalidates and deletes any certificate or certificate request that is stored on the device.

Self Signed Certificate — Use this option to create and install a self-signed certificate.

Click ***Create*** to create and install a self-signed certificate. A new page opens, enter your details and click ***OK*** to generate and install the certificate.

This option is unavailable if a certificate is already installed.

Certificate Authority — Use this option to create a certificate request to submit to a Certification Authority for signing. Certificate Authority Certificates created this way are specific to this device.

Click ***Create*** to create a certificate request. A new page opens, enter your details and click ***OK*** to generate the certificate request. Copy the certificate request displayed in the browser and submit it to a Certification Authority for signing.

After the certificate request has been signed and returned, ***Browse*** to the location of the saved certificate, then ***Upload*** it to the device.

You can ***View*** and ***Delete*** a certificate request if one is available.

Installed Certificate — ***View*** and ***Delete*** the installed certificate.

Site Database

Use the following parameters to configure the Control Center Site Database that will determine which devices are monitored. You can specify the host as a fully qualified domain name or IP address. Using a NetBIOS name is not sufficient.

- **Site Database UNC Path**: Path to the Control Center Site Database network share.
- **User Name**: Network share user name to use when accessing the database.

The "Name" for the user as seen in Windows must be used rather than the "Full Name".

- **User Password**: Network share password to use when accessing the database. Enter the password again to confirm it.

Notice *It is highly recommended to create a Windows account that is solely for the purpose of accessing the Site Database network share. This account should have restricted access to any other network service and the username/password used should be unique.*

Alarms

- **Alarm Server**: Check this box to enable logging of alarms to an Alarm Server.

To specify a valid Alarm Server, enter the IP address of the server where Detectors will be configured to pick up the alerts from this CyberVigilant device.

- **Alarm Collapsing**: Check this box to enable Alarm Collapsing of alerts to the Alarm Server.

  Alarm Collapsing combines multiple related alerts into a single alarm to avoid unnecessary repetition of identical alarms and significantly reduce and control the number of alarms that CyberVigilant can transmit to the Alarm Server.

Notice *Disabling Alarm Collapsing is useful for configuration and problem diagnosis but it is recommended to be enabled for standard use.*

Authorized Devices

This page allows you to specify trusted devices that interact with surveillance devices, but are not included in the Control Center site, for example:

- Workstations allowed to stream video from surveillance devices
- Servers such as NTP, DNS, DHCP, SMTP
- Control Center Web application and media servers

To specify trusted devices, do the following:

- **Authorized Addresses** — lists the IP addresses of the devices that are authorized to interact with surveillance devices.

  To remove an address, select the address and click ***Remove***. Shift-click or Control-click to select more than one address.
- **Add Address** — enter an IP address and click ***Add***.

  You can also enter a CIDR address including a netmask, for example `192.168.128.0/24`.

Notice *When not in Full Protection Operation Mode, all Authorized Devices can be used to configure Surveillance Devices without raising configuration attempt alarms.*

Honey Pots

CyberVigilant allows the use of unused, or decommissioned, ONVIF cameras to act as decoy devices, or Honey Pot devices. These devices are cameras that are not, or are no longer, part of the active surveillance site, but remain connected to the network being protected by CyberVigilant. These devices should not be listed in the Site Database. There is no requirement for honey pot devices to be in a usable physical location, just within the CyberVigilant protected network.

Any direct access to a honey pot device, with the exception of ONVIF discovery, will result in an alarm in Control Center and, if configured, the remote log. By suitably renaming the camera the intention is to attract attackers away from active, working cameras and towards the heavily monitored, inactive and unused decoys.

Some thought should be applied to the name of the ONVIF camera. It should be consistent with the naming strategy of cameras in the active site. The camera name should be potentially interesting to an attacker, for example `Jackpot Table`, or hint at a potential security weakness e.g. `Unconfigured Camera - Do not use`.

To configure an ONVIF camera to act as a honey pot device, it must be possible to disable all services that will cause the camera to generate packets, such as NTP, DNS, DHCP, UPnP. The camera must be configured with a static IP address. The camera should remain discoverable through ONVIF but should still be secured as much as possible such as by disabling Telnet/SSH, using HTTPS, secure password and IP firewall. Untrusted ONVIF devices should not be used.

This page allows you to specify devices that will act as the decoy honey pot devices. To specify honey pot devices, do the following:

- **Honey Pot Addresses** - lists the IP addresses of configured honey pot cameras
  To remove an address, select the address and click ***Remove***. Use Shift-click or Control-click to select more than one address.
- **Add Address**
  To add an address, enter an IP address and click ***Add***.

Advanced Settings

This page allows you specify IEEE 802.1Q tagged VLAN IDs to filter incoming monitored traffic. Only packets tagged with a VLAN ID listed on this page can generate an alarm. If no VLAN IDs are specified in the list, then VLAN filtering is disabled.

To specify VLAN IDs, do the following:

- **VLAN IDs** — lists the VLAN IDs that will be monitored.
  To remove an address, select the VLAN ID and click ***Remove***. Shift-click or Control-click to select more than one VLAN ID.
- **Add VLAN ID** — enter a valid VLAN ID in the range 1 to 4094 inclusive and click ***Add***.

Notice *This advanced feature requires VLAN tags to be preserved on the network switch mirroring port. Please consult your switch configuration guide or switch manufacturer.*

Caution *If tagged VLAN filtering is enabled, your CyberVigilant device must be in one of the tagged VLANs in order for it to be protected.*

Firmware Upgrade

Browse to the vex file you require to upgrade your unit, then click ***Perform Upgrade***. Uploading the vex file may take a few minutes. After the file has been uploaded, follow the on-screen instructions to start the upgrade process. The upgrade itself will take several minutes. It is important not to power off the unit or disconnect it from the network during this process.

Diagnostics

These pages provide support information which may be requested by your IndigoVision supplier.

- **Remote Logging** - Check this box to enable remote logging.
  To specify a valid syslog server to send log messages, do one of the following:

- Enter the IP address of the server.
- If a name server has been configured, enter a resolvable hostname.

CyberVigilant transmits status information, including alarms, to the server through UDP port 514.

To detect alarms in the remote log, use the keyword string `CVALARM`.

To use the Remote Logging feature, you must specify a valid Alarm Server IP address on the Alarms web page.

- **Support Information** - This button downloads a zip archive containing diagnostic information. Provide this file to Technical Support when reporting any issues with the unit.
- **Maintenance:**
  - **Reset** - Click to reset all CyberVigilant settings configured from the web pages and the device password, and reboot the unit.

    The CyberVigilant device retains its IP address, subnet mask, gateway and DNS servers, and HTTPS configuration.
  - **Reboot** - Click to reboot the device.
  - **Power Off** - Click to power off the device.

Caution

If the device is powered off using this option, the device will only power on again when the physical power button on the front panel is pressed.

8 HARDWARE SPECIFICATION

This chapter details the hardware specifications for the CyberVigilant device.

Network

- Dual 100/1000 BaseT RJ-45
- Protocols — UDP, ICMP, IGMP, HTTP, HTTPS, NTP, SSH, SFTP

Environment

Operating temperature:

- 0°C to 35°C (32°F to 95°F)

Performance

The CyberVigilant has the following Switch Uplink Throughput:

- 16 Channel variant:
  - Egress: 10Gbps
  - Ingress: 30Mbps
- 24 Channel variant:
  - Egress: 40Gbps
  - Ingress: 45Mbps

Regulatory

- EN55024 (2010) ITE immunity standard
- EN 55032 (2012) ITE emission standard – Class A
- IEC60950-1
- 47CFR (2011) Part 15 subpart B - Class A (US federal code of regulations)
- This product complies with the European Low Voltage Directive 2006/95/EC and EMC Directive 2004/108/EC
- EN 60068-2-29:1993 (15G)
- EN 60068-2-64:1995 (Random)
- EN 60068-2-96:1996 (Sine)
- EN 60068-2-30
- EN 60068-2-1 at 0°C
- EN 60068-2-2 at +35°C

- This product meets the requirements of the EC restriction of hazardous substances (RoHS) directive 2002/95/EC

In accordance with the EC Waste Electrical and Electronic Equipment (WEEE) directive 2002/96/EC this product must be sent to a recycling plant for proper disposal at the end of its use.

A GENERAL PUBLIC LICENSE

IndigoVision's CyberVigilant products use code that is freely available under the General Public License (GPL).

This license makes it a requirement to release changes made to the source code. In compliance, the GPL source code and any changes made by IndigoVision are available on request through IndigoVision Customer Support.

B EXTERNAL DETECTOR INPUT NUMBERS

When configuring an External Detector on an Alarm Server the following values may be used.

Table 2: External Detector Input Numbers

Input Number	Usage
1000	CyberVigilant has detected a possible attack on the system.
2000	CyberVigilant is now tracking one or more ongoing and persistent possible attacks on the system.
2001	CyberVigilant is not tracking any ongoing and persistent possible attacks on the system.
3000	CyberVigilant has a fault that may be preventing it from generating possible cyber-attack notifications.
3001	CyberVigilant is fully configured and monitoring the network.

C ATTACK DETECTION RULES

Description (as it appears in Control Center)	Mode	Rule ID
Honey pot device access	Always	1500000-1500003
Potential scan of surveillance device	Always	2000002/4
Unauthorized device access	Always	2000005/6
Unauthorized NTP time/DNS/SMTP server	Always	2000007-2000009
Suspected denial-of-service attack (……)*	Always	2000015-2000019
Attempt to modify insecure access on device	Always	2000022
Unauthorized HTTP/HTTPS access attempt on CyberVigilant	Always	2000768
FTP access on device on CyberVigilant	Always	2000769
HTTP access attempt on IP camera**/NVR	Full Protection	2000256/7, 2000512
Attempt to log-in to device	Full Protection	2000010
FTP access attempt on IP camera	Full Protection	2000160
HTTPS access attempt on device	Full Protection	2000020
Unauthorized HTTP access attempt on IP camera**/NVR	Configuration	2000258/9, 2000513
Attempt to access device with insecure protocol	Configuration	2000001
Unauthorized SSH log-in attempt to device	Configuration	2000011
Unauthorized FTP access attempt on IP camera	Configuration	2000161
Unauthorized HTTPS access attempt on device	Configuration	2000021

* RTSP SYN, HTTP POST (ONVIF), ICMP ping, NTP flood, HTTP SYN

** Except ONVIF commands