IndigoVision Control Center suite

Security Hardening

THIS MANUAL WAS CREATED ON TUESDAY, SEPTEMBER 6, 2022.

DOCUMENT ID: IU-SMS-MAN011-11

Legal Considerations

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

Copyright

Contact address

IndigoVision

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

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.

TABLE OF CONTENTS

1 INTRODUCTION

The Security Hardening Guide is intended to guide administrators in securely configuring IndigoVision Control Center. It is intended to supplement but not replace an organization's existing physical and information security policies.

The guide helps to securely configure the components which comprise the Control Center suite, as well as the environment in which it is deployed, including:

- Network infrastructure
- Control Center application and workstations
- Cameras, encoders, and NVRs
- Servers hosting the Site Database Server, Windows NVR-AS, License Server, Camera Gateway, Control Center Web, and other network services

Guidance is divided into two levels of protection:

- **Standard Protection**
  Guidance considered mandatory for any deployment of Control Center.
- **Enhanced Protection**
  Guidance for organizations who need to meet strict compliance requirements and have dedicated cyber-security resources.

2 NETWORK INFRASTRUCTURE

This section provides guidance in securing the network infrastructure used by Control Center.

Standard protection

This section provides guidance considered mandatory for any deployment of Control Center.

Physical security

All network infrastructure should be located in physically secure spaces, for example, communications cabinets. Access to these spaces should be monitored, logged, and restricted only to authorized administrators.

Isolate the Control Center network

Physical security systems such as Control Center should be deployed on a dedicated network which is physically isolated from corporate networks and the internet.

In a converged network environment, Control Center should be deployed on a network segment which is logically separated from other networks. This is commonly achieved using VLANs.

Firewalls should be deployed to control access between VLANs, as well as traffic between the Control Center network and external corporate networks or the internet.

Access to or from the Control Center network should only be authorized with a validated business requirement. Ports and protocols should be restricted only to those required.

Network segmentation

Large Control Center sites may consist of many hundreds of cameras and encoders. IndigoVision recommends that you follow networking best practices and separate the network into subnets.

Each subnet is typically routed using common Layer 3 networking protocols, such as OSPF for unicast data, or PIM Sparse Mode for multicast data.

For systems designed in this manner, IndigoVision recommends that you prevent each subnet containing cameras and encoders from accessing devices on other similar subnets.

Access between subnets may be carried out by a dedicated firewall appliance or by the simpler Access Control List (ACL) functionality, which is available on most routers and switches.

Firewalls

Firewalls should be deployed to control access between VLANs, as well as traffic between the Control Center network and external corporate networks or the internet.

Access to or from the Control Center network should only be authorized with a validated business requirement. Ports and protocols should be restricted only to those required.

► For details of the network ports required by IndigoVision hardware and software, refer to the Control Center Installation Guide Appendix IndigoVision Firewall Requirements.

Cameras, encoders, NVRs, and software components of the Control Center suite should NEVER connect directly to the internet.

Services designed to provide remote access, for example, Control Center Web, should always be positioned behind a firewall.

A Virtual Private Network (VPN) should be used to provide remote Control Center users with secure access to their system.

Switch ports

To reduce the risk that anyone will gain unauthorized access to the Control Center network, disable unused network switch ports.

Additionally, switch port security should be configured to ensure that only authorized device MAC addresses are allowed.

Fault monitoring

IndigoVision recommends that you configure fault detectors within Control Center for all cameras, encoders, NVRs, and license servers within a site.

Fault detectors can provide advance warning of an attempt to compromise or interfere with devices, as well as notification of device failure.

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

Enhanced protection

This section provides guidance for organizations who need to meet strict compliance requirements and have dedicated cyber-security resources.

Deploy CyberVigilant

An Intrusion Detection System (IDS), for example CyberVigilant, monitors a network continuously and can spot anomalies in network traffic patterns. These anomalies may be indicators of compromise (IoCs) which can be used to alert administrators of imminent attacks, and provide forensic evidence to assist with prosecution after a successful attack.

CyberVigilant from IndigoVision is an IDS that has been specifically designed for use with the Control Center suite. CyberVigilant reduces deployment time and cost by using the Control Center Site Database to automatically configure monitoring for video surveillance devices.

To complement CyberVigilant IDS sensor appliances, the CyberVigilant in Camera feature can be configured to block unauthorized access and generate alerts on supported cameras.

► For more information on IndigoVision CyberVigilant, refer to the CyberVigilant User Guide.

Use 802.1x Network Access Control (NAC)

Video surveillance devices may be physically deployed beyond an organization's perimeter. Network infrastructure used to provide connectivity to cameras could provide an attacker with access to the Control Center network.

Cameras, encoders, and NVRs can be configured to authenticate with network switches using 802.1x. Certificate-based authentication is recommended, although older devices may only support password authentication.

Network switches should be configured to enforce 802.1x NAC to ensure that only authenticated and authorized devices can access the network.

3 CONTROL CENTER APPLICATION AND WORKSTATIONS

This section provides guidance in securing Control Center workstations.

Standard protection

This section provides guidance considered mandatory for any deployment of Control Center.

Enable BIOS passwords and Secure Boot

To prevent the running of unauthorized software, or other attempts to bypass software security measures, IndigoVision recommends that you configure all Control Center workstation PCs with a BIOS password.

Passwords should meet the requirements of the National Institute of Standards and Technology (NIST) Special Publication 800-63-3:

- Minimum length of 8 characters
- Randomly generated using a password manager when possible
- Commonly used passwords should not be used

IndigoVision recommends using password manager software to securely store passwords.

Configure all workstations to use Secure Boot to ensure they only run authorized operating system software.

User authentication

Control Center can authenticate users using either a username and password combination delegating to Windows user authentication.

When Windows user authentication is used, IndigoVision recommends that you manage user accounts using Active Directory.

Passwords should meet the requirements of the National Institute of Standards and Technology (NIST) Special Publication 800-63-3:

- Minimum length of 8 characters
- Randomly generated using a password manager when possible
- Commonly used passwords should not be used

.

Control Center user accounts roles, and administrative privileges

Control Center user accounts should always be assigned the **Operator** role unless they require administrative privileges.

Users who require administrative privileges should always be assigned the **Restricted Administrator** role unless they require the ability to add or modify user accounts and permissions.

The **Full Administrator** role should only be used for administrators with a validated business requirement for adding or modifying user accounts and permissions.

Services which require access to Control Center resources, for example, Control Center Web or 3rd party integrations, should never use a full administrator account, or an account owned by a user. Service accounts should be created with least-privilege for their use-case.

When creating the Control Center site database, least-privilege can be enforced by ensuring that default access permissions for non-administrator users is set to **None**.

Windows user accounts

Prior to Control Center version 17.0, it was possible to assign multiple Control Center users to a single Windows user account. This was not recommended, and will prevent completion of the upgrade to Control Center version 17.0.

Control Center operators should not require privileges to install software or do administrative tasks, and therefore should not be assigned a Windows account with administrative privileges.

From Control Center version 18.2, it is possible to link a Control Center User Group to one or more Windows Active Directory groups. Any user who is part of a linked Active Directory group can log in to Control Center with the linked role and permissions without the need to be individually created as a Control Center user.

For security and clarity (to avoid unintended users accessing Control Center) it is recommended that the new Windows Active Directory groups are created. These may follow your organizations naming conventions, but it is recommended that they are clear which Control Center role they are tied to, for example, `MyOrg-IVCC-Operators`, or `MyOrg-IVCC-ResAdmin`.

Site database files

Prior to Control Center version 17.0, the Control Center site database was stored in a secure file share.

From Control Center version 17.0, most components of the Control Center site database are securely stored by the Site Database Server. However, a secure file share is still required for some items including maps, audio messages, and PTZ configuration files.

The file share should be configured so that it is only readable by authorized Control Center user accounts. Additionally, write permissions should only be assigned to Control Center administrator users and any operator that needs the ***Rename*** access permission.

Remove old or duplicate site databases

Some administrators may create duplicate copies of the Control Center site database during migrations, upgrades, or for backup purposes. These copies should be deleted if

they are not in use, or stored securely offline if required for backup.

When upgrading to Control Center version 17.0 or later, the Site Database Server Setup tool preserves the files contained in the site database directory to avoid service interruption for Control Center workstations which have not yet been upgraded.

After all workstations have been upgraded, these files should be deleted.

► For more information on the upgrade process, refer to the Control Center Installation Guide.

Windows Update

IndigoVision recommends that all workstations running the Control Center front-end application have Windows Update enabled and that updates are applied as soon as practicable after release.

IndigoVision only supports operation of Control Center on operating systems that remain within Microsoft's support policy.

► For more information, refer to the Control Center Client front-end application operating system specifications in the Installation Guide.

Software and firmware update

You should routinely review and update other software and device drivers installed on a Control Center workstation to ensure they are up to date.

Reputable software manufacturers regularly update their software in light of security vulnerabilities. If you do not keep ancillary software on a workstation up to date, this may lead to the security of the workstation being compromised.

Some updates make changes to licensing agreements. Make sure you understand these changes before applying the update. For example, the latest Java versions may require a commercial agreement.

IndigoVision recommends that you do not install additional software on Control Center workstations without a validated business need.

Endpoint protection and antivirus

Endpoint Detection and Response (EDR) solutions should be used to supplement Windows Security and centrally manage security policies and malware protection.

Although IndigoVision recommend deploying Control Center on dedicated workstations which are not used for other business applications or internet access, this may not be possible in some customer environments. In these cases, it is particularly important to deploy endpoint protection and antivirus software to protect against threats which may be introduced by other applications.

Control video exports

Export Locations in Control Center should be used to ensure that video export is only allowed to authorized storage locations.

Control Center users assigned the **Operator** role should only be granted ***Export*** permission with a validated business need to export recorded video.

Secure site database communications

Control Center uses the Server Message Block (SMB) protocol to communicate with the file share which hosts the Control Center site database, prior to version 17.0, or site database files, beginning with version 17.0.

SMB encryption should be enabled to provide end-to-end encryption of the site database files in transit between Control Center and the site database file share. Refer to Microsoft's documentation to enable SMB encryption.

SMBv1 and SMBv2 should not be used.

Workstations and file servers should always be configured in accordance with the latest Microsoft security guidance and patched regularly to protect against SMB vulnerabilities such as ***SMB Ghost*** and ***SMBleed***.

► For more information on the configuration of SMB, refer to Microsoft's documentation.

Enhanced protection

This section provides guidance for organizations who need to meet strict compliance requirements and have dedicated cyber-security resources.

Deploy Control Center Client

The Control Center application is the Control Center suite's user interface for configuration, viewing video, and handling alarms. A hardened version of Control Center, called Control Center Client, is also included in the Control Center suite.

Control Center Client cannot write to the site database, regardless of file share permissions or Site Database Server configuration.

If there is no need for administrators to modify the site database on a given workstation, IndigoVision recommends that you deploy Control Center Client to that workstation.

Audit logging

Control Center can maintain a central audit log of actions carried out within the Control Center front-end application.

IndigoVision recommends that you configure an audit log database to allow actions of operators to be reviewed for suspicious activity, and for forensic purposes in the event of misuse.

IndigoReports can be deployed to simplify audit log deployment and provide comprehensive reporting capabilities.

Alternatively, Control Center can be configured to use ODBC to log to a customer-hosted database. In this case, the customer-hosted database should be hardened according to the database vendor's recommendations or Center for Internet Security (CIS) benchmark, if one exists.

Offline Windows Updates

Many security networks do not have a direct Internet connection. Microsoft provide Windows Server Update Services (WSUS) which allows updates to be distributed within an otherwise isolated network.

You should also use WSUS to test updates for correct operation prior to rolling out to all workstations.

Alternatively, a 3rd-party patch management solution should be used to keep all Control Center workstations up-to-date.

Vulnerability scanning

Automated vulnerability scanning tools should be used to scan workstations on a regular basis. These tools ensure that workstations are updated, patched, and configured according to an organization's security policies or operating system benchmark.

Hardware security

IndigoVision recommends that you control access to Control Center workstations using physical access control measures.

USB ports should be disabled or physically protected without a validated business need to use them.

Tools, for example Nirsoft's USB LogView or USBDeview, can be used to monitor usage of USB devices on workstations.

4 CAMERAS, ENCODERS, AND NVRS

This section provides guidance in securely configuring cameras, encoders, and NVR appliances.

NVR appliances refer to IndigoVision NVR-AS 3000, Compact NVR-AS 4000, and Enterprise NVR-AS 4000 Linux appliance.

Security guidance for NVR-AS 4000 Windows as well as 3rd party servers hosting Windows NVR-AS software is provided in the information about servers.

► For more information, *see "Servers" on page 23*.

Standard protection

This section provides guidance considered mandatory for any deployment of Control Center.

Firmware

Firmware is the software installed within a camera or encoder that controls the operation of the device. IndigoVision regularly updates the firmware for its range of cameras and encoders with new features, security enhancements, and bug fixes. Before use, update the firmware for each device to the most recent version.

IndigoVision Control Center offers a mechanism to bulk upgrade both IndigoVision devices and 3rd party devices which support ONVIF firmware upgrade.

Reset to factory default settings

Before attempting to install or secure a device, reset the device to its factory default settings.

► For more information, refer to the appropriate guide for the device.

Set the administrator password

Setting a strong administrator password on a device is critical to ensuring its network security and ensuring that it can only be accessed by authorized users.

Passwords should meet the requirements of the National Institute of Standards and Technology (NIST) Special Publication 800-63-3:

- Minimum length of 8 characters
- Randomly generated using a password manager when possible
- Commonly used passwords should not be used
- Different from the default password

Warning

Most modern devices do not have default passwords, and require the user to configure a password on first boot. On legacy devices or 3rd party devices which are supplied with a default password, IndigoVision recommends changing the password before deployment.

Caution

Some modern devices are pre-configured with HTTPS communications out-of-the-box. If HTTPS is not configured prior to changing the device password, eavesdropping may be possible. Enable HTTPS prior to changing the password when possible, or change the password again after enabling HTTPS.

- Unique passwords should be used for each device

Enable NVR-AS authentication

Before deployment, configure NVR-AS to require authenticated access. Unauthenticated access should not be permitted.

Passwords should meet the requirements of the National Institute of Standards and Technology (NIST) Special Publication 800-63-3:

- Minimum length of 8 characters
- Randomly generated using a password manager when possible
- Commonly used passwords should not be used
- Unique passwords should be used for each device

Configure time synchronization

Ensuring time synchronization across all devices within a Control Center system is required for proper system operation, performance, and security. Specifically, time synchronization is a key element in proving the integrity of video recordings, alarm events, and audit logs.

Time synchronization discrepancies are often a result of misconfiguration, but they may also indicate malicious activity.

► For more information on Control Center time synchronization requirements, as well as instructions for installing and configuring an NTP server, refer to the Control Center Install Guide.

Although you can manually configure the time on a given device, IndigoVision recommends that you use the Network Time Protocol (NTP) to automatically and continuously synchronize the time.

Every IndigoVision Camera and Encoder has the ability to specify an NTP time server.

► For more information on configuring the NTP time server, refer to the appropriate guide for the device.

Disable unnecessary or insecure services

To minimize the attack surface for intruders, disable services on a given device that are not required for normal operation.

The following services are commonly used on surveillance devices but are not required for basic Control Center operations, and should be disabled unless justified by a validated business requirement:

- SFTP
- SSH
- DDNS
- SMTP
- SNMP
- Bonjour
- GB/T28181
- ARP/Ping configuration of IP addresses
- Audio
- IPv6
- ONVIF WS Discovery (required for device discovery but can be disabled after adding the device to Control Center)

Additionally, some surveillance devices may support services which have been deprecated after the device was manufactured and are no longer considered secure. Where possible, these services should always be disabled and should never used:

- Telnet
- FTP
- SNMPv1
- SNMPv2
- HTTPS using TLSv1 or TLSv1.1

Disable basic HTTP authentication

Some third-party IP cameras support HTTP basic authentication, which sends passwords in plain text over the network. Ensure that HTTP basic authentication is disabled.

Control Center supports HTTP digest authentication which securely hashes passwords used in ONVIF requests.

Enhanced protection

This section provides guidance for organizations who need to meet strict compliance requirements and have dedicated cyber-security resources.

Enable HTTPS

HTTPS is a secure communications protocol used between clients, for example, Control Center or a web browser, and web servers, for example, cameras and encoders. HTTPS provides security in two ways:

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

Cameras typically have three interfaces which can be secured using HTTPS:

- The camera's web interface, which is accessed using a browser for configuration.
- The camera's ONVIF configuration interface, which is used by Control Center for command-and-control communications, for example ONVIF media profile information, alarms and events, or control of relay outputs.
- The camera's ONVIF streaming interface, which is used by Control Center for streaming video.

Many modern cameras support the use of HTTPS for web interfaces as well as ONVIF interfaces, while some cameras may only support the use of HTTPS to secure the web interface.

Where possible, both web interfaces and ONVIF interfaces should be secured using HTTPS.

► For more information on camera HTTPS configuration, refer to camera documentation.

Some modern cameras are pre-configured with a self-signed HTTPS certificate. Otherwise, most cameras allow the user to generate a self-signed certificate for quick configuration of HTTPS. Using HTTPS with a self-signed certificate does provide enhanced security over HTTP by encrypting the communications. However, authenticity of the sender and receiver cannot be confirmed by a trusted certificate authority when using a self-signed certificate. Therefore, use of certificates issued and signed by a trusted certificate authority is recommended.

When creating the Control Center site database, HTTPS should be enabled if the site's cameras provide HTTPS support. This allows Control Center to add cameras to the site using HTTPS for ONVIF configuration communications. After cameras have been added, their live and recording profiles should be configured to use the **Firewall Friendly** transport type to ensure video streaming over HTTPS.

► For more information on Control Center HTTPS configuration, refer to Control Center help.

While the exclusive use of HTTPS instead of HTTP is a best practice, many customer sites may be significantly comprised of cameras which do not fully support HTTPS. IndigoVision recommends that all customers move toward exclusive use of HTTPS as soon as practically possible.

Configure a dedicated Control Center device user account on each camera

In a typical installation, devices are accessed in the following ways:

- Through the administration web user interface for configuration purposes
- Through the ONVIF protocol for use as part of the Control Center suite

IndigoVision recommends that you create a dedicated administrator-level user to allow Control Center to access the device.

This allows you to change the main administrator account password without requiring Control Center to be reconfigured or operations to be interrupted.

Enable CyberVigilant-in-Camera, or the camera's firewall

All IndigoVision cameras and encoders, as well as most 3rd party surveillance devices, contain a built-in firewall. Firewalls should be enabled and configured to ensure that only authorized devices communicate with a given camera.

Authorized devices could include Control Center workstations, NVRs, NTP or DNS servers, network monitoring systems, or workstations used for administration using camera web interfaces.

Depending on the device, this feature may be called ***CyberVigilant-in-Camera*** (on supported IndigoVision cameras), firewall, or IP Filtering.

Some firewalls allow both blacklisting and white-listing, while some only allow one or the other.

Using blacklisting, only those IP addresses on the blacklist are not allowed to communicate with the device.

Using white-listing, only devices on the white-list are allowed to communicate with the device.

White-listing is more secure, and should always be used where possible.

CyberVigilant-in-Camera's authorized device list is a white-list. After enabled, only those devices on the authorized device list will be allowed to communicate with the camera.

► For more information on configuring camera firewalls, refer to camera documentation.

Use 802.1x Network Access Control (NAC)

Video surveillance devices may be physically deployed beyond an organization's perimeter. Network infrastructure used to provide connectivity to cameras could provide an attacker with access to the Control Center network.

Cameras, encoders, and NVRs can be configured to authenticate with network switches using 802.1x. Certificate-based authentication is recommended, although older devices may only support password authentication.

Network switches should be configured to enforce 802.1x NAC to ensure that only authenticated and authorized devices can access the network.

Encrypt FrontLine video storage and VideoManager communications

IndigoVision recommends that you encrypt the directory that you use to store the video retrieved from FrontLine cameras. This is the default setting when configuring Motorola Solutions VideoManager. Encryption ensures that unauthorized users cannot access video footage after it is downloaded from the cameras but before it is imported into the NVR-AS video library.

► For more information on enabling footage encryption, refer to the Motorola Solutions VideoManager documentation.

IndigoVision also recommends that you use HTTPS for the VideoManager web interface to ensure confidentiality and prevent interception by third parties. Using HTTPS secures the communication channel between the FrontLine Manager Interface and VideoManager used by Control Center and the NVR-AS for managing Body Worn Video users and importing video footage.

► For more information on enabling HTTPS, refer to Chapter 3 of the FrontLine Manager Administrator's Guide.

Physical access to FrontLine camera docks

Using a FrontLine dock controller allows you to position the camera docks in a physically separate location to the NVR-AS. The docking stations are connected to the dock controller

by USB. The dock controller communicates with VideoManager over a network connection. This allows you to position the NVR-AS in a secure space, for example, a server room, while still enabling users to dock and undock cameras elsewhere on the premises.

► For more information on dock controllers, refer to the VideoManager documentation.

Secure access to VideoManager credentials

Sensitive information used by the FrontLine Manager Interface to communicate with Motorola Solutions VideoManager is stored in the Windows registry. This information is encrypted but to prevent access by unauthorized users, you should still configure appropriate access controls on the NVR-AS.

5 SERVERS

This section provides guidance for securing Windows-based servers used for hosting components of the Control Center suite including the Site Database Server, Windows NVR-AS, License Server, Camera Gateway, Control Center Web, and other integrated network services.

Standard protection

This section provides guidance considered mandatory for any deployment of Control Center.

Physical security

All network infrastructure should be located in physically secure spaces, for example, communications cabinets. Access to these spaces should be monitored, logged, and restricted only to authorized administrators.

Enable BIOS password

Enable requiring a password for BIOS setting changes to prevent malicious actors from disabling any other security measures that are put in place at the BIOS level.

Change iDRAC password

Each IndigoVision Enterprise NVR-AS 4000 comes with a default iDRAC password. This password is unique for each system, however, IndigoVision still recommends changing the password.

Windows Update

IndigoVision recommends that you enable Windows Update on all NVR-AS 4000 Windows Appliances and third-party Windows servers, and that you apply updates as soon as practicable after release.

IndigoVision only supports operation of Control Center on operating systems that remain within Microsoft's support policy.

Software and firmware update

Firmware for NVR-AS 3000 and NVR-AS 4000 Linux appliances is regularly updated with security and other bug fixes. You should apply updates as soon as practicable after release to ensure the on-going security of the Control Center site.

As with Control Center workstations, you should regularly review and update software, device drivers or embedded firmware for components of NVR-AS 4000 Windows appliances or other third-party Windows servers.

Antivirus

IndigoVision recommends that Windows Security is enabled and updated on all servers for malware protection.

On servers hosting Windows NVR-AS, Camera Gateway, or Video Stream Manager, Windows Security, exclusions for these services should be added to Windows Security Virus and Threat protection to prevent performance impact.

On servers hosting Windows NVR-AS, the video storage directory should also be added as an exclusion to Windows Security Virus and Threat protection.

If another antivirus or EDR solution is deployed instead of Windows Security, the exceptions described above should be configured.

Windows firewall

IndigoVision recommends enabling the Microsoft Windows firewall on all servers and ensuring that only authorized applications may access the network.

- For information about the network ports required by the Control Center front-end application, refer to the Control Center Installation Guide Appendix IndigoVision Firewall Requirements.

Isolate storage networks

When using Windows NVR-AS software with a third-party network storage solution using iSCSI or Network Attached Storage (NAS), the storage device should be located on a dedicated network which is logically isolated and firewalled from the Control Center network, corporate networks, and the internet.

Secure baseline configuration

IndigoVision NVR-AS4000 appliances are supplied with a hardened configuration, and unnecessary services are disabled or removed.

3rd party Windows-based servers used to host IndigoVision applications should be hardened with a secure baseline configuration, or using the relevant Center for Internet Security (CIS) benchmark for the server's version of Microsoft Windows.

Enhanced protection

This section provides guidance for organizations who need to meet strict compliance requirements and have dedicated cyber-security resources.

Automate security policy auditing

Automated vulnerability scanning tools should be used to scan workstations on a regular basis. These tools ensure that servers are updated, patched, and configured according to an organization's secure baseline configuration or operating system benchmark.

Secure Boot

Secure Boot is a part of the UEFI specification. It prevents a system from using boot loaders, drivers, or other critical operating system files if they do not have a recognized digital signature. This prevents a system from using those files if they are affected by malware or other malicious actors.

► For more information on how to enable Secure Boot, refer to the appropriate guide for the system.

Disable insecure TLS versions

IndigoVision recommends disabling TLS 1.0 and 1.1 for the Windows Schannel Security Support Provider (SSP) on all NVR-AS 4000 Windows appliances and third party Windows servers.

► For more information on how to disable TLS 1.0 and 1.1, refer to Microsoft's documentation.

6 CONTROL CENTER WEB

This section provides guidance for securing the Control Center Web server.

All recommendations made for other Control Center servers apply to servers running Control Center Web. IndigoVision recommends additional security measures as Control Center Web is intended to provide remote access to internet-based web and mobile users.

The Control Center Web server should not be deployed directly on the internet. Control Center Web should always be deployed behind a firewall which restricts all inbound traffic which is not required for normal operation.

► For more information on firewall port requirements, refer to the appropriate appendix in the Control Center Installation Guide.

Site Database

Control Center Web is designed to work seamlessly with the same site database as an existing Control Center installation. It provides access to all users configured in the site database to all cameras they can access through Control Center.

If remote web or mobile access is only required for a small subset of the cameras or users in the Control Center site database, a separate site database should be used which only contains those cameras and users required for remote web or mobile access.

► For more information on configuring the site database securely, *see "Site database files" on page 12*.

Media server operating system updates

IndigoVision strongly recommends that the PC or virtual machine running the media server is kept up to date by enabling automatic OS updates through the `unattended-upgrades` package.

► For more information on how to configure OS updates, refer to the Control Center Web Administrator's Guide

Application Pool Identity

Control Center Web uses the `ApplicationPoolIdentity` Identity by default. This is the most secure and least privileged way to run the application pool.

In order to use a shared site database, it may be necessary to change this Identity to a different user account. When doing so, IndigoVision recommends that you choose an account that has the minimum privileges required for accessing the site database and no additional permissions.

IndigoVision strongly discourage the use of `NetworkService`, `LocalService` and `LocalSystem` identities with Control Center Web.

► For more information on using a shared site database in Control Center Web, refer to the Control Center Web Administrator's Guide.

HTTPS and TURNS

Control Center Web is designed to only support encrypted communication channels between client devices on the Internet and the Control Center Web servers.

It is not possible to use HTTP with the application server, as only HTTPS is supported.

While it is possible for an Administrator to configure the coTURN server on the media server to use TURN without encryption, IndigoVision strongly recommends that TURNS is used with the media server to ensure all signaling is encrypted.

IndigoVision recommends that the coTURN password configured on the media server should meet the following requirements.

Passwords should meet the requirements of the National Institute of Standards and Technology (NIST) Special Publication 800-63-3:

- Minimum length of 8 characters
- Randomly generated using a password manager when possible
- Commonly used passwords should not be used