

SN-7

Security Hardening Guide

Version 1.3.0
(June. 19. 2026)

Table of Contents

Abbreviation	4
1 Introduction	5
2 Overview of IDIS Security Features	6
2.1 Security Features List	6
2.2 Default Security Configuration	7
2.3 Security Levels.....	9
2.4 Personal Information Security Configuration	10
2.5 Secure Communication Environment.....	10
3 Data Security Features	11
3.1 iBank	11
3.2 Chained Fingerprint.....	11
3.3 Password Encryption	13
3.4 Configuration Data Encryption.....	13
3.5 Extracted Data Encryption.....	13
3.6 Secure Data Protection in IDIS Devices	15
3.7 Implementation of a Secure Element for Secure Storage.....	15
4 Transmission Security Features	18
4.1 Staged SSL/TLS including Intelligent TLS	18
4.2 FEN (For Every Network) Security.....	21
4.3 IDIS Web Server	22
4.4 ICM (IDIS Cloud Manager) Security	24
4.5 Data Integrity	25
5 Access Security Features	26
5.1 Closed Network with Separate Subnet	26
5.2 Certificate-based Mutual Authentication (DirectIP 2.0)	26
5.3 Password Policy.....	27
5.4 Backdoor-Free Architecture	28
5.5 2FA (Two-Factor Authentication).....	28
5.6 IP Filtering.....	29
5.7 Firewall	30
5.8 IEEE 802.1X Authentication	31
5.9 Restricted Network Port Access	31
5.10 IDIS Inbound Essential Network Port List	32
5.11 USB Interface and Class Support.....	32
5.12 Access Control for Specific User or User Group	32
5.13 Covert.....	34
6 Personal Information Security Features	36
6.1 Privacy Masking.....	36
6.2 IDIS Vulnerability Management Policy	40
6.3 Vulnerability Assessment Principles.....	41
6.4 Secure Firmware Upgrade Sequence for IDIS Products	42
7 Manufacturer's Obligations for Providing Security and Safety Information to Users	43
7.1 Security Update Notifications and Customer Communication Procedures	43
7.2 Cyber Security Policy	43
7.3 Security Precautions for Product Transfer or Disposal	43

Contact Us..... 45
References 45
Version History 46

Abbreviation

- BRP: Boost Remote Performance
- DirectCX: IDIS HD Analog System Solution
- DirectIP: IDIS IP System Solution
- DVR: Digital Video Recorder
- EAP: Extensible Authentication Protocol
- FEN: For Every Network
- GUI: Graphic User Interface
- HTTP: Hypertext Transfer Protocol
- HTTPS: Hypertext Transfer Protocol Secure
- ICM : IDIS Cloud Manager
- ICMP: Internet Control Message Protocol
- ID: Identification
- IDPM: IDIS Dynamic Privacy Masking
- ISS: IDIS Solution Suite
- NAT: Network Address Translation
- NVR: Network Video Recorder
- OTP: One-Time Password
- PCI: Payment Card Industry
- SHA: Secure Hash Algorithm
- RSA: Rivest–Shamir–Adleman (public-key cryptosystem)
- SSL: Secure Socket Layer
- TLS: Transport Layer Security
- TVR: HD-TVI DVR
- 2FA: Two-Factor Authentication

1 Introduction

In the past, video surveillance systems were typically completely separate from the local area network and the Internet, sending video of coaxial cables directly to a recorder. Cybersecurity requirements were fairly low due to their isolated nature. Primary concerns were physical attacks, such as destruction of the equipment (most often the cameras), illegally deleting or copying the recorded data, cutting video cables, covering the camera lens, etc.

Today, many video surveillance systems now used IP-based equipment which send the recorded video across ethernet cables to local, remote, and cloud-based recorders, sometimes using the same local area network infrastructure that is used by general office workers. Additionally, remote monitoring and control of these systems via network clients or mobile applications is now very common. Today's systems also support data communication with third-party systems such as access control, intrusion detection, and video analytics solutions.

In this environment, the threat of cyberattack against a video surveillance system has greatly increased, making cybersecurity a top area of concern for customers and operators. The same local security issues of past systems are also still present and must be addressed in the overall security posture. Overall, the integrity, confidentiality, and accessibility of video surveillance data must be protected during recording, retrieval, and while in-transit, whether across the local network or across a public network to a remote location. To meet these challenges, IDIS has designed and built various security technologies and features into our products and continues to add to and strengthen these technologies as the security climate evolves.

This document describes the security features and functions of IDIS video surveillance products and how to configure the features to optimize the security of your surveillance system. A general overview of all IDIS security features is described in chapter 2, while a more thorough explanation of each feature and its configuration options follows in the following chapters.

This document is a general guideline for configuring IDIS products, so the pictures of the user interfaces may vary slightly depending on the version and type of product being configured.

2 Overview of IDIS Security Features

2.1 Security Features List

The following table is a listing of all of the current and under development security features of IDIS products.

Category	Security features	Applied products	Security requirement	Identity
Data Security	iBank	All	Confidentiality, Integrity, Availability	Yes
Data Security	Chained Fingerprint	All	Integrity	Yes
Data Security	Edge Encryption Recording	All (Under development)	Confidentiality, Integrity	Yes
Data Security	Password Encryption	All	Confidentiality	
Data Security	Information and Configuration Data Encryption	All	Confidentiality	
Data Security	Extracted Data Encryption	All	Confidentiality	
Data, Access Security	Video Clip Management and Security	The customized solution	Availability	Yes
Transmission Security	Staged SSL/TLS including Intelligent TLS	All	Confidentiality, Integrity, Availability	Yes
Transmission Security	FEN Security	All	Confidentiality, Availability	Yes
Transmission, Access Security	IDIS Web Server	IP camera, NVR, TVR, IDIS Solution Suite	Confidentiality, Availability	Yes
Transmission, Access Security	ICM (IDIS Cloud Manager) Security	ICM	Confidentiality, Availability	Yes
Transmission Security	Staged SSL/TLS	All	Confidentiality	Yes
Transmission Security	FEN Security	All	Confidentiality	Yes
Transmission, Access Security	IDIS Web Server	IP camera, NVR, TVR, IDIS Solution Suite	Confidentiality	Yes
Access Security	Closed Network with Separate Subnet	IP camera, NVR	Availability	Yes
Access Security	Complex Password Entry	All (In progress)	Availability	
Access Security	Backdoor Free Architecture	All	Availability	
Access Security	2FA (Two-Factor Authentication)	NVR	Availability	
Access Security	IP Filtering	IP camera, IDIS Solution Suite	Availability	
Access Security	Firewall	H.265 NVR, IDIS Solution Suite	Availability	

Category	Security features	Applied products	Security requirement	Identity
Access Security	Certificate-Based Mutual Authentication (DirectIP 2.0)	DirectIP 2.0 IP camera and NVR	Availability	Yes
Access Security	IEEE 802.1X Authentication	IP camera	Availability	
Access Security	Restricted Network Port Access	All	Availability	
Access Security	Remote Connection Control	H.265 NVR	Availability	
Access Security	Accessible Time Restriction	IDIS Solution Suite	Availability	
Access Security	Covert	All	Availability	
Access Security	Temporary Remote Access Authentication (OTP)	H.265 NVR (In progress)	Availability	
Personal Information Security	Static Privacy Masking for Live Monitoring and Recording	All	Privacy	
Personal Information Security	Static Privacy Masking for Video Clip	IDIS Solution Suite	Privacy	
Personal Information Security	Dynamic Privacy Masking for Video Clip	IDPM software	Privacy	Yes

2.2 Default Security Configuration

2.2.1 Fixed security features

The following security features are enabled by default and cannot be disabled by the user.

Features	Products	Default
iBank	All	Applied
Chained Fingerprint	All	Applied
Password Encryption	All	Applied
Information and Configuration File Encryption	All	Applied
Closed Network with Separated Subnet	IP camera, NVR	Applied
Certificate-Based Mutual Authentication	DirectIP 2.0 IP camera and NVR	Applied
Backdoor Free Architecture	All	Applied
Restricted Network Port Access	All	Applied
Video Clip Management and Security	The customized solution	Applied

2.2.2 Configurable security features

The following security features are configurable by the user.

Features	Products	Default	Configurable options
Edge Encryption Recording	All	Off	Off / On
Extracted Data Encryption	All	Off	Off / On
Staged SSL/TLS	IP camera <-> NVR	Off, None	None / Standard / High / Very High
	NVR, TVR <-> remote client software	Off	Off / On
	IDIS Solution Suite services and client	None	None / Header / Exclude Multimedia / Full / Intelligent TLS
FEN Security	All	Applied	Same as Staged SSL/TLS
ICM Security	ICM service <-> ICM client	Applied	None
	IP camera, NVR, TVR <-> ICM service	Applied	None
	IP camera, NVR, TVR <-> ICM client	Off	Same as Staged SSL/TLS
IDIS Web Server	IP camera	On	Off / On
	NVR, TVR	Off	Off / On
	IDIS Solution Suite	Registered (On) – when a web service is installed	Register (On) / Unregister (Off)
Complex Password Entry	DirectIP 2.0 IP camera and NVR	Initially required	Password changeable
	Other products except DirectIP 2.0 products	Not initially required (a default password is used)	Complex password entry is not currently required, but it will be required in the near future.
2FA (Two-factor Authentication)	NVR	Off	Off / On
IP Filtering	IP camera, IDIS Solution Suite	Off	Off / On On: Allow or deny specific IP addresses
Firewall	H.265 NVR, IDIS Solution Suite	Off	Off / On On: Drop, allow, or deny specific IP or MAC addresses, port numbers, etc.
IEEE 802.1X Authentication	IP camera	Off	Off / On On: Certificate and EAP information
Remote Connection Control	H.265 NVR	Off	Off / Camera is Hidden / Schedule / Auto Expiration / Waiting Period
Accessible Time Restriction	IDIS Solution Suite	Always Allowed	Always Allowed / Time Coverage Setup / Set Manually
Covert	IP camera, NVR, TVR	Off	Off / Covert 1 / Covert 2
	IDIS Solution Suite	Unsupported	Covert can be approximated using the device access authority feature
Temporary Remote Access Authentication	H.265 NVR	Off	Off / On
Static Privacy Masking for Live Monitoring and Recording	All	Off	Off / On On: Set the specific privacy masking area

Features	Products	Default	Configurable options
Static Privacy Masking for Video Clip	IDIS Solution Suite	Off	Off / On On: Set the specific privacy masking area
Dynamic Privacy Masking for Video Clip	IDPM software	Off	Off / On On: Set the specific privacy masking area

2.3 Security Levels

Each security feature can be set depending on the required security level. The following table shows an example configuration of each security feature based on security level.

Features	Products	Level 1 (Low)	Level 2 (Middle)	Level 3 (High)
Edge Encryption Recording	All	Off	On	On
Extracted Data Encryption	All	On	On	On
Staged SSL/TLS, FEN Security	IP camera <-> NVR	None	Standard, High	Very High
	NVR, TVR <-> remote client software	Off	On	On
	IDIS Solution Suite services and client	None	Header, Exclude multimedia	Full
ICM Security	IP camera, NVR, TVR <-> ICM client	None, Off	Standard, On	Full, On
Complex Password Entry	All	Use complex password	Use complex password	Use complex password
2FA	NVR	Off	On	On
IP Filtering	IP camera, IDIS Solution Suite	On	On	On
Firewall	H.265 NVR, IDIS Solution Suite	On	On	On
IEEE 802.1X authentication	IP camera	Off	Off	On
Remote Control Connection	H.265 NVR	On	On	On
Accessible Time Restriction	IDIS Solution Suite	On	On	On
Temporary Remote Access Authentication	H.265 NVR	On	On	On

2.4 Personal Information Security Configuration

The recommended configuration for personal information security such as covert or privacy masking is shown below.

Features	Products	Configuration
Covert	IP camera, NVR, TVR	Covert 1 or Covert 2
Static Privacy Masking for Live Monitoring and Recording	All	On
Static Privacy Masking for Video Clip	IDIS Solution Suite	On
Dynamic Privacy Masking for Video Clip	IDPM software	On

2.5 Secure Communication Environment

For security reasons, IDIS products must only be used in a protected communication environment.

- VPN environment: Ensure that remote access to devices is established through a secure VPN tunnel.
- Dedicated line: When applicable, connect via a private, dedicated line isolated from public networks.
- Physically/Logically Protected Network: Devices must be deployed in a network that is physically secured or logically segmented (e.g., VLAN, firewall protection).

Users are strictly advised not to connect IDIS products directly to an unprotected or public network.

3 Data Security Features

3.1 iBank

iBANK is IDIS proprietary multimedia database for robust and effective data recording and searching even when multimedia data is overwritten or deleted frequently.

The iBANK architecture is used by all IDIS recorders and is setup when a recorder's storage is formatted as the Record type. This creates multiple banks on the storage device.

This makes it very difficult for unauthorized users to read the data recorded by IDIS recorders without IDIS specific player software. In addition, the iBANK can search all recorded data except the damaged data even if a part of HDD is damaged such as bad sectors and important data such as index is lost.

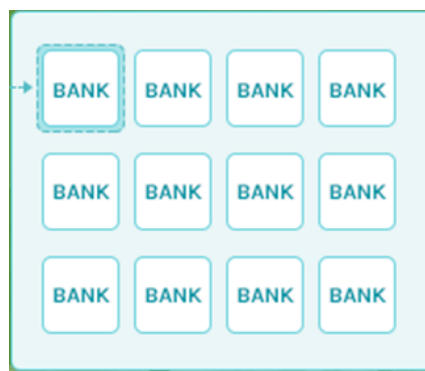


Figure 3.1.1: iBank structure: multiple banks on storage device

3.2 Chained Fingerprint

3.2.1 Introduction

Video fingerprinting is a technique in which software identifies, extracts, and then summarizes characteristic components of a video recording, enabling that video to be uniquely identified by its resultant 'fingerprint'. This technology has proven to be effective at identifying and comparing digital video data [1].

However, this common video fingerprinting technique is not a good enough to ensure a video has not been altered either from corruption or intentionally, because it is not easy to detect a change in a single frame/image among the large amounts of frames/images in a video clip.

IDIS Chained Fingerprint¹ is an efficient digital fingerprinting technique, designed to solve this problem, making it simple to authenticate whether the video clip is a faithful copy of the originally recorded video footage.

As shown in Figure 3.2.1, when image (A) is recorded, a digital fingerprint (A') is generated and stored with the image. This fingerprint (A') is used along with information from image (B) to generate fingerprint (B'). This continues with each new recorded image, creating a continuous chain of fingerprints such as A', B', and C'.

Now, if one of images in the chain or its fingerprint is modified, the chain is broken, which is easily detectable. Thus, the authenticity of recorded video can be detected by the chained fingerprint method.

¹ Patent No.: [10-0440783 \(Jul. 2004. KOR\)](#)

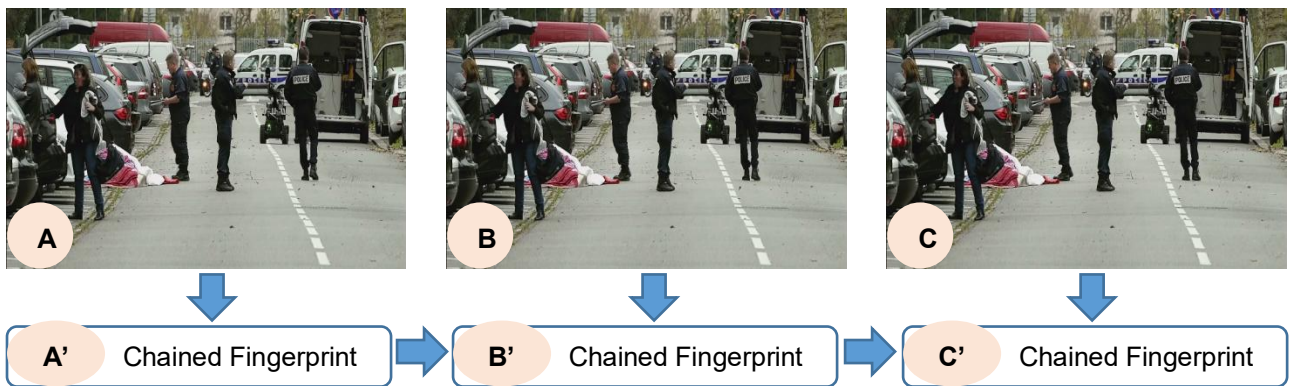


Figure 3.2.1. Chained Fingerprint Method

In addition, whenever recorded video is exported as a clip file, IDIS recorders and software will check the authenticity of each image using the chained fingerprint value and regenerate the fingerprint value for the new clip file. Thus, the authenticity of video footage is validated and preserved during export.

Please note that transcoding or editing the video, often used for privacy masking a video clip, breaks the chain making it impossible for others to authenticate the video.

3.2.2 Checking the authenticity of recorded or clipped video using chained fingerprint

The chained fingerprint functionality is enabled by default and there are no configuration options.

When playing a recorded video on an IDIS recorder, if the recorded image and the chained fingerprint value do not match, the video will not play or will display abnormal images. Additionally, a 'Fingerprint: broken!' error message will typically be visible in the debug log.

When playing a clip file, the authenticity of the clip will be shown as an icon in the bottom-right side of the video as shown in Figure 3.2.2. If the clip is authentic a green checkmark will be displayed, otherwise a red error symbol will be displayed.

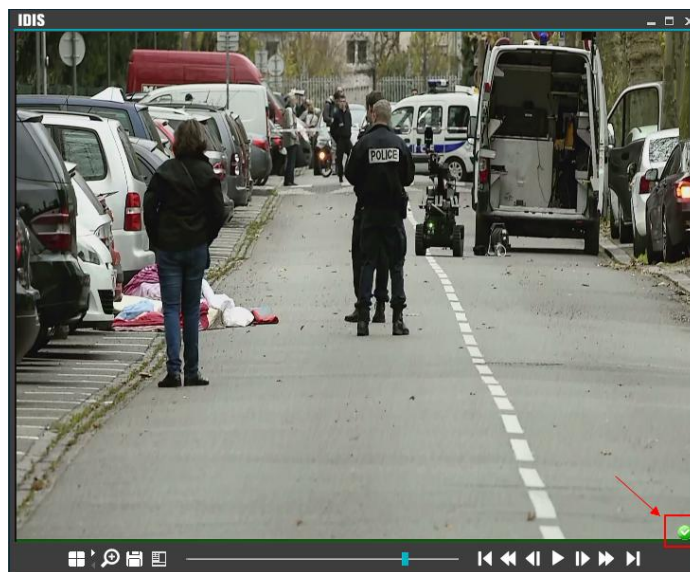


Figure 3.2.2. The green checkmark icon shows that the video clip hasn't been altered

3.3 Password Encryption

The passwords for registered users and devices are automatically encrypted to prevent them from being decrypted by unauthorized users.

In addition, IDIS NVRs encrypt both the user ID and password used in network communications protocols such as RTSP/RTP, DirectNDC (VNC), SMTP, NetFS (FTP), and HTTP notification by issuing self-signed certificates. These passwords can be set and managed separately from the passwords used for general operation such as setup, monitoring, and searching.

3.4 Configuration Data Encryption

The configuration data (including user and device information) of IP cameras and recorders are stored as binary files, not plain-text file, which aren't readable in a simple text editor. IDIS NVRs encrypt the user information data such as account, password, and email, which are saved in non-volatile memory.

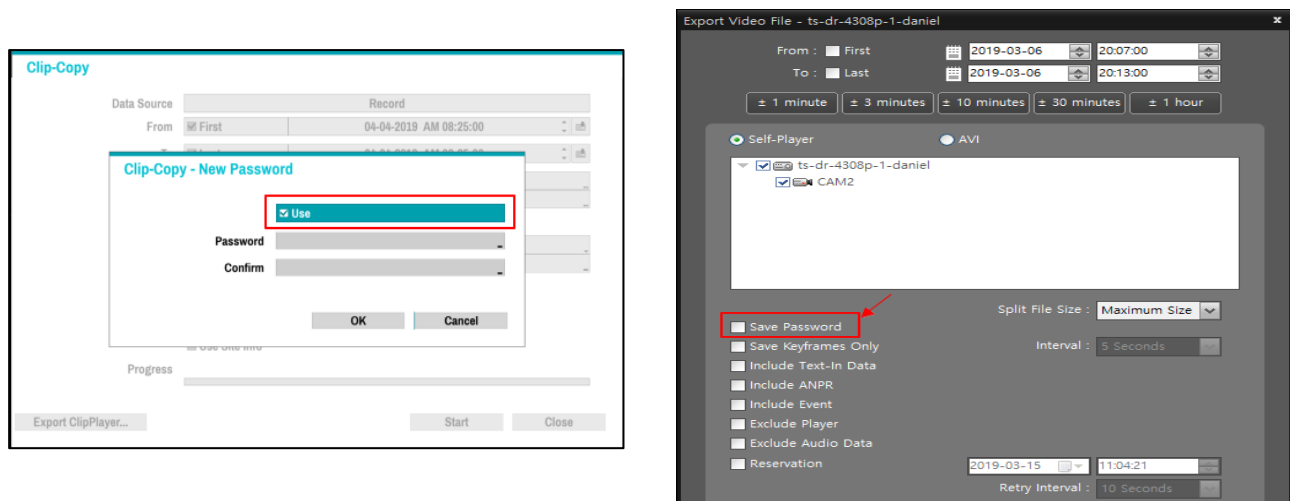
These measures make it difficult for unauthorized users to access and exploit this important and sensitive information.

3.5 Extracted Data Encryption

For enhanced data security, passwords can be set on clip and log data extracted from devices. If a password is set, all extracted data is encrypted using the specified encryption algorithm to prevent reading the extracted data without the password.

3.5.1 Clip data encryption with password

Clip data can be encrypted with a password using the 'Search > Clip-Copy > New Password' option on NVRs, the 'Search > Export > Clip-Copy > Password' option on TVRs, or the 'Export Video File > Save Password' option on IDIS Center or IDIS Solution Suite as shown in Figure 3.5.1.



(a) IDIS NVR and TVR

(b) IDIS Center and IDIS Solution Suite

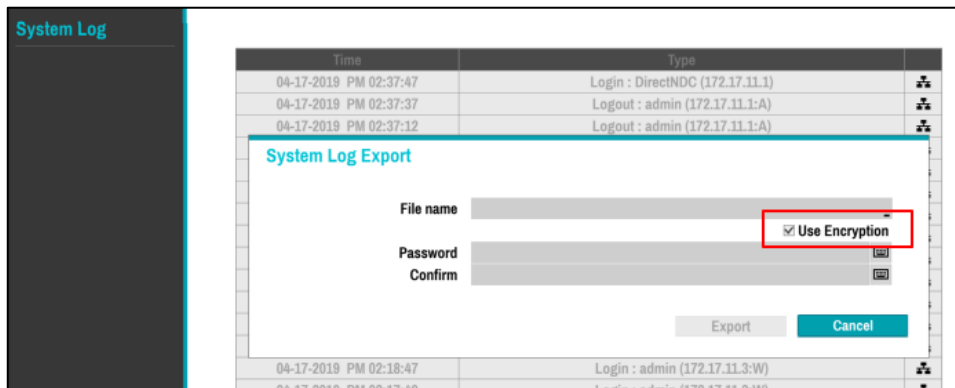
Figure 3.5.1. Clip data encryption with password

The data recorded on a SD card in an IP camera can be extracted to an encrypted clip file using IDIS Center or IDIS Solution Suite.

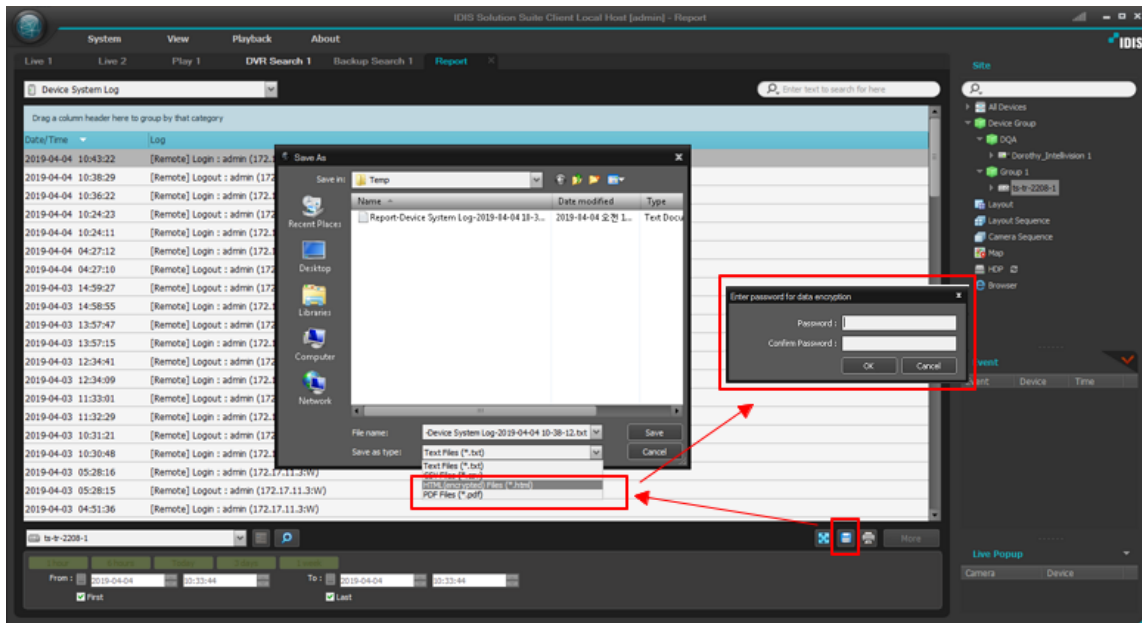
3.5.2 Log data encryption with password

System log data can be encrypted with a password using the ‘System > General > Show System Log...> Export > Use Encryption’ option on NVRs.

Various log data such as system, event, and service logs can be encrypted with a password using the ‘Report > Save As > HTML (encrypted) Files or PDF Files’ option on IDIS Center or IDIS Solution Suite as shown in Figure 3.5.2.



(a) IDIS NVR



(b) IDIS Center and IDIS Solution Suite

Figure 3.5.2. Log data encryption with password

3.6 Secure Data Protection in IDIS Devices

IDIS devices adopt AES-256 encryption, a globally recognized encryption standard, to secure sensitive data both in storage and during transmission.

AES-256 is applied to protect critical information such as device certificates, private keys, user credentials, and recorded data, ensuring confidentiality and resilience against unauthorized access.

AES-256, standardized by NIST (National Institute of Standards and Technology), is widely used in government and enterprise environments, and ensures IDIS devices meet the highest level of data security compliance.

By implementing AES-256 encryption, IDIS guarantees that all sensitive information remains secure, providing customers with trusted protection against modern cyber threats.

3.7 Implementation of a Secure Element for Secure Storage

To maximize the reliability of the video surveillance system and to protect sensitive data within the device safely against unauthorized access and external leaks, IDIS cameras feature a dedicated TPM (Trusted Platform Module) certified with **FIPS 140-3 Level 3**, providing robust secure storage functionality.

3.7.1 Overview of the FIPS 140-3

FIPS 140-3 is a global standard that evaluates the safety and reliability of cryptographic modules, such as secure storage. Compared to its predecessor, security requirements have been significantly enhanced across all domains.

- **Alignment with ISO/IEC Standards:** It has been consolidated based on the ISO/IEC 19790 (Security Requirements) and ISO/IEC 24759 (Test Requirements) standards, strengthening global compliance.
- **Hardware-Centric Integrity Verification:** When verifying software and firmware integrity, whereas Level 2 permits MAC-based verification, Level 3 strictly mandates digital signature-based integrity verification to achieve a higher level of security.
- **Self-Tests:** The module must perform pre-operational self-tests before initialization and conditional self-tests when executing specific functions.
- **Life-Cycle Assurance:** Stringent security requirements are applied to cover the entire life cycle of the cryptographic module, spanning from design, development, and deployment to retirement.

3.7.2 Comparison of FIPS 140-3 Security Levels and IDIS Selection Criteria

FIPS 140-3 is classified into four distinct security levels. IDIS provides a differentiated level of security by adopting a **Level 3** certified TPM, engineered to defend against highly sophisticated physical and non-intrusive attacks.

Security Level	Key Requirements & Features	IDIS Adoption Status
Level 1	Requires basic cryptography and key management functionality. (Suitable for software-only modules.)	-
Level 2	Introduces role-based authentication and tamper-evident physical security (e.g., locks, tamper-evident seals).	-
Level 3	Identity-based authentication, tamper-resistant physical protection against intrusion attempts, and safeguards against environmental attacks (e.g., temperature/voltage fluctuations).	Officially Adopted
Level 4	Active tamper detection and response, multi-factor authentication, and immediate zeroization (deletion) of sensitive data upon breach detection.	-

[Key Security Benefits of Level 3] The Level 3 certified TPM adopted by IDIS ensures enhanced security compared to Level 2 across all domains, including roles/services/authentication, software/firmware security, physical security, non-intrusive security, security parameter management, and life-cycle assurance.

3.7.3 Data Protection Mechanisms and Asset Classification

As a responsible manufacturer, IDIS proactively identifies and securely manages sensitive data requiring protection—such as cryptographic keys and user-defined passwords—without introducing unnecessary complexity or inconvenience to the user.

All sensitive data is encrypted while stored on the device (**Data-at-Rest**). The device-unique symmetric keys used for this encryption are securely protected inside the **FIPS 140-3 Level 3 certified Secure Element (TPM)**. Consequently, the probability of key exposure is extremely low. Furthermore, even in the rare event of a leak on a single device, the system architecture ensures **isolation**, strictly limiting the impact to that specific device only.

Asset Classification: Sensitive Data Requiring Protection

Category	Detailed Item & Usage
User-defined passwords	<ul style="list-style-type: none"> • Device access and login authentication • Access credentials for SMTP / FTP / SIP servers
User-defined cryptographic keys	<ul style="list-style-type: none"> • Private keys and certificates for 802.1X network access • CA certificates for verifying the authenticity of 802.1X authentication servers
Manufacturer-defined cryptographic keys	<ul style="list-style-type: none"> • Private keys and certificates for HTTPS/TLS and device authentication • CA certificates for verifying the authenticity of mutual authentication • Secret keys for system backup and restoration processes

4 Transmission Security Features

4.1 Staged SSL/TLS including Intelligent TLS

4.1.1 Introduction

SSL (Secured Socket Layer) and TLS (Transport Layer Security) help prevent sniffing, modification, and destruction of data as it is transmitted between devices across a network.

TLS is more efficient and secure than SSL as it has stronger message authentication, key-material generation, and additional encryption algorithms. For example, TLS supports pre-shared keys, secure remote passwords, elliptical-curve keys, and Kerberos while SSL does not. TLS and SSL are not interoperable, but TLS does offer backward compatibility for older devices still using SSL [2].

IDIS products support various SSL/TLS options including Intelligent TLS technology for providing secure data transmission with reducing the performance degradation according to data encryption and decryption.

Please note that system performance may be reduced when the TLS option is enabled.

4.1.2 SSL/TLS option between IP camera and NVR

Several SSL/TLS options can be selected in the 'Camera > Advanced Setup > SSL' option on IDIS NVR's as shown in Figure 4.1.1.

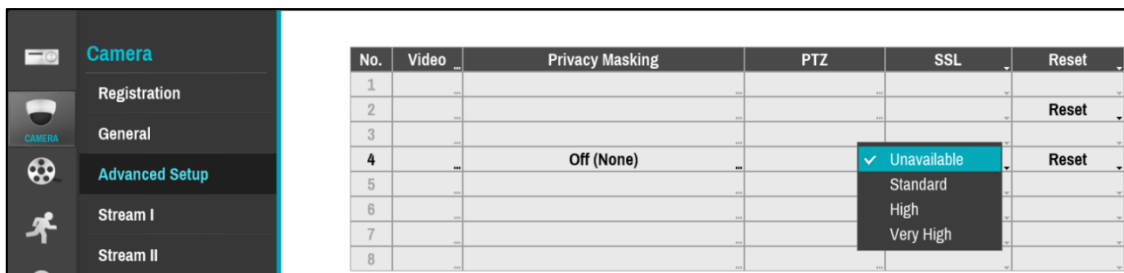


Figure 4.1.1. SSL/TLS options for communication between IP cameras and NVR

Table.4.1.1 shows the behavior of each SSL/TLS option.

Table.4.1.1. Description of SSL/TLS options between IP cameras and NVR

Option	Operation
Unavailable	Disable SSL/TLS encryption (default)
Standard	Encrypt non-multimedia data
High	Encrypt non-multimedia data and only some areas of the multimedia data such as audio and video data
Very High	Encrypt all data including multimedia data

4.1.3 SSL/TLS options between IP cameras and remote client software

The SSL/TLS option can be selected from the 'Network > Security > SSL' option in each IP camera's setup menu as shown in Figure 4.1.2.

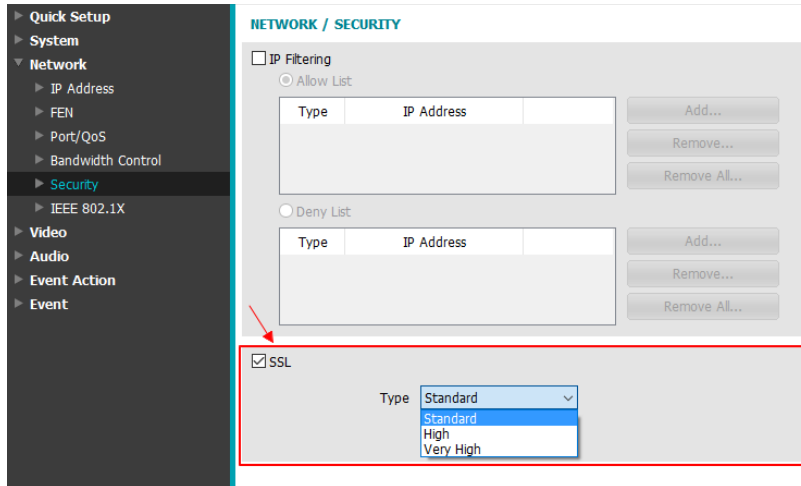


Figure 4.1.2. SSL/TLS options for communication between IP cameras and remote client software

4.1.4 SSL/TLS option between NVR/TVR (HD-TVI DVR) and remote client software

The SSL/TLS option can be selected from 'Network > General > Enable SSL for Transferring Data' in NVR's setup as shown in Figure 4.1.3. This option can be selected from 'General > Network > Enable SSL for Transferring Data' on TVR's setup as shown in Figure 4.1.4.

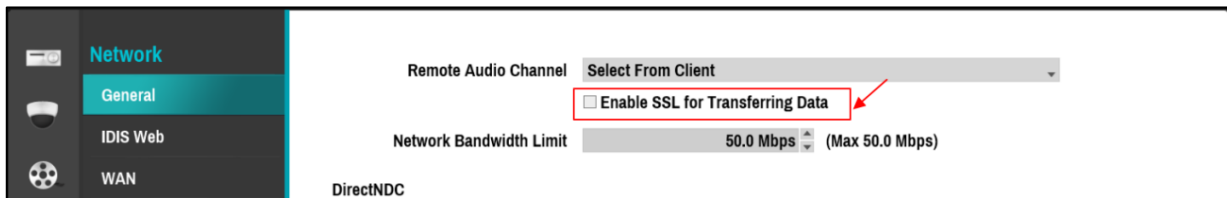


Figure 4.1.3. SSL/TLS option for communication with remote client software on NVRs

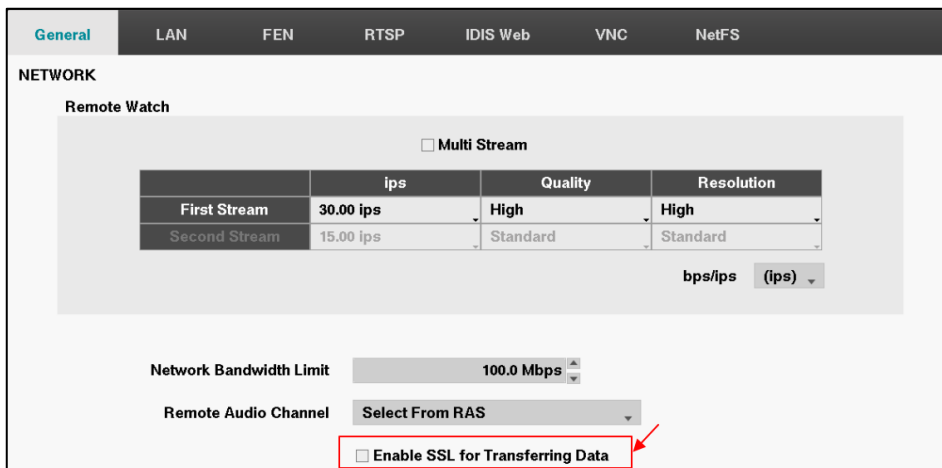


Figure 4.1.4. SSL/TLS option for communication with remote client software on TVRs

Table.4.1.3 shows the behavior of each SSL/TLS option.

Table.4.1.3. Description of SSL/TLS options between NVRs and remote client software

Option	Operation
Uncheck	Disable SSL/TLS encryption (default)
Check	Encrypt non-multimedia data

4.1.5 SSL/TLS option between ISS (IDIS Solution Suite) Service and ISS Client

The SSL/TLS option can be selected from 'System Setup > SSL > SSL Setup > Use SSL' on ISS System Setup as shown in Figure 4.1.5.

Table.4.1.5 shows the behavior of each SSL/TLS option. Please note that the performance degradation rate may differ depending on the network configuration and the performance of the hardware that ISS Service and ISS Client are installed on.

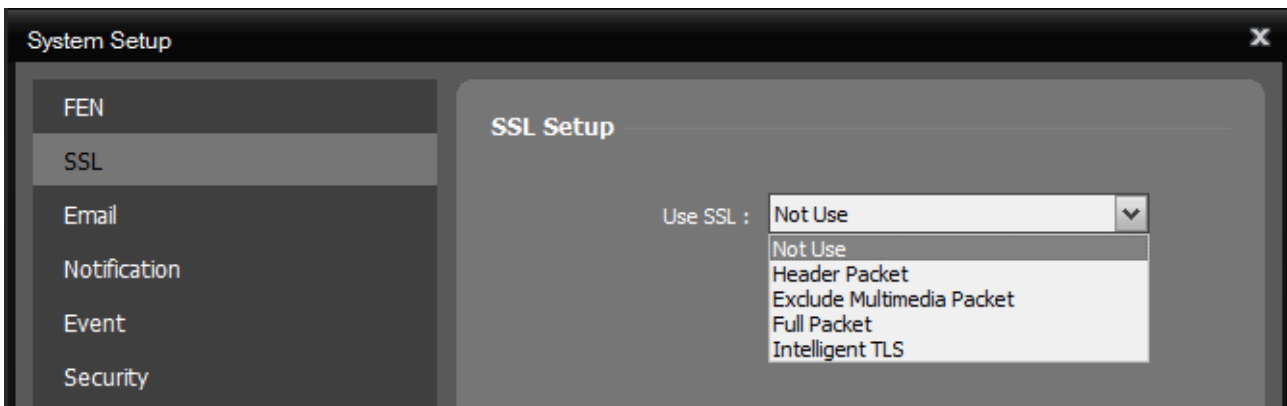


Figure 4.1.5. SSL/TLS options for communication between ISS service and ISS client on ISS system

Table.4.1.5. Description of SSL/TLS option between ISS service and ISS client

Option	Operation
Not Use	Disable SSL/TLS encryption (default)
Header Packet	Encrypt network packet header only
Exclude Multimedia Packet	Encrypt non-multimedia data
Full Packet	Encrypt all data including multimedia data
Intelligent TLS	Encrypt non-multimedia data and only some areas of the multimedia data such as audio and video data This option behaves similarly to the 'High' option of SSL/TLS between IP cameras and NVR, but with an enhanced security algorithm.

The SSL/TLS operation between IDIS devices, ISS streaming service, and ISS client will be different depending on whether or not ISS streaming service is activated, as shown in Figure 4.1.6.

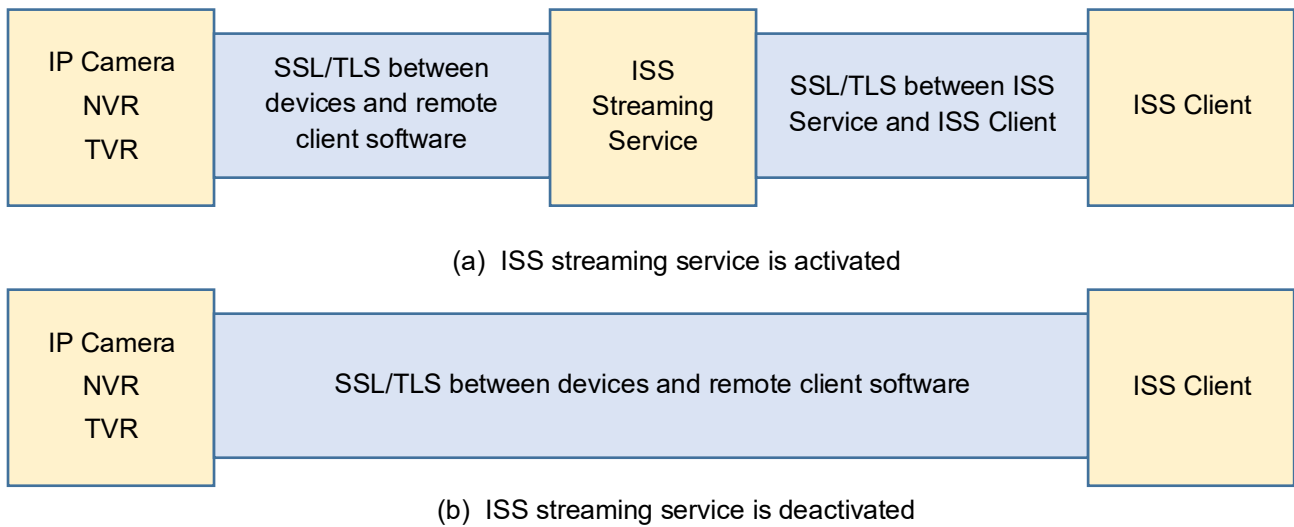


Figure 4.1.6. SSL/TLS operation between IDIS devices and ISS client

4.2 FEN (For Every Network) Security

FEN service is an automated network configuration service which simplifies installation of networked surveillance systems. FEN enables the user to setup and configure surveillance systems without needing a professional knowledge of the routers and NAT devices on the network.

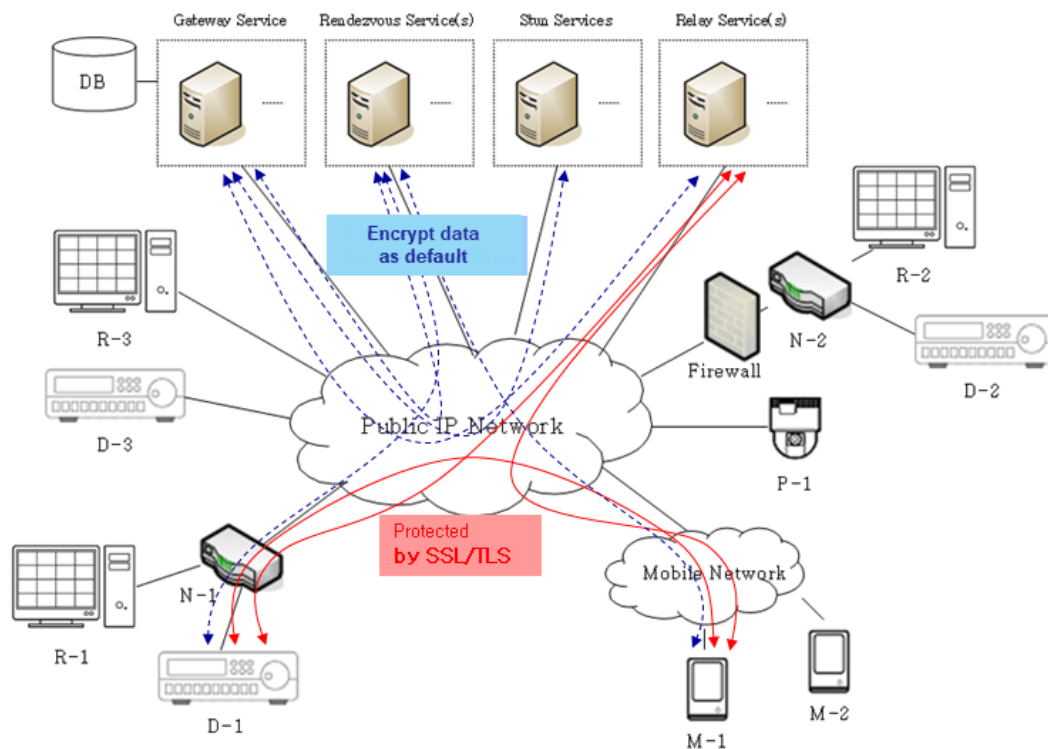


Figure 4.2.1. Secured data communication on FEN service

FEN service utilizes two methods to secure data communication between devices, clients, and other FEN services, preventing unauthorized users from accessing IDIS network devices on public networks as shown in Figure 4.2.1.

The first method is the data encryption which secures data communication between services, or between services and devices/clients. This data encryption is always enabled and cannot be shut off.

The second method is SSL/TLS which secures data communication between devices and clients, or between the relay service and devices/clients. SSL/TLS protection is optional and is applied when the SSL/TLS option of the device is activated.

4.3 IDIS Web Server

Many network security issues have arisen from vulnerabilities in common web servers such as Apache web server [3].

Most of the network service modules in IDIS products are proprietary, as is the case for the HTTP server and client modules used in most of our products, designed to protect our products from these types of vulnerabilities.

4.3.1 IDIS Web Server on IP camera

The IDIS Web Server is supported on all IDIS IP cameras and can be enabled from 'Network > Port/QoS > IDIS Web' on the IP camera setup screens as shown in Figure 4.3.1. The default port is 80 but can be changed.

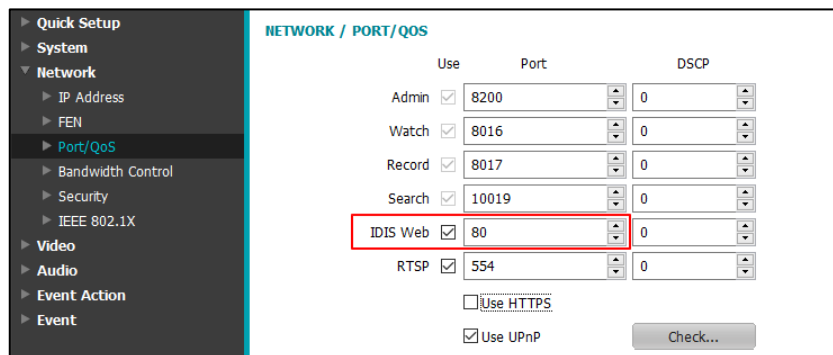


Figure 4.3.1. HTTP option of IDIS Web Server on IP camera setup screen

For additional security, SSL encryption of IDIS Web Server traffic can be enabled by clicking the "Use HTTPS" option as shown in Figure 4.3.2. The default port is 443 but can be changed.

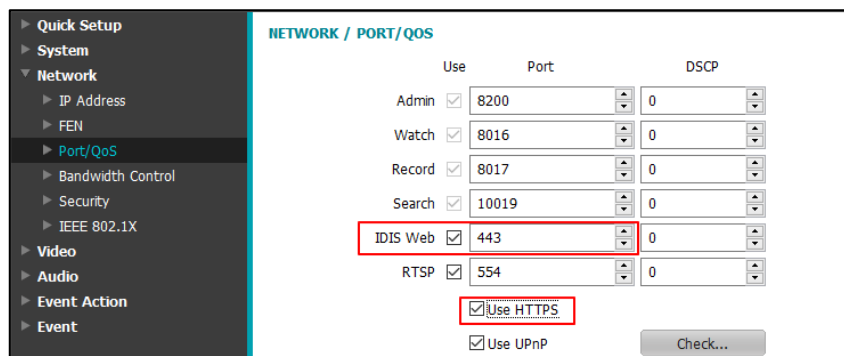


Figure 4.3.2. HTTPS option of IDIS Web Server on IP camera setup screen

4.3.2 IDIS Web Server on NVR and TVR

The IDIS Web Server, a secure proprietary web server, is supported on IDIS NVRs and TVRs as well as conventional DVRs built since 2012.

The IDIS Web Server can be enabled from 'Network > IDIS Web' on the NVR and TVR setup screens as shown in Figure 4.3.3. The default port is 12088 but can be changed.



Figure 4.3.3. HTTP option of IDIS Web Server setup on NVR or TVR

For additional safety, the IDIS Web Server on H.265 NVRs was internally verified using the PCI (Payment Card Interface) Compliance evaluation test, the standard's requirement for maintaining secure web applications [4].

The IDIS Web Server on H.265 NVRs can also provide secure data communication by issuing its own root certificate authority (Root CA) and host certificate authority (Host CA) as shown in Figure 4.3.5.



Figure 4.3.4. HTTPS (SSL) option of IDIS Web Server setup on NVR

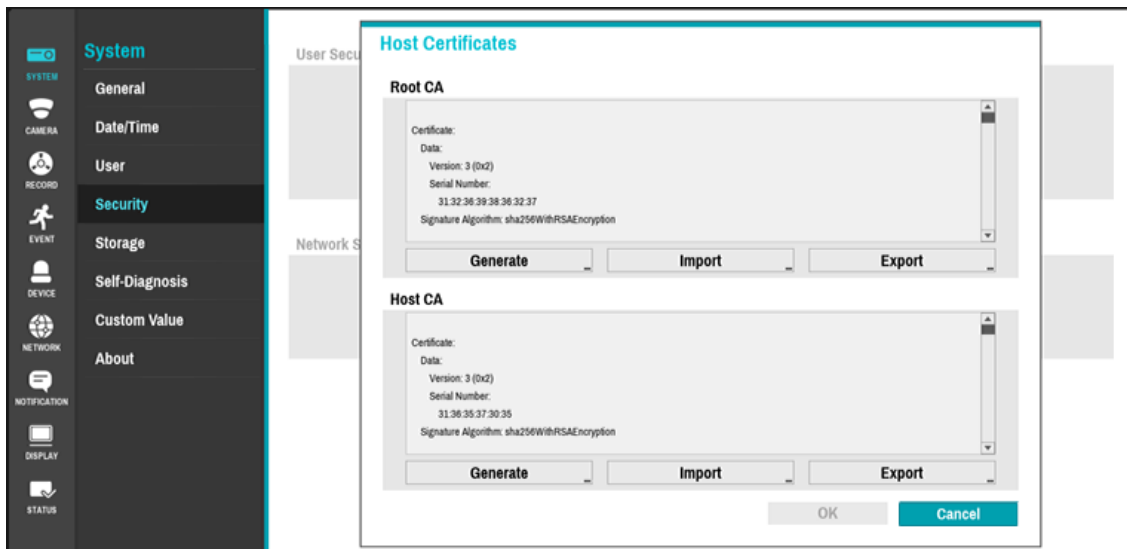


Figure 4.3.5. Root and host certificates setup on NVR

4.3.3 IDIS Web screen on web browser

The IDIS Web Server is enabled, IDIS NVRs, TVRs, and IP cameras can be accessed via a web browser (Internet Explorer pictured) as shown in Figure 4.3.6.

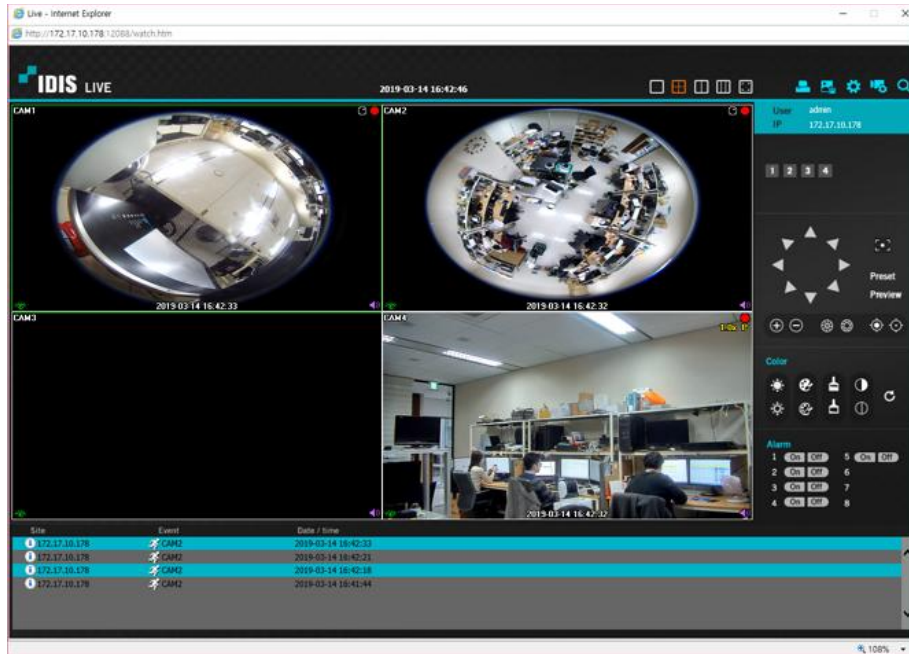


Figure 4.3.6. Live monitoring screen on IDIS Web

4.3.4 IDIS Web Server on IDIS Solution Suite

IDIS Web Server has been supported on IDIS Solution Suite since version 3.1.0. Before that, Apache was used for a short period as shown in Table 4.3.1.

Table.4.3.1. Type of web server per IDIS Solution Suite version

IDIS Solution Suite version	Web Server
3.1.0 or greater	IDIS own webserver (Proprietary)
2.9.0 ~ 3.0.0	Apache 2.2.25
2.8.2 or less	n/a

4.4 ICM (IDIS Cloud Manager) Security

IDIS IP cameras, HD analog DVRs and NVRs except IR-series can be managed by ICM in the cloud environment. ICM can check the status of multiple devices on intuitive dashboard and setup the recorder and IP cameras remotely on Internet Explorer web browser.

For enhancing cybersecurity in the cloud environment, ICM Server, ICM Client and ICM Device transmit TLS encrypted information and data to each other. Especially, Intelligent TLS, IDIS’s network data encryption technique that reduces performance degradation, can be applied for device control, status and multimedia data transmission between ICM Client and ICM Device.

In addition, the encrypted user and device information are stored to ICM Database for cloud database security.

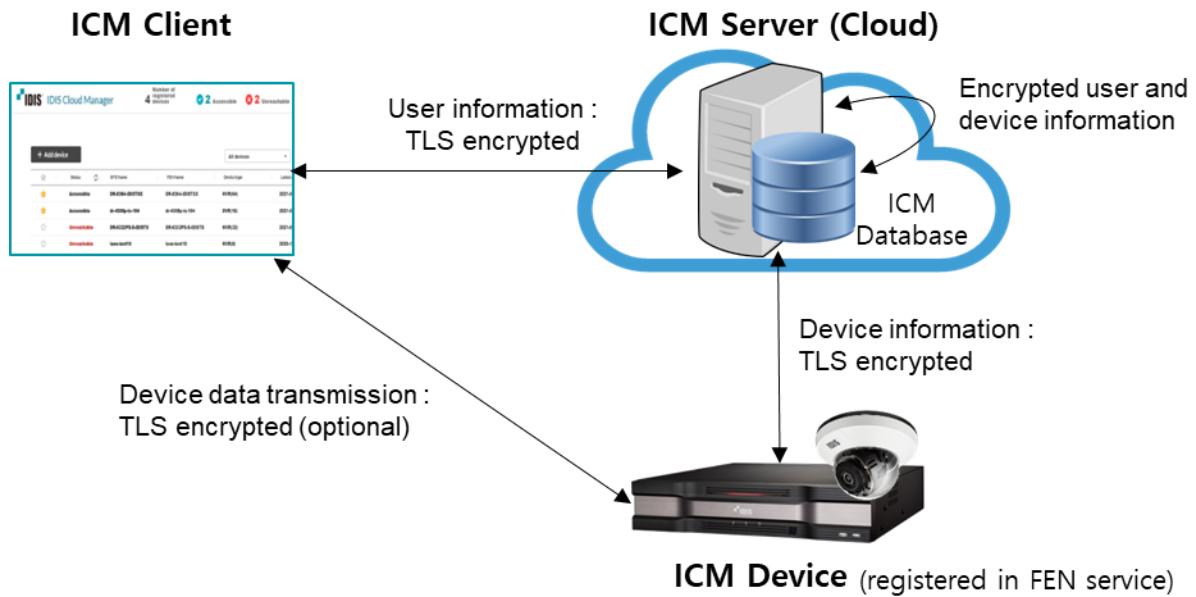


Figure 4.4.1. Information and data security on ICM

4.5 Data Integrity

IDIS devices ensure the integrity of stored and transmitted data by using the SHA-256 hashing algorithm. SHA-256 generates a fixed 256-bit hash value, which changes if the input data is altered, allowing any tampering to be detected.

All critical data, including logs, video files, and configuration information, are stored along with their SHA-256 hash values. During data transmission, the hash values are also verified to confirm integrity. This ensures that the data remains unchanged during storage and transmission and can serve as reliable evidence in the event of a security incident.

5 Access Security Features

5.1 Closed Network with Separate Subnet

A closed network topology provides better performance and higher network security than an open network topology.

Though IDIS DirectIP supports both open and closed network topologies, it is designed to easily create a closed network using separate built-in video input and network ports, keeping the video network separate from the client network, as shown in Figure 5.1.1. By separating the video network from the client network, DirectIP ensures that data is transmitted with more stable frame rates and lower delays between IP cameras and the NVR, while also minimizing data access to unauthorized users.

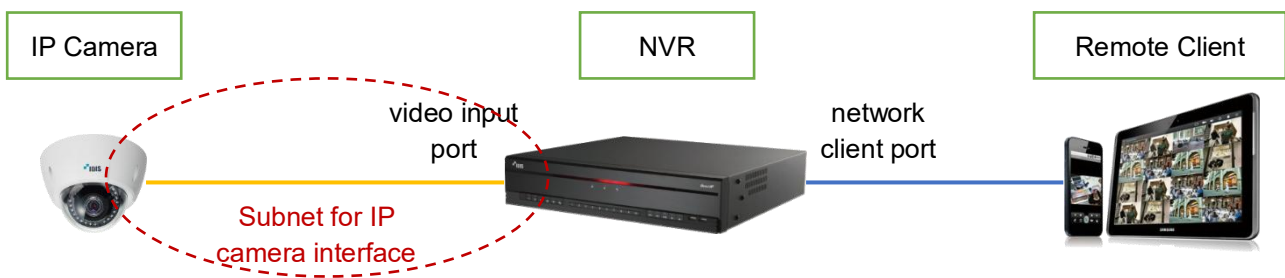


Figure 5.1.1. DirectIP closed network w/ separate video subnet

5.2 Certificate-based Mutual Authentication (DirectIP 2.0)

The beauty of IP networking is that you can access virtually any device on Earth, as long as it is reachable over IP network. However, such power comes with increased security risks, even when the IP network is a private network. For reliable IP-based video surveillance, the user has to be able to trust each IP camera video stream is coming from the intended source (IP camera) and is being recorded to its intended destination (NVR).

Just knowing the IP and MAC addresses and login credential of each IP camera is not sufficient enough to ensure device access security: for example, it does not prevent IP and MAC address spoofing of IP cameras. Furthermore, a single user account and password is sometimes mistakenly reused on multiple devices to simplify installation and management of the network, but this behavior creates additional security vulnerabilities.

DirectIP 2.0 addresses these issues with Certificate-Based Mutual Authentication, allowing users to connect multiple devices quickly and safely using certificates instead of a vulnerable user account and password.

When a DirectIP 2.0 IP camera is paired with a DirectIP 2.0 recorder, they exchange and store their respective certificates, using these certificates to authenticate each other every time they establish a communication session, as shown in Figure 5.2.1. For example, when a DirectIP 2.0 NVR re-establishes a connection with a paired IP camera, authentication involves mutually checking each other's certificates against the stored certificates. If the certificates match, ensuring that both devices are who they say they are, the communication session is established.

Through this operation, the recorder can distinguish whether the correct video is transmitted from the paired camera or whether the incorrect video is transmitted from unauthorized video source.

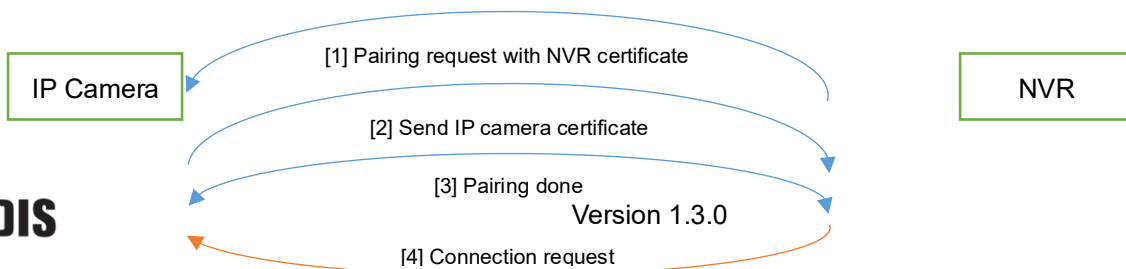




Figure 5.2.1. Certificate-based mutual authentication in DirectIP 2.0

5.3 Password Policy

5.3.1 Password Requirements

- The Passwords for registered users and devices are automatically encrypted using the popular SHA-256 algorithm to prevent them from being decrypted by unauthorized users.
- Complex password Entry even though user passwords are encrypted by a secure hash algorithm.
- User must enter the new password during the initial setup, without creating the new password, the user will not be able to enter camera setup and configure.

5.3.2 Complex Password Entry

Even though user passwords are encrypted by a secure hash algorithm, as mentioned in Chapter 3.3, if a user doesn't change the initial password during installation, a security vulnerability is exposed. It is strongly recommended to change the initial password based on the following guidelines.

- Use 8 ~ 16 characters
- Use at least 3 character types (upper, lower, digit, special) (e.g. jA38v2c4, a1##sb32)
- Don't use the User ID as part of the password
- Don't use sequential numbers (e.g. 123, 321)
- Don't use characters in alphabetical order (e.g. abc, cba, ABC, CBA)
- Don't use repeating characters (e.g. 111, aaa, AAA)

Currently, IDIS H.265 products enforce the above guidelines when passwords are updated.

In addition, all non-discontinued IDIS products are being updated to force user passwords to be updated prior to first use.

5.3.3 Password Management

- Initial Setup: The user (purchaser) must enter the new password during the initial installation of IP CCTV Camera. Failure to setup the initial password will not allow the user to enter the camera system.
- Password Rotation: Due to the functional & operational nature of the device, mandatory rotation is not required. Once the device is handed to users (purchaser), they would follow their password policy, which is out of IDIS scope of password management.

- **Storage:** Passwords are stored using the popular SHA-256 algorithm with salting to prevent unauthorized access.

5.3.4 Access Control

- **User Roles:** Access to the camera system is restricted to authorized users (e.g., administrators and the users with passwords created by administrators).
- **Session Timeout:** Idle sessions will automatically log out after 10 minutes of inactivity.

5.3.5 Enforcement

- **Device Enforcement:** IDIS H.265 products enforce the above guidelines during password creation and updates.

5.4 Backdoor-Free Architecture

A backdoor is a method, often secret, of bypassing normal authentication or encryption in a computer system or embedded devices [5]. A back door often takes the form of a program designed to provide remote support to customers for technical issues, but it can also be used monitor, track, or take over a remote system, a major system vulnerability.

IDIS products are designed without backdoors, such that not even an IDIS developer can access a user's product without the user's explicit approval.

5.5 2FA (Two-Factor Authentication)

In today's online environment, the username and password approach to security is an easy target for cyber criminals [6]. Two-Factor Authentication, also known as 2FA, is a method of confirming a user's identity by utilizing a combination of two different pieces of information.

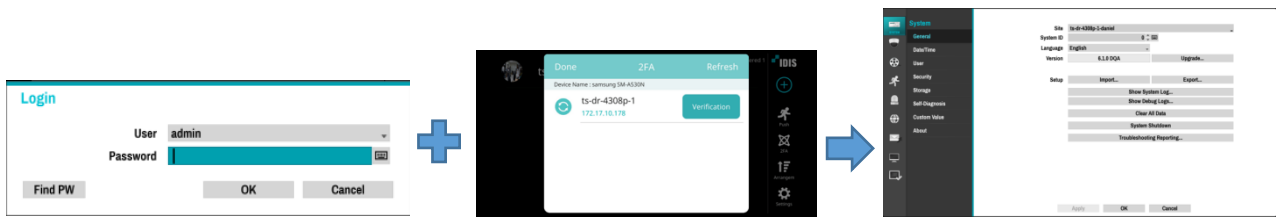
IDIS NVRs support 2FA to prevent the unauthorized altering of device settings and upgrading of the device software, as well as limiting search capabilities.

If 2FA is enabled, a user only gains access to an IDIS NVR after passing the following two authentications as shown in Figure 5.5.1.

First, the username and password must be entered correctly in the login window of NVR.

Second, the VERIFICATION button must be pressed after selecting IDIS NVR on the IDIS Mobile application installed on a mobile phone. The mobile phone must be already registered in IDIS NVR.

IDIS NVRs can register up to 16 mobile devices for 2FA, and the IDIS Mobile application must be running on each mobile device. 2FA can only be enabled and configured by the administrator account.



(a) username and password login (b) device verification on IDIS Mobile (c) control NVR after 2FA

Figure 5.5.1. 2FA operation on IDIS NVR

Please refer to the 'Part 2 – Configuration > Security > User 2FA' chapter in the NVR's operations manual for details on configuring 2FA.

5.6 IP Filtering

IP filtering is a function that can be used to allow or deny access to a device based on the IP address of the incoming connection/device. IP filtering is support on IDIS IP cameras and IDIS Solution Suite.

When IP filtering is enabled, individual IP addresses added to the 'Allow List' or 'Deny List', will be allowed or denied access respectively to the device.

5.6.1 IP Filtering on IP camera

IP filtering is disabled by default but can be enabled from the 'Network > Security > IP Filtering' option in the IP camera setup as shown in Figure 5.6.1.

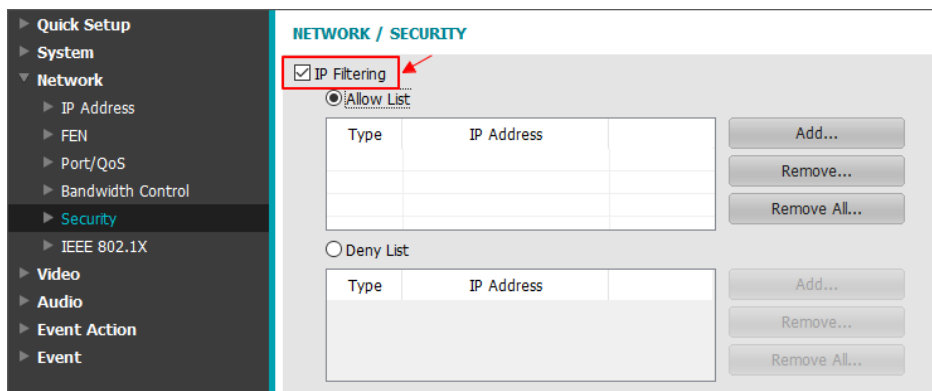


Figure 5.6.1. IP filtering setup on IP cameras

5.6.2 IP Filtering on IDIS Solution Suite



Figure 5.6.2. IP filtering setup on IDIS Solution Suite

IP filtering is disabled by default, but can be enabled from the 'User > Edit User > IP AccessControl' option in the IDIS Solution Suite setup as shown in Figure 5.6.2.

5.7 Firewall

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on a predetermined set of security rules [7]. Both IDIS H.265 NVRs and IDIS Solution Suite support a firewall.

5.7.1 Firewall on NVR

The firewall on IDIS NVRs provides much more functionality than just IP filtering. IDIS H.265 NVRs can accept or reject specific devices based on various parameters such as IPv4, IPv6, MAC, port number, ICMP, etc. Additionally, new firewall rules can be applied to the connected video input devices and remote network sessions at runtime starting with firmware versions 6.1.0 and greater.

The firewall can be enabled and configured at 'Network > Firewall' in the NVR setup screens as shown in Figure 5.7.1.

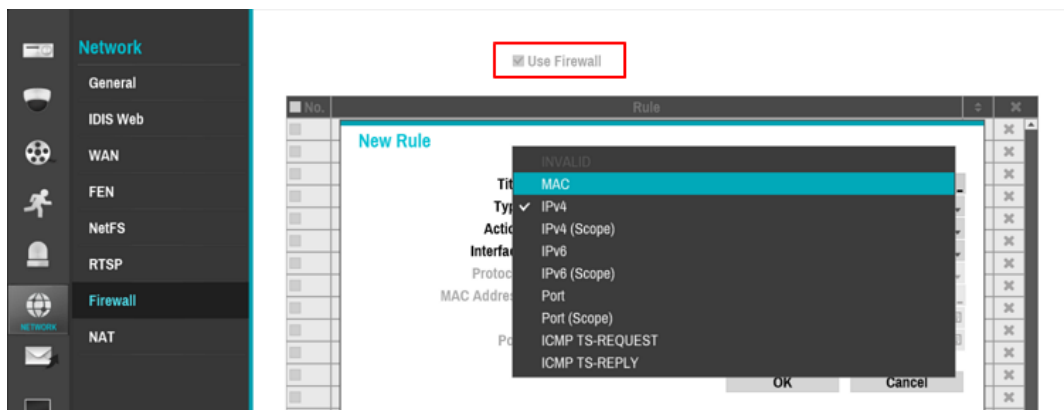


Figure 5.7.1. Firewall setup on IDIS NVR

5.7.2 Firewall on IDIS Solution Suite

IDIS Solution Suite does not have its own firewall, but instead relies on the built-in firewall off the Windows OS, that can be setup and configured using the 'Windows Firewall with Advanced Security' application as shown in Figure 5.7.2.

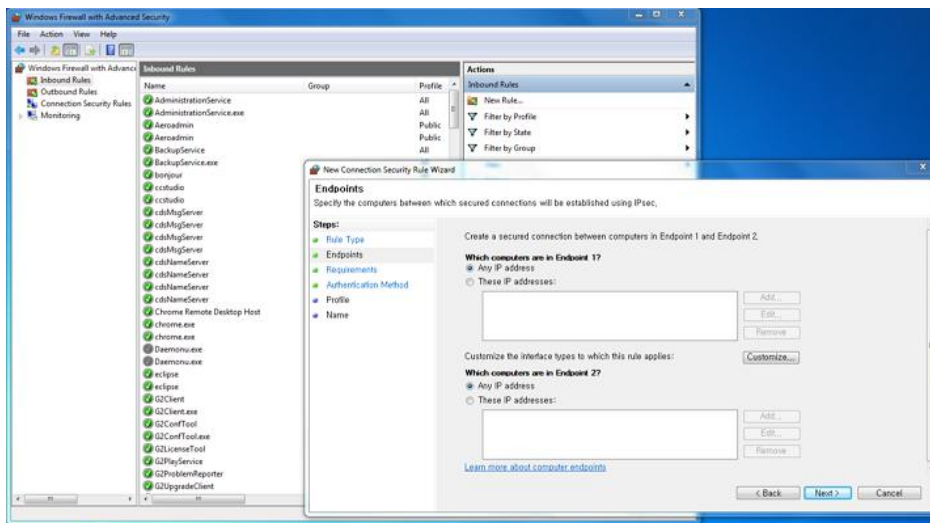


Figure 5.7.2. 'Windows Firewall with Advanced Security' setup on Windows

5.8 IEEE 802.1X Authentication

IEEE 802.1X is an IEEE standard for Port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols and provides an authentication mechanism to devices wishing to connect to a LAN or WAN [8].

IDIS cameras support IEEE 802.1X authentication and can connect with an 802.1X protected network by enabling and configuring the settings under the 'Network > IEEE 802.1X' option of the IP camera setup as shown in Figure 5.8.1.

Please refer to the 'Part 1 – Remote Setup > Network > IEEE 802.1X' section of the operations manual for IDIS IP cameras for more detailed information about IEEE 802.1X setup.

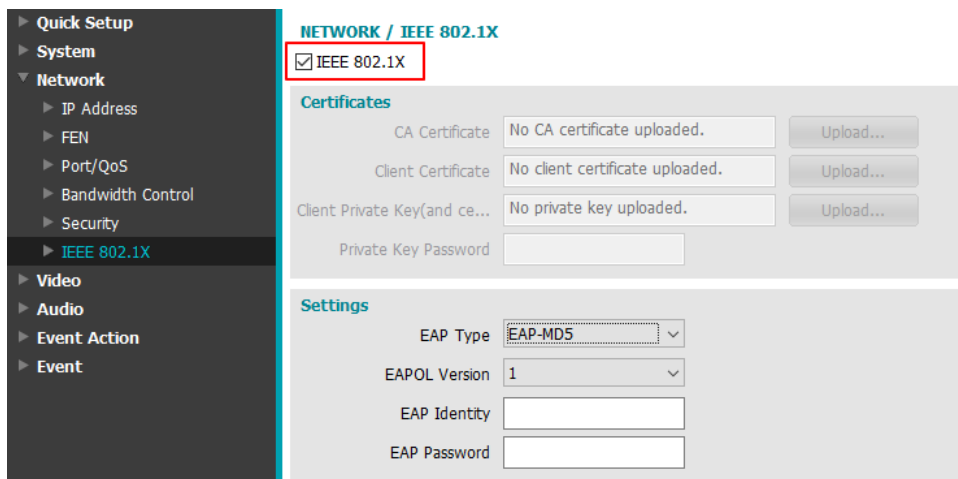


Figure 5.8.1. IEEE 802.1X setup on IP cameras

5.9 Restricted Network Port Access

IDIS hardware-based products and PC-based NVRs run on Linux OS and Windows Embedded OS

respectively, and have had any unnecessary networking ports disabled, such as telnet and samba filesharing, making them more robust against malicious code injections attacks via the network compared to standard Windows OS-based servers and workstations.

Additionally, the default port numbers of installed and supported services (such as HTTP, RTP/RTSP, VNC, FTP, etc.) can be changed in the devices setup screens or completely disabled if desired.

Before making changes or disabling specific ports, please contact us for detailed information about the ports/services needed for your specific application by referring to the 'Contact Us' section at the end of this document.

5.10 IDIS Inbound Essential Network Port List

This is a description of the TCP and UDP ports that are open (LISTEN) for inbound communication on IDIS devices.

Product	Feature	Feature Description	Default Port	Adjustable Port Range	TCP / UDP	Service Mode	Inbound / Outbound
IP camera	HTTP / HTTPS Server	Web service	80 / 443	10 ~ 14000	TCP	Server	Inbound
IP camera	mDNS	mDNS Service	5353	5353	UDP	Server	Inbound
H.265 IP camera	IDIS Protocol (Unified)	Administration, Live monitoring(Audio/Video/PTZ ...), Record, Search and Playback, Network Keyboard (NK-xxxx)	8016	8000 ~ 12000	TCP	Server	Inbound
H.264 IP camera	IDIS Protocol (Admin)	Administration	8200	8000 ~ 12000	TCP	Server	Inbound
H.264 IP camera	IDIS Protocol (Watch)	Live monitoring(Audio/Video/PTZ ...)	8016	8000 ~ 12000	TCP	Server	Inbound
H.264 IP camera	IDIS Protocol (Record)	Record	8017	8000 ~ 12000	TCP	Server	Inbound
H.264 IP camera	IDIS Protocol (Search)	Search and playback	10019	8000 ~ 12000	TCP	Server	Inbound
Standalone NVR	mDNS	mDNS Service	5353	5353	UDP	Client, Server	Both
Standalone NVR	IDIS Protocol (Unified)	Administration, Live monitoring(Audio/Video/PTZ ...), Record, Search and Playback, Network Keyboard (NK-xxxx)	8016	8000 ~ 12000	TCP	Server	Inbound
Standalone NVR	NTP Sever	Network time sync (for time sync. with IP camera)	123	123	UDP	Server	Inbound
Standalone HD DVR	mDNS	mDNS Service	5353	5353	UDP	Server	Inbound
Standalone HD DVR	IDIS Protocol (Unified)	Administration, Live monitoring(Audio/Video/PTZ ...), Record, Search and Playback, Network Keyboard (NK-xxxx)	8016	8000 ~ 12000	TCP	Server	Inbound
Standalone HD DVR	NTP Sever	Network time sync (for time sync. with IP camera)	123	123	UDP	Server	Inbound

5.11 USB Interface and Class Support

IDIS NVRs and IDIS Servers support USB interfaces.

- **HID Class:** Recognizes keyboard and mouse devices
- **CDC Class:** Recognizes serial port devices
- **Mass Storage Class:** Supports saving and reading files such as configuration, firmware upgrades, and logs via USB sticks

No unnecessary USB classes are included.

Note : IDIS products do not have any physically disabled interfaces.

5.12 Access Control for Specific User or User Group

5.12.1 Remote Connection Control on IDIS H.265 NVR

The administrator can set the available access times and camera visibilities on IDIS H.265 NVRs at a remote

site for a specific user group using 'System > User > Group – xxx > Remote Connection Policy' menu on H.265 NVRs as shown in Figure 5.12.1. This feature is useful to prevent users from accessing the device outside the allowed times or viewing the footage of cameras in unauthorized areas.

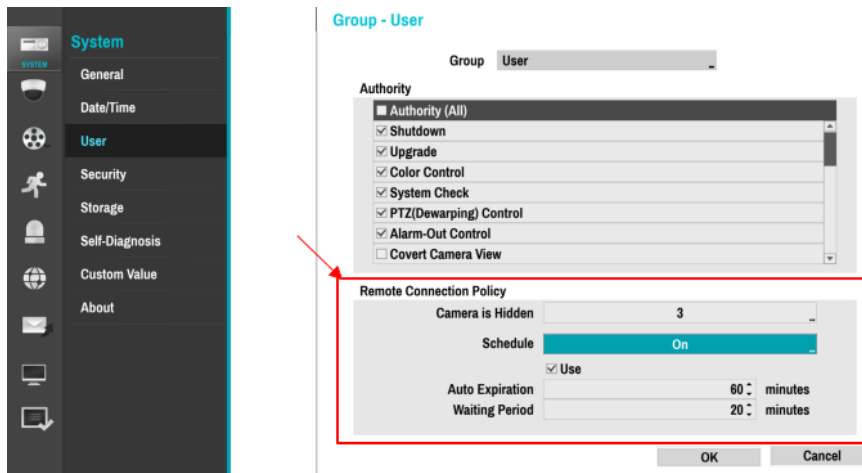


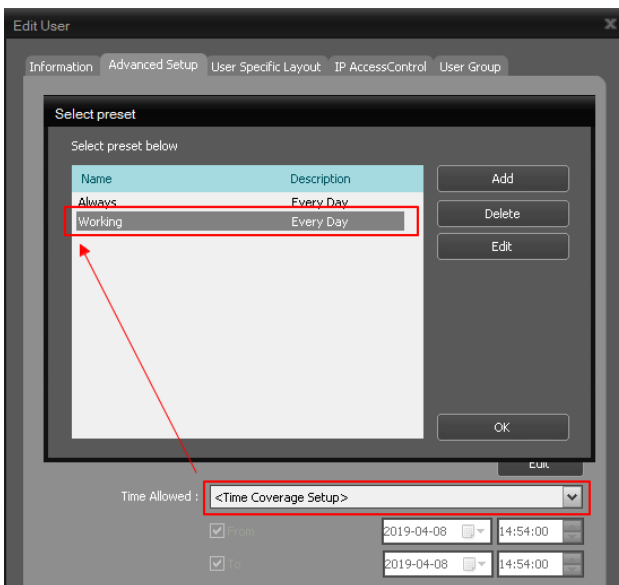
Figure 5.12.1. Remote connection policy setup on H.265 NVR

In addition, the session auto expiration and reconnection waiting period times can be adjusted to disconnect idle users and prevent them from continuously reconnecting.

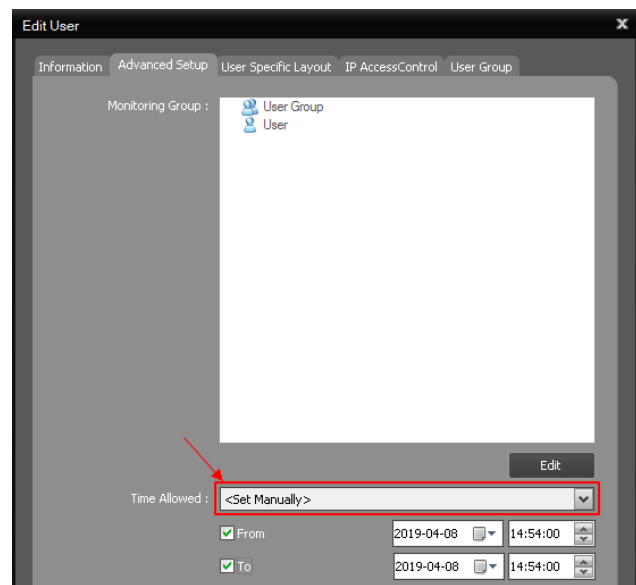
5.12.2 Access Time Restrictions on IDIS Solution Suite

IDIS Solution Suite allows the administrator to set individual access times for each registered user. This feature prevents a specific user from holding device resources and network bandwidth for excessive amounts of time.

The access times of each user on IDIS Solution Suite can be set in the 'Time Coverage Setup' option or 'Set Manually' option as shown in Figure 5.10.1. For example, the administrator can set it so particular users can only access the system during work hours using the 'Time Coverage Setup' option.



(a) 'Time Coverage Setup' option



(b) 'Set Manually' option

Figure 5.10.1. Access time setup for each user on IDIS Solution Suite

5.13 Covert

IDIS recorders and IDIS Solution Suite support the 'Covert' feature that can hide cameras and their associated details from a specific user group. This feature provides system administrators with the ability to prevent certain users from monitoring, reviewing, or searching footage and information from specific cameras, potentially in secure or highly sensitive areas.

The administrator can assign one of the following covert options for the specific user group.

Covert 1: Hides images from the camera, but shows the camera title and status icons.

Covert 2: Hides images from the camera, as well as the camera title and status icons.

5.13.1 Covert setup on IDIS NVR or TVR

For the covert option to work, the administrator must first disable the 'System > User > Covert Camera View' option under the setup section of the NVR or TVR for the specific user group as shown in Figure 5.11.1.

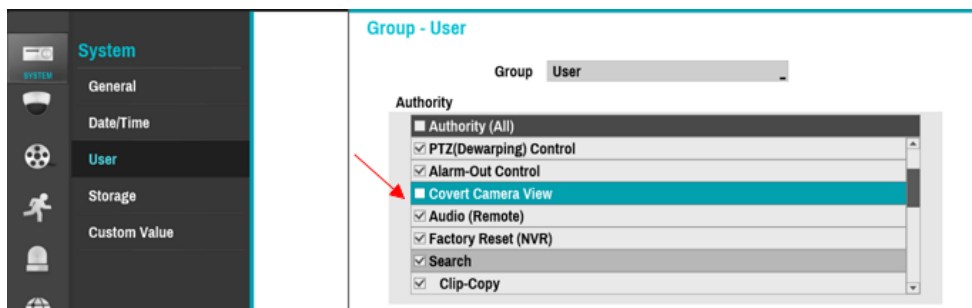


Figure 5.11.1. 'Covert Camera View' option on user authority of NVR or TVR

If 'Covert Camera View' is enabled, users in the group will be able to view a cameras footage and details regardless of its individual 'Covert' setting.

Enable the covert option for each desired camera from the 'Camera > General > Covert' area of the setup section of the NVR or TVR as shown in Figure 5.11.2.

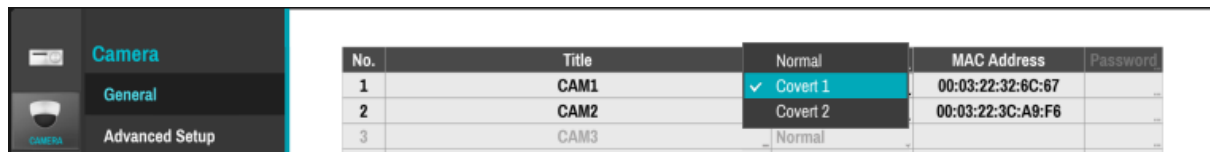
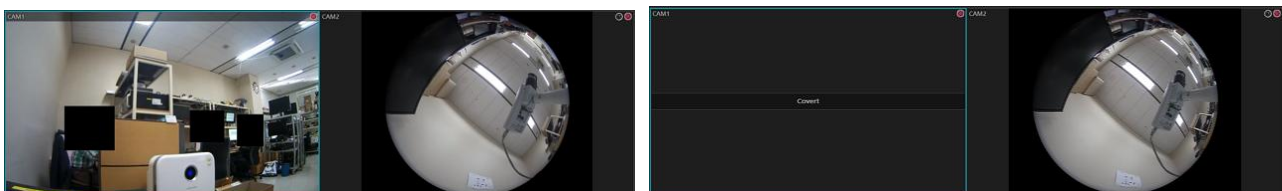


Figure 5.11.2. 'Covert' option for each camera on TVR or NVR

When restricted users access the live monitoring mode, they can't see the camera feed of cameras where the 'Covert' option was activated as shown in Figure 5.11.3.

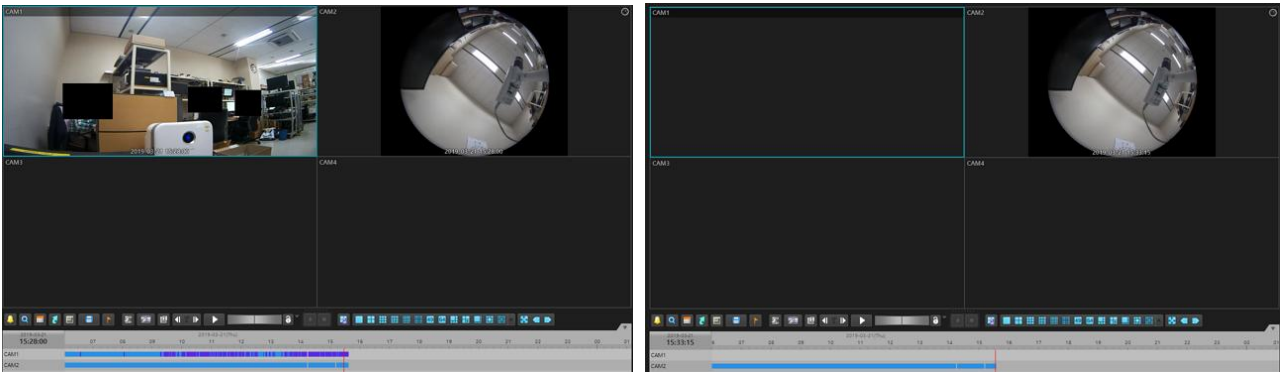


(a) Normal live view of cameras

(b) 'Covert 1' applied to 1st camera

Figure 5.11.3. Covert image on live monitoring screen of NVR or TVR

Similarly, when restricted users access playback mode, they can't see the recorded information and footage of cameras where the 'Covert' option was activated as shown in Figure 5.11.4.



(a) Normal playback of cameras

(b) 'Covert 1' applied to 1st camera

Figure 5.11.4. Covert image on playback screen of NVR or TVR

5.13.2 Device Access Authority setup on IDIS Solution Suite

IDIS Solution Suite doesn't have the same 'Covert' option as IDIS NVRs and TVRs, but similar functionality can be obtained by using the "Device Access Authority" option.

Access to specific cameras can be turned on and off for a user group by going to the 'User > Edit User Group > Device Access Authority' as shown in Figure 5.11.5, producing similar results to the 'Covert' option.

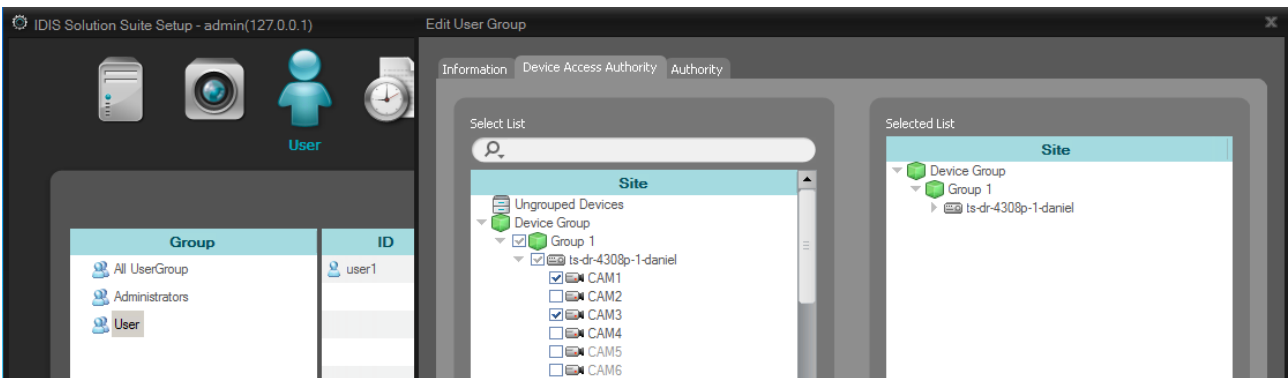


Figure 5.11.5. 'Device Access Authority' setup on IDIS Solution Suite

6 Personal Information Security Features

The need for personal information security, such as protecting a person's identity, has been increasing with the new application of international legislation and protocols to the ever-changing technology landscape. Generally, the situation can be summed up by the following excerpt from the European Convention on Human Rights (ECHR) [9].

"Everyone has the right to respect for his private and family life, his home and his correspondence".

6.1 Privacy Masking

Privacy masking is a feature found in many video surveillance products, used to protect personal privacy by concealing parts of the image with a masked area [10][11].

IDIS supports two types of privacy masking, static and dynamic, for enhanced personal information security. Static privacy masking is supported for live, recorded, and clipped video while dynamic privacy masking is supported for clipped video. A static privacy mask is created by defining a fixed area in the image that will be masked, regardless of the movement in the image. Dynamic privacy masking allows an operator to define an area of masking that can move with the object being masked.

Privacy masking can be applied differently depending on the type of video as shown in Table.6.1.1.

Table.6.1.1. IDIS privacy masking features

Operation	Apply privacy masking		
	Static Privacy Masking for Live Monitoring and Recording	Static Privacy Masking for Video Clip	Dynamic Privacy Masking for Video Clip
Live Monitoring Video	O	X	X
Recorded Video	O	X	X
Original Video Clip	O	O	X ⁽¹⁾
Copied Video Clip	O	O	O

⁽¹⁾ The original video clip can be overwritten instead of creating new video clip after applying dynamic privacy masking

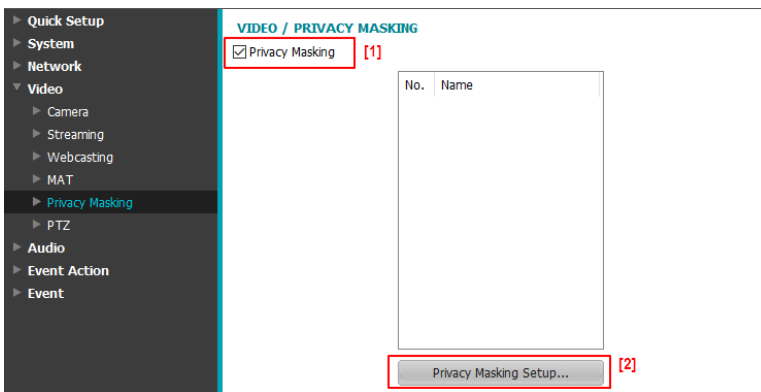
6.1.1 Static Privacy Masking for Live Monitoring and Recording

6.1.1.1 Static privacy masking on IP camera

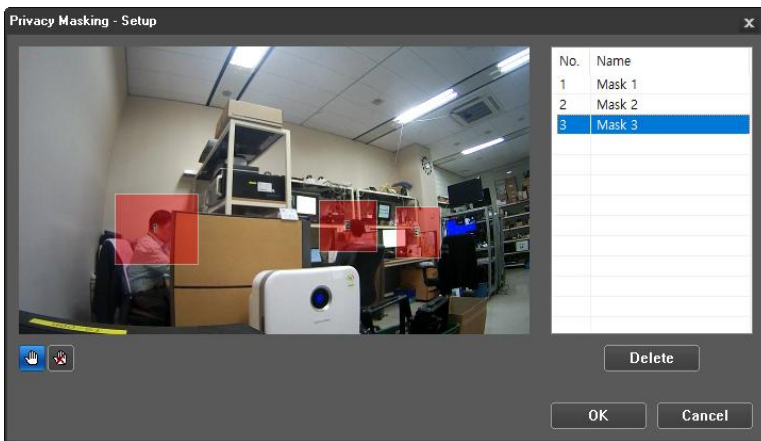
Privacy masking is initially disabled and can be enabled with the 'Video > Privacy Masking > IP Filtering' option in the NVR setup as shown in Figure 6.1.1.

6.1.1.2 Static privacy masking on IDIS NVR or TVR

Privacy masking is initially disabled and can be enabled with the 'Camera > Advanced Setup > Privacy Masking' option for each IP camera in the NVR setup as shown in Figure 6.1.2. After enabling 'Privacy Masking', setting the privacy mask for the camera is the same as in Figure 6.1.1.



(a) Activate 'Privacy Masking'



(b) Specify 'Privacy Masking' area

Figure 6.1.1. Static privacy masking setup on IP camera

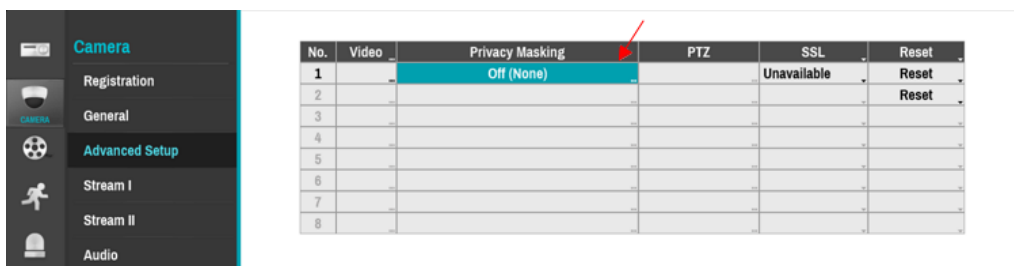


Figure 6.1.2. Static privacy masking setup on NVR

Privacy masking can also be enabled from the 'Camera > Privacy Masking' option for each HD analog camera in the TVR setup as shown in Figure 6.1.3. After enabling 'Privacy Masking' for a camera, setting the mask is similar to the process pictured in Figure 6.1.1 even though the setup GUI of IDIS TVRs is a little different from that of IP products.

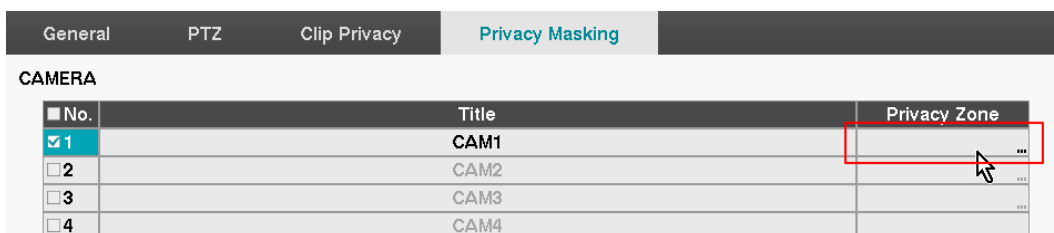


Figure 6.1.3. Static privacy masking setup on TVR

6.1.1.3 Static privacy masking on remote client software

Privacy masking can also be setup using remote client software such as IDIS Solution Suite and IDIS Center. Using the ‘Remote Setup Device...’ menu as shown in Figure 6.1.4, privacy masking options of cameras, NVRs, and TVRs can be configured.

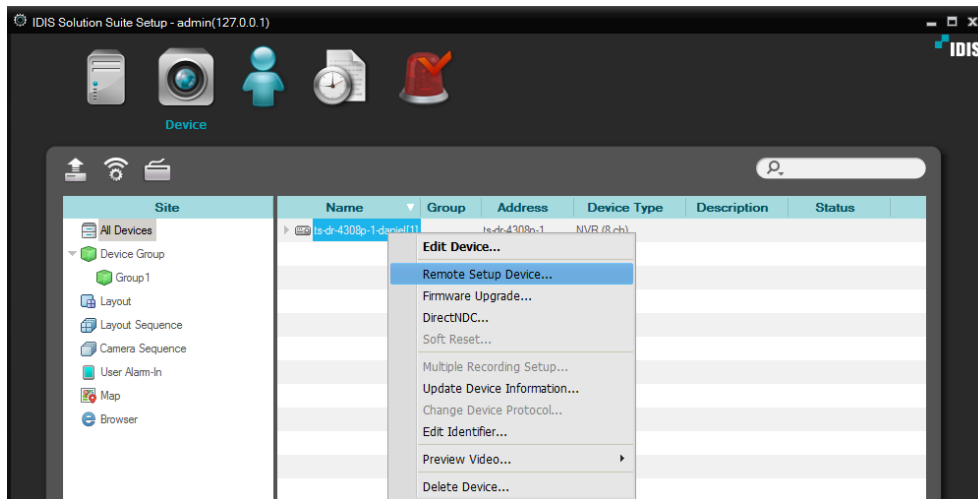
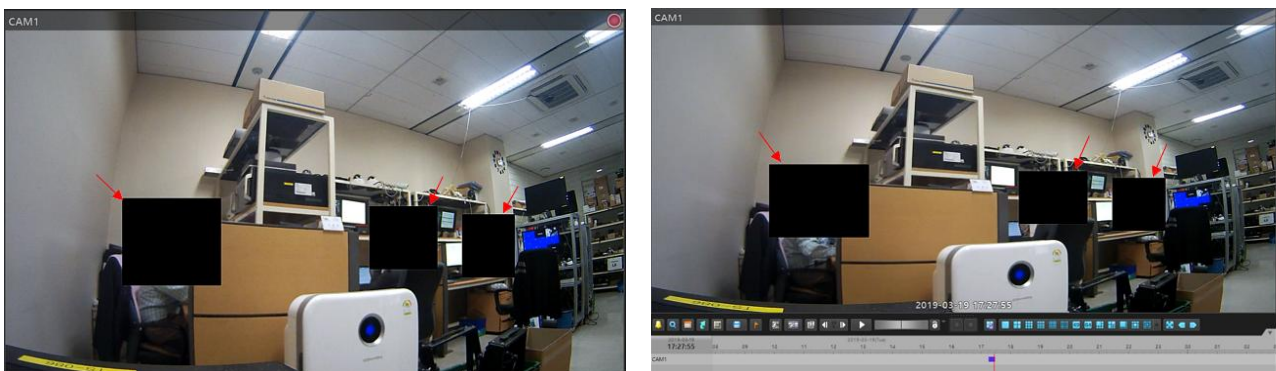


Figure 6.1.4. ‘Remote Setup Device...’ menu in IDIS Solution Suite

6.1.1.4 Live monitoring and recorded video with static privacy masking

When privacy masking is applied, the privacy masked area will not be visible in live monitoring or recorded video as shown in Figure 6.1.5.



(a) Live monitoring video

(b) Recorded video

Figure 6.1.5. Live monitoring and recorded video with static privacy masking

6.1.2 Static Privacy Masking of Video Clips

Using IDIS Solution Suite, static privacy masking can be applied to video clips extracted from recorded data even if there is no privacy masking on the recorded data.

The privacy masking area can be set in IDIS Solution Suite using the ‘Device > Edit Device > Clip Privacy Zone’ menu as shown in Figure 6.1.6.

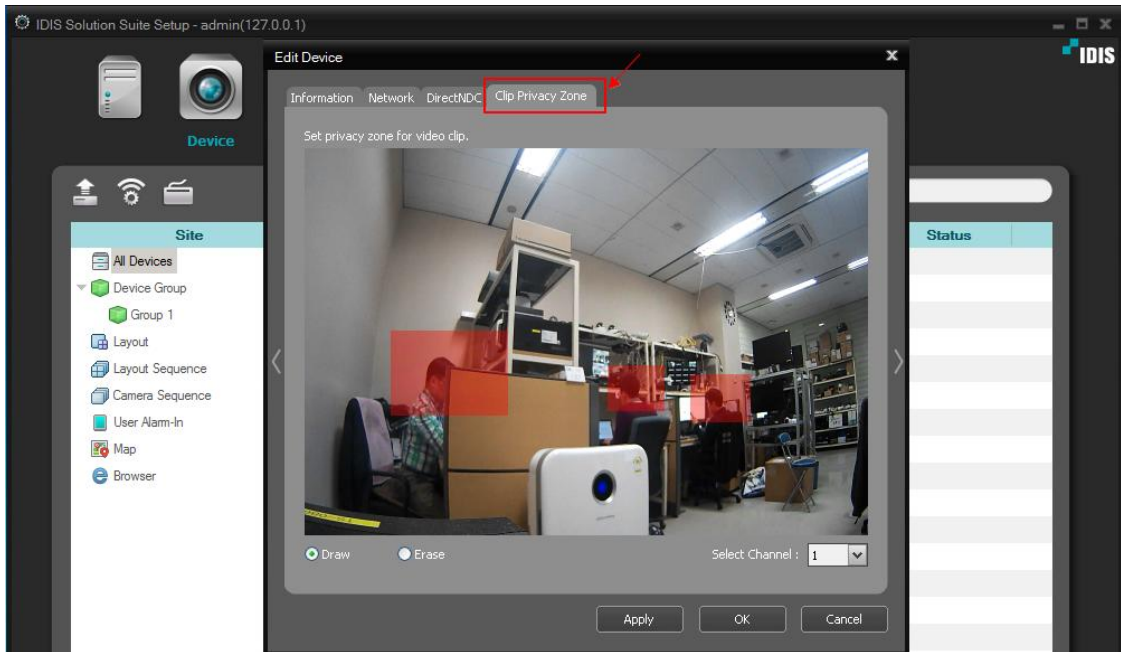


Figure 6.1.6. Static privacy masking for video clip in IDIS Solution Suite

6.1.3 IDPM (IDIS Dynamic Privacy Masking) Compact for Video Clip

Just like static privacy masking, dynamic privacy masking can be applied to a specific area of an extracted video clip using IDPM Compact software.

IDPM Compact software loads the original video clip, applies the dynamic privacy masking, and then saves the final masked video clip as shown in Figure 6.1.7.



(a) Video clip without privacy masking



(b) Video clip with privacy masking

Figure 6.1.7. Dynamic privacy masking of video clip using IDPM software

IDPM Compact software can apply privacy masking to moving objects, automatically tracking their movement through the image, but can be manually adjusted, if needed.

Please refer to the [IDIS Privacy Masking User Guide Video](https://youtu.be/gNscfDGOszI) (<https://youtu.be/gNscfDGOszI>) for more specific instructions on the usage of IDPM.

6.2 IDIS Vulnerability Management Policy

IDIS adheres to industry best practices in managing and responding to any security vulnerabilities detected in our products. While it is impossible to ensure that our products and services are completely devoid of vulnerabilities - a reality that is not unique to IDIS but common to all software and services - we can assure you that we make a sustained effort at every stage of development to identify and address potential vulnerabilities. This approach significantly reduces the risk associated with deploying our products and services in customer environments.

6.2.1 Response Team

The IDIS Cybersecurity Team(security@idisglobal.com) is a specialized department committed to identifying and addressing any potential security vulnerabilities within IDIS's products. We are dedicated to swift and effective responses in the event of a security vulnerability, which includes comprehensive analysis and the development of countermeasures. Should you encounter any signs of security vulnerability in your product, please do not hesitate to inform us. We assure you that our team is equipped to handle the situation promptly and efficiently.

6.2.2 Response Process

Upon receipt of a security vulnerability report, we immediately assemble our Security Breach Incident Response Team. This team's principal mission is to meticulously dissect the nature and implications of the vulnerability, to devise an effective resolution, and to expediently release the updated, patched firmware on our website with the utmost urgency.

6.2.3 Notice Policy

The firmware that has been patched for vulnerabilities is uploaded to our website alongside the Vulnerability Report. To prevent zero-day attacks, we withhold the details of the vulnerability (including the nature of the vulnerability, information on affected products and firmware versions, risks, and countermeasures) until the patched firmware is released on our website. In order to deter potential mimicry of attacks, we also avoid disclosing specifics such as attack scenarios related to the vulnerabilities. If the vulnerability impacts multiple products, we ensure the simultaneous release of the respective firmware patches.

6.2.4 Report a Vulnerability

If you have discovered a new vulnerability in any of our products or services, we encourage you to submit your discovery to security@idisglobal.com. The IDIS Cybersecurity Team will respond to your vulnerability submission within 7 days and aim to assess your report within the same timeframe.

After thoroughly reviewing the information you provided, if any vulnerabilities are identified, we will contact you individually with details, and you can also track the progress of your report [here](#).

6.2.5 Safe Harbor Declaration

We value responsible disclosure. If you report a vulnerability to us in good faith and comply with our guidelines, IDIS commits not to pursue legal action against you. Your efforts to help improve the security of our products and services will be appreciated and protected under this safe harbor declaration.

6.3 Vulnerability Assessment Principles

IDIS manages potential vulnerabilities in its products and services by referring to the Common Vulnerability Scoring System ([CVSS](#)). Vulnerabilities are prioritized based on severity, impact, and affected area (e.g., firmware, software, hardware). For third-party open-source components, additional evaluation is carried out considering their relevance to the actual deployment environment of IDIS products.

6.3.1 Vulnerability Response Priority

Critical/High (CVSS 7.0 ~ 10.0)

Vulnerabilities that may cause severe threats such as service disruption, remote exploitation, or privilege escalation are addressed promptly with security patches or mitigation measures (e.g., configuration changes, feature restrictions).

For open-source components, remediation time may vary depending on external vendor patch releases.

Medium/Low (CVSS 0.1 ~ 6.9)

Vulnerabilities that generally require privileged local access or have limited impact are addressed as part of scheduled software releases or mitigated through operational guidelines when necessary.

6.3.2 Security Updates and Software Support

IDIS provides prompt firmware updates for its major products whenever security issues or functional improvements are required.

The support period for each product is defined according to IDIS's lifecycle policy, and after the end of support date, new security updates may no longer be provided.

- IDIS offers software support for major products for a certain period even after the product is discontinued.
- The latest firmware and security advisories can be accessed through the official IDIS website and technical support channels.

6.3.3 Security Advisories and Communication

IDIS issues **Security Advisories** for vulnerabilities that may directly affect customers.

Each advisory includes the severity level, scope of impact, and remediation methods (e.g., patch release, configuration guidance).

6.4 Secure Firmware Upgrade Sequence for IDIS Products

1. Firmware Integrity through Hash Verification
 - Users can verify the integrity of the firmware using the SHA-256 file and directly check whether the downloaded file has been corrupted.
2. Establishing TLS Connection (Authentication-based)
 - A TLS session is established using the Discovery Tool with private keys and certificates.
 - This ensures encrypted communication between the device and the server, preventing man-in-the-middle (MITM) attacks or eavesdropping.
3. Transmission of Encrypted Firmware
 - The encrypted firmware package is transmitted through a TLS-protected channel.
 - This prevents data tampering during transmission and ensures secure delivery.
4. Firmware Decryption
 - The received firmware is decrypted into plaintext.
 - The AES-256-CBC algorithm is used for decryption.
5. Decryption Key Management
 - A different decryption key is applied for each product type.
 - Keys are generated based on product identifiers, such as camera model names.
 - Generated keys are protected using IDIS's proprietary obfuscation method and stored in the firmware code in an obfuscated form.

7 Manufacturer's Obligations for Providing Security and Safety Information to Users

7.1 Security Update Notifications and Customer Communication Procedures

IDIS operates a regular technical notification system to ensure that information about product security updates is delivered to customers promptly and clearly.

Information is provided to customers through two primary channels:

1. **Partner Page** – Security update information is shared via the *Notice* and *FAQ* boards on the Partner Page (<https://partners.idisglobal.com>).
2. **Technical Notifications via Email** – When updates are released to address security vulnerabilities or improve functional stability, IDIS issues a document in the format of “**IDIS Technical Notification**” (e.g., *IDIS Technical Notification_July. 25th. 2025.pdf*) and distributes it to customers by email.

Each notification includes the following key information:

- New or Updated Firmware Release
- A&E Specification, User Manual, Product Feature Highlights
- ECN Note, Technical Note, FAQ, Secure Update Notification
- Third-Party Integration, Design Tools, Technical Training

Through these procedures, IDIS ensures that customers fully recognize the importance of security updates and are guided to take timely and appropriate actions.

7.2 Cyber Security Policy

If you have discovered a new vulnerability in any of our products or services, we encourage you to submit your discovery to security@idisglobal.com. The IDIS Cybersecurity Team will respond to your vulnerability submission within 7 days and aim to assess your report within the same timeframe.

After thoroughly reviewing the information you provided, if any vulnerabilities are identified, we will contact you individually with details, and you can also track the progress of your report [here](#).

7.3 Security Precautions for Product Transfer or Disposal

When the product is transferred, disposed of, or otherwise passed on to a third party, there is a risk that personal information and security-related data recorded on the device or on associated storage media may be exposed.

To prevent such risks, the following procedures are strongly recommended when the product is no longer in use:

- **Factory Reset:** Initialize the product to completely delete configuration data, administrator accounts, network settings, and other stored information.
- **Storage Media Handling:** Delete all data on HDDs, SD cards, or other storage media and physically destroy them to ensure they cannot be recovered by third parties.

- **External Service Accounts:** Delete device and user account information registered to external services or applications, such as cloud managers or remote management systems.

⚠ Failure to follow these procedures may result in security risks, including account theft, data leakage, or misuse of server information.

Contact Us

This document may be updated at any time without notice. Please make sure you have the latest version of this document. Please contact the IDIS technical support team closest to you if you have any question related to this document.

- Technical support team in IDIS Headquarters: techsupport@idisglobal.com
- Technical support team in IDIS America: techsupportus@idisglobal.com
- Technical support team in IDIS Europe: uksupport@idisglobal.com
- Technical support team in IDIS Benelux: support@bnl.idisglobal.com

References

- [1] https://en.wikipedia.org/wiki/Digital_video_fingerprinting
- [2] <https://www.networkworld.com/article/2303073/lan-wan-what-is-transport-layer-security-protocol.html>
- [3] <https://cve.mitre.org/>
- [4] <https://www.qualys.com/apps/pci-compliance/>
- [5] [https://en.wikipedia.org/wiki/Backdoor_\(computing\)](https://en.wikipedia.org/wiki/Backdoor_(computing))
- [6] <https://www.securevoy.com/en-gb/two-factor-authentication/what-is-2fa>
- [7] [https://en.wikipedia.org/wiki/Firewall_\(computing\)](https://en.wikipedia.org/wiki/Firewall_(computing))
- [8] https://en.wikipedia.org/wiki/IEEE_802.1X
- [9] <https://rightsinfo.org/the-rights-in-the-european-convention/>
- [10] <https://www.networkwebcams.co.uk/blog/2008/07/07/privacy-masking/>
- [11] [https://www.bsia.co.uk/Portals/4/Publications/197-cctv-privacy-marking-02%20\(2\).pdf](https://www.bsia.co.uk/Portals/4/Publications/197-cctv-privacy-marking-02%20(2).pdf)

Version History

Version	Writer	Revision Date	Remarks
1.3.0	Roy Lee	Jun.19.2026	Added 3.7 Implementation of a Secure Element for Secure Storage
1.2.0	Roy Lee	Sept. 10. 2025	Addition of items in accordance with the Japanese JC-STAR standards
1.1.1	Daniel Lee	Jun. 25. 2021	ICM (IDIS Cloud Manager) security was updated.
1.1.0	Daniel Lee	Feb. 25. 2020	The features under review were removed.
1.0.9	Daniel Lee	Feb. 24. 2020	HTTPS option and host certificate setup on NVR were added in '4.3.2 IDIS Web Server on NVR and TVR'. Some comments in '5.2 Certificate-based Mutual Authentication' were added.
1.0.1	Daniel Lee	Sep. 10. 2019	Intelligent TLS was added as one of SSL/TLS options between ISS server and ISS client.
1.0.0	Daniel Lee, Tommy Zamberlan	Apr. 29. 2019	Initial Release