i-PRO Network Camera Hardening Guide

April 2022

Table of contents

Introduction

Conventional security systems based on analog cameras and recorders were mainly used in closed networks such as corporate networks. However, as the transition of security systems from analog to digital advances, the scale of the network configuration has increased and networks connected to the Internet are becoming the mainstream. Also, as surveillance camera systems are now recognized as part of important social infrastructure, the risk of cyberattacks is increasing day by day just like other IoT devices.

This Guide describes the security features of i-PRO network cameras and how to configure them to reduce risks of cyberattacks.

1. Protection level

Measures against security threats must be taken by considering the environment where the system is installed as well as the assets and information to be protected.

In general, the following procedures are used when considering the cybersecurity of surveillance camera systems.

Step 1: Clarify the overall configuration of the target surveillance camera system.

Step 2: Clarify the information, functions, and assets to be protected in the system.

Step 3: Clarify the expected threats to the information, functions, and assets to be protected (threat analysis).

Step 4: Clarify the best practices against such threats.

Step 5: Select the measures to implement in consideration of the threat level, damage level, costs, etc.

In the following chapters, this Guide describes the security settings of i-PRO network cameras according to the protection level. Perform a thorough threat analysis and then take necessary and sufficient measures according to the protection level.

Protection level	Explanation
Entry	The lowest recommended protection level. It is suitable for small companies and offices where the operator also serves as the administrator.
Standard	This setting is recommended for companies with a full-time administrator.
Advanced	This setting is recommended for large-scale network infrastructures where there is an IT/IS department.

Protection level	Setting item	Default	Recommended setting
Entry	Initialization of configuration data	-	-
	Use of the latest firmware	-	-
	Administrator password	Not set	-
	User account	Not set	-
	User authentication	Digest	Digest
	Network	DHCP	-
	Date and time	NTP: Manual	NTP: Synchronization with NTP server
	Audio settings	OFF	OFF
	Encryption of video recording data in SD card	OFF	ON
Standard	FTP server	Prohibited	Prohibited
	UPnP	OFF	OFF
	Easy IP Setup	20 minutes	20 minutes
	SMTP	SSL disabled	SSL enabled
	Host authentication	Not performed	Performed
	HTTPS	HTTP+HTTPS	HTTPS
	Internet mode	OFF	ON

	Data encryption	OFF	ON
	Detection of alternation	OFF	ON
	SRTP	OFF	ON
Advanced	IEEE 802.1X	OFF	ON
	SNMP	SNMPv1/v2	v3
	Log	-	-

2. Entry

This protection level is the recommended minimum protection level. It is suitable for small companies and offices where the operator also serves as the administrator.

2.1. Initialization of configuration data

First, confirm that the product settings are set to the default settings. Initialization will set the minimum protection level on the i-PRO network camera. If the settings are unknown, initialize the configuration data from the maintenance screen.

2.2. Use of the latest firmware

The firmware of the i-PRO network camera is checked for vulnerabilities before shipment based on past vulnerability information. Vulnerabilities may be found after the firmware is released. If a new vulnerability is found, then i-PRO will quickly make corrections and update the firmware. Convenience for customers will also be improved and problems will be corrected. Therefore, please regularly check for updates and always use the latest firmware.

The firmware and release notes describing the update details can be downloaded for free from the i-PRO website below.

https://i-pro.com/global/en/surveillance/training-support/documentation-database-list

Note that release notes may not contain details of measures against vulnerabilities.

The firmware is encrypted and cannot be analyzed.

2.3. Setting administrator password

The administrator password must be set when accessing the i-PRO network camera for the first time. Passwords are the most important elements of protection for the i-PRO network

camera. Use a strong password that is difficult to predict and manage your password to prevent it from being leaked.

Follow the rules below when setting a password.

(1) Use at least three of the following for passwords: uppercase letters, lowercase letters, numbers, and symbols.

(2) Change the password periodically.

(3) The password should not include your user name.

2.4. Setting user accounts

To prevent the risk of leaking the administrator password, create users and use them to perform regular operations. There are three user access levels: "Administrator", "Camera control", and "Live only". Set the minimum access level according to the tasks each operator needs to perform.

2.5. User authentication

Even if the system is operated with proper user names and passwords, depending on the authentication method, they may be illegally obtained by cyber attackers through network capture.

There are two authentication methods defined in HTTP/RTSP as shown below.

(1) Basic authentication

With basic authentication, user names and passwords are transmitted in plain text.

(2) Digest authentication

With digest authentication, user names and passwords are hashed before being transmitted, so that no plain text IDs or passwords flow over the network.

Digest authentication is specified on i-PRO network cameras by default. Basic authentication should not be used unless it is absolutely necessary to maintain backward compatibility.

2.6. Network Settings

Network settings for i-PRO network cameras can be accessed from [Network] - [Network] in the Settings menu. The connection mode can be selected from Static, DHCP, Auto

(AutoIP), and Auto (Advanced). Enter the correct setting according to the preliminary network design.

When not using the DNS function, it is recommended to leave it unset.

2.7. Date and time settings

From a security perspective, keeping the correct date and time is important. For example, this will ensure that the system logs are recorded with the correct time.
It is recommended to synchronize the clock of the i-PRO network camera with the Network Time Protocol (NTP) server. To configure the NTP settings, select [Network] - [Advanced] in the Settings menu and use the "NTP" tab displayed.

2.8. Audio settings

On models that support audio, audio is disabled by default. In general, audio requires stricter management than video in order to protect privacy and integrity. It is recommended to check the applicable regulations before using audio.

2.9. Password lock for SD card

When recording video to an SD card using an i-PRO network camera that supports SD cards, it is recommended to set a password lock for the SD card. This will prevent the saved video from being played by an unauthorized individual even if they take the SD card.

3. Standard

The use of video management system (hereinafter referred to as VMS) software or network disk recorder (hereinafter referred to as NVR) is recommended for medium and large corporations that use a professional surveillance camera system. When using VMS, follow the VMS manufacturer’s recommendations regarding cybersecurity.

Some of the settings described in this section have already been preset in the factory. Confirm that the settings have been configured correctly by following the procedure below.

3.1. Open ports

On i-PRO network cameras, the following ports are open by default.

Port	Service
TCP-80	HTTP
TCP-443	HTTPS
TCP-554	RTSP
UDP-3702	ONVI WS-Discovery
UDP-162	SNMP
UDP-10670	Easy IP Setup

3.2. Disabling unused services

Although unused services do not necessarily pose an immediate threat to security, disabling them is recommended in order to reduce unnecessary risks. The following are some of the services that can be disabled when they are not in use.

3.2.1. FTP server

When the FTP server function is enabled, the i-PRO network camera can be accessed from FTP clients via FTP. As FTP communications are not encrypted, setting the FTP server function to OFF is recommended when the FTP server function is not used in order to prevent user names, passwords, and transferred data from being stolen. To set the FTP server function to OFF, select [Network] - [Network] in the Settings menu and set "FTP access to camera" to "Forbid".

3.2.2. FTP client

Enabling the FTP client function enables the transfer of image files to external FTP servers. Since FTP communications are not encrypted, setting the FTP client function to OFF is recommended during use in unsafe environment in order to prevent user names, passwords, and transferred data from being stolen.

3.2.3. UPnP

When the automatic port forwarding setting of UPnP is implemented, the port forwarding setting will be executed on the NAT router, making the i-PRO network camera accessible from the external Internet. To deny access from external environments, select [Network] - [Advanced] in the Settings menu and set "Auto port forwarding" in the "UPnP" tab to "Off".

3.2.4. Easy IP Setup

When Easy IP Setup for the i-PRO network cameras is enabled, the IP address of the i-PRO network cameras on the same network can be acquired from the Easy IP Setup tool. If a third party acquires the IP address of a network camera, the risk of unauthorized intrusion or DOS attacks increases. After the Easy IP Setup for the i-PRO network camera is completed, it is recommended to change the term of validity from no limit to 20 minutes in order to prevent the i-PRO network camera from being searched from the Easy IP Setup tool. To restrict the Easy IP Setup, select [Network] - [Network] in the Settings menu and set "Easy IP Setup valid period" to "20 minutes".

3.2.5. SMTP

When emails are sent via SMTP, user names and passwords for connecting the SMTP server are not encrypted and may be stolen. For this reason, it is recommended to send emails to a server that supports SMTPoverSSL when sending emails via SMTP. To enable SMTPoverSSL, select [Network] - [Advanced] in the Settings menu and set "SSL" to "On" in the SMTP (E-mail) tab.

3.3. Host authentication (IP address filtering)

If the same client IP address is always used for accessing the i-PRO network camera or the camera belongs to a specific network, you can block access to the network from locations other than the registered host by setting host authentication (IP address filtering).

To set host authentication, select [User mng.] - [Host auth.] in the Settings menu and set "Host auth." to "On".

To authorize only a specific IP address, enter the address "192.168.0.100," for example. To authorize access only from the network that the camera belongs to, enter a subnet in CIDR format, for example 192.168.0.0/24, in order to authorize access from the entire subnet.

You must carefully confirm that the range of access is correct during configuration. If the camera became unaccessible due to an incorrect setting, initialize the configuration data. Also, please note that when IPv6 is enabled, access from IPv6 addresses is enabled even when IP address filtering is implemented.

3.4. HTTPS

HTTPS (Hypertext Transfer Protocol Secure) is a protocol for secure communication via

HTTP. HTTP communication is executed over secure connection provided by the SSL/TLS protocol.

For the HTTP server in the i-PRO network camera, both HTTP and HTTPS communications are enabled by default. Changing the setting to only enable HTTPS communication is recommended for safer communication. To enable only HTTPS communication, select [Network] - [Advanced] in the Settings menu and change the "Connection" setting in the HTTPS tab to "HTTPS".

A server certificate is required to operate the HTTPS server. The following two types of server certificates can be used with i-PRO network cameras.

(1) Pre-installed certificate (self-signed certificate for some models)

(2) CA certificate

The certificate pre-installed on the i-PRO network camera is signed by the CA of GlobalSign K.K., and not signed by the CA established by the company itself. When using a CA certificate, a CSR must be generated from a CRT key in advance and a certificate must be issued by a trusted certification organization.

3.5. Internet mode

RTSP/RTP/RTCP used for streaming purposes do not support encrypted communication by SSL like HTTP. Therefore, user names, passwords, and transferred data may be stolen or altered in RTSP/RTP/RTCP. In order to prevent this, it is recommended to use HTTPS for streaming or tunnel RTSP/RTP/RTCP by HTTPS. In order to use HTTPS tunneling for streaming from a browser, the Internet mode setting must be configured. To configure the Internet mode setting, select [Image/Audio] - [Image] in the Settings menu and set "Internet mode" to "On".

3.6. Data encryption

As HTTPS and VPN are protocols used for secure communication, communicated data is decrypted. Therefore, if recorded data leaks after communication, the data can be viewed as is. Meanwhile, in data encryption, data itself is the subject of encryption so data remains encrypted even when it is recorded to a storage medium. Therefore, the unauthorized viewing of images is disabled even when hard disk or SD card is stolen or data on the cloud is breached.

To enable data encryption on the i-PRO network camera, select [User mng.] - [Data encryption] in the Settings menu and use the tab displayed.

3.7. Detection of alternation

The use of data encryption prevents the unauthorized viewing of data recorded on a storage medium such as an SD card or HDD. However, it cannot eliminate risks of tampering with the data itself. The tamper detection function can detect the tampering of data recorded on SD cards.

Select [Basic] - [SD memory card] in the Settings menu and click "Additional info for detection alternation" to open a different window. Set "Additional info for tamper detection" to "On" and click the "Set" button to confirm the setting. Tamper detection only supports video (MP4 format). Recorded data can be checked for tampering by using dedicated software.

3.8. SRTP

The RTP/RTSP protocol used for streaming video data is different from HTTPS in that user names, passwords, video data, and other information flow through the communication channel without being encrypted. SRTP is a protocol for encrypting RTP packets and streaming. In SRTP communication, the RTSP protocol is also encrypted by SSL so there is no risk of unauthorized viewing of user names or passwords. Port number "322" of the i-PRO network camera is used for RTSPS (RTSPoverSSL) communication. To use the SRTP function, SecurityCenter provided by Genetec Inc. is required as a client.

4. Advanced

This protection level is recommended for large-scale network infrastructure managed by an IT/IS department.

4.1. IEEE 802.1X network access control

IEEE 802.1x is a technology to enable only authorized devices to be connected to a network. The use of this system can prevent people with malicious intentions from connecting a PC to an available switching hub port, hacking into a network, and gain unauthorized access or eavesdropping.

The types of EAP include EAP-MD5, PEAP, and EAP-TLS. EAP-MD5 and PEAP are authentication methods using an ID and password, while EAP-TLS uses an electronic

certificate.

To configure the settings on the i-PRO network camera, select [User mng.] - [IEEE 802.1x] in the Settings menu and use the tab displayed.

4.2. SNMP monitoring

In SNMP v1/v2, packets can be eavesdropped or tampered with as the packets themselves are not encrypted. In an environment with a risk of eavesdropping or tampering by a third party, the use of SNMPv3 is recommended as it has an encryption function as well as a function to detect tampering. SNMPv3 can be used by selecting [Network] - [Advanced] in the Settings menu and setting "SNMP version" in the SNMP tab to "SNMPv3".

5.3 Log

Monitoring to check for unauthorized access to the network camera is important to ensure security. The i-PRO network camera displays logs of access failures that can be viewed by selecting [Maintenance] - [System log] in the Settings menu. Check the system log regularly to check for any abnormalities such as unauthorized logins.

About i-PRO Co., Ltd.

i-PRO Co., Ltd. is a leading global provider of sensing solutions that are essential in the fields of security surveillance, public safety, and medical imaging. The company was established in 2019, inheriting various sensing technologies and innovations accumulated by Panasonic over more than 60 years.

With our advanced sensing technology to capture every moment and highly reliable solutions that support all types of environments, we support professionals who protect and save people's lives and contribute to the achievement of a safer and more secure society.

Hideo Noguchi

Director, Module Development | Global Security Products

The Power of Truth

4-1-62 Minoshima, Hakata-ku, Fukuoka-shi, Fukuoka, 812-8531 Japan

i-pro.com/corp/jp/