Hanwha Vision

White Paper

Device Manager

January 05, 2024

Contents

Contents

1. Overview

Hanwha Vision's Device Manager is a convenient and practical solution that streamlines the management of video surveillance devices, empowering users to control them with comprehensive management and monitoring capabilities for a wide range of equipment.

Through Device Manager, users can view all connected devices at a glance through a centralized interface, allowing real-time monitoring of device status, operational status, sensor data, and more. Moreover, users can efficiently configure basic functionalities for multiple devices connected to the network all at once. They can effortlessly check the firmware version of each device and conduct remote updates to ensure they are running on the latest version. In addition, the solution facilitates security management by supporting features for certificate registration and management.

Device Manager offers the following features:

- Discover devices installed on the same network automatically.
- Categorize and manage devices by product groups.
- Register devices manually if the device is not discovered automatically.
- Manage devices by projects based on their intended use, with the option to set passwords for each project to enhance security.
- Configure basic functionalities for multiple devices discovered on the same network.
- Check and update firmware versions for registered devices.
- Manage credentials/certificates for registered devices.
- Import/export configurations for registered devices
- View system logs for registered devices.

Hanwha Vision's Device Manager combines a user-friendly interface with powerful functionalities to efficiently support users in managing equipment. This white paper explains how to configure and use Hanwha Vision's Device Manager. For more information, please refer to the Device Manager User Manual.

2. System Requirements

To install and use Device Manager, the following environment is required:

- Operating System: Windows 7, 10, 11 (64-bit)
- Application: Microsoft .NET Framework 4.7.2 Client Profile,

  Microsoft Visual C++ 2010 Redistributable Package (x86)

  (Included in the Device Manager installation package.)
- CPU: Intel CPU i5 8th generation or higher
- Graphics: Video graphics card
- RAM: DDR4 8G or higher
- Resolution: 1366x768 (Scaling options are not officially supported.)
- Network Port

  - IP/TCP Based

    HTTP: 80

    HTTPS: 443

    RTSP : 554

  - UDP Based

    Discovery, IP setting, Initial PW : 7701, 7711

Note

System requirements may vary when using WiseDetector from the Device Manager. (For example, Microsoft Visual C++ 2015~2022 versions are required when using WiseDetector) The Device Manager sends camera information discovered on the network to WiseDetector, allowing the camera's live video feed to be connected. With WiseDetector, users can generate training data from video footage collected from the connected cameras and send the training data to designated cameras for object detection. WiseDetector is available only on cameras compatible with WiseDetector (such as P AI Series). For more information, please refer to the online help documentation provided by Device Manager.

3. Installation

3.1. Download and Installation Guide

3.1.1. Download Path

You can download the Wisenet Device Manager installation program from the Hanwha Vision website. Visit the Hanwha Vision website (https://www.hanwhavision.com) and click on [Support] > [Online Tool] > [PC Installation Tool] > [Wisenet Device Manager] > [Download].

Alternatively, you can download the installation program from the following links.

- English: https://www.hanwhavision.com/en/support/online-tool
- Korean: https://www.hanwhavision.com/ko/support/online-tool

3.1.2. Installation Guide

1) Double-click the downloaded Wisenet Device Manager installation program.
2) From the [Installer Language] window, select the desired language. (Choose either English or Korean.)
3) From the [Wisenet Device Manager Setup] window, review and accept the terms of the license agreement, choose the destination folder, and press [Install] to proceed with the installation.
4) After the installation is complete, click [Finish] and close the [Wisenet Device Manager Setup] window. If you put a checkmark on the [Run Wisenet Device Manager] checkbox before pressing the [Finish] button, the program will launch immediately upon closing the window.

3.1.3. Run Device Manager

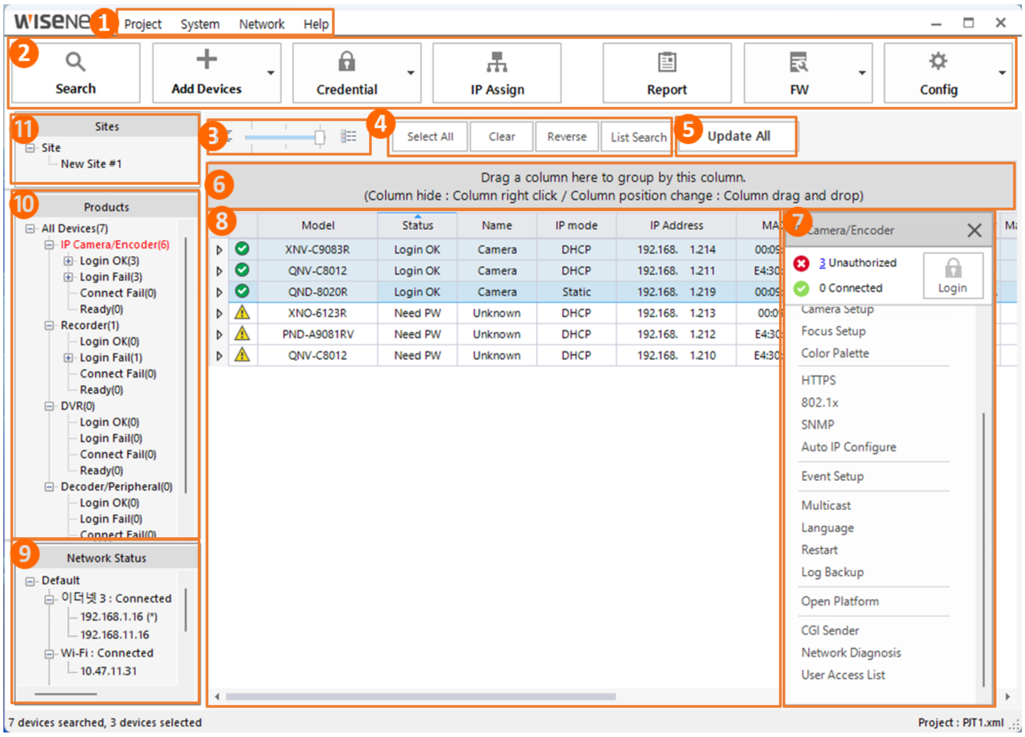
1) Run Device Manager installed on your PC.
2) You can create a new project or select an existing one.
   - New Project: When the [New Project] window appears, set the project name and path.
   - Add Project: Go to the project folder path where you want to add a project, then add the project file (*.xml) to include it in the project list.
   - Select Project: Choose the project you want to run from the project list, then click [Open].

> **Note**
>
> If you select [Auto-run the last imported project], the next time you launch Device Manager, the [Open Project] window will not appear, and the previously loaded project will run automatically.

4. User Guide

4.1. Screen Layout

Shown below is the Device Manager screen layout.



Drag a column here to group by this column.
(Column hide : Column right click / Column position change : Column drag and drop)

	Model	Status	Name	IP mode	IP Address	MA
✓	XNV-C9083R	Login OK	Camera	DHCP	192.168. 1.214	00:09
✓	QNV-C8012	Login OK	Camera	DHCP	192.168. 1.211	E4:30
✓	QND-8020R	Login OK	Camera	Static	192.168. 1.219	00:09
⚠	XNO-6123R	Need PW	Unknown	DHCP	192.168. 1.213	00:0
⚠	PND-A9081RV	Need PW	Unknown	DHCP	192.168. 1.212	E4:30
⚠	QNV-C8012	Need PW	Unknown	DHCP	192.168. 1.210	E4:30

7 devices searched, 3 devices selected

Project : PJT1.xml

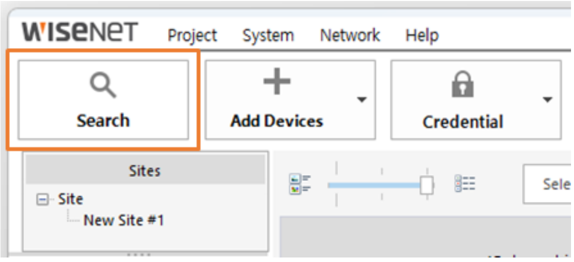
Category		Description
①	Menu Bar	Access to functions to interact with the program.
②	Toolbar	Device control settings.
③	Layout Selection Bar	Choose the layout of the registered device list. (From left to right: SnapShot view/Show all information/Display profile by channel)
④	Device Selection Tool	Select registered devices.
⑤	Update All	Update the status of all registered devices.

⑥	Group Device List	Group the list of devices and display.
⑦	Device Setup Menu	Configure the functions of the selected device.
⑧	Device List	Display the list of registered devices.
⑨	Network Status	Display the PC's current network status and IP address.
⑩	Products	Classify and display searched devices by product category.
⑪	Sites	Organize and manage devices grouped by sites.

4.2. Search Camera

Search for Hanwha Vision devices that are connected to the same network.

1) Click [Search] in the toolbar to search for devices.



2) After the search is complete, a list of devices connected to the network will be displayed.

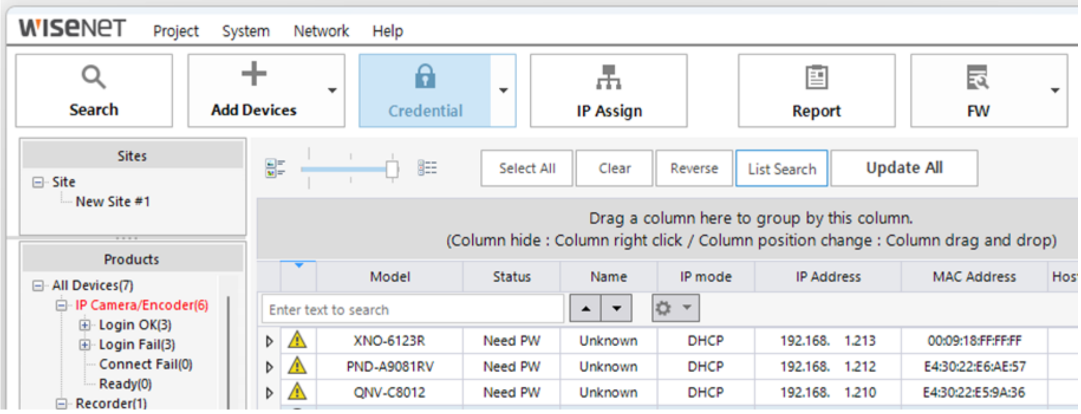
> **Note**
>
> The device search time can be adjusted from [System]>[Device Search Time Setting]. (The search time duration is set to 5 seconds by default. The search time duration can be set up to 60 seconds in increments of 5 seconds.) NVR devices may not be found due to IP conflicts. In this case, check the network settings of the NVR device. Refer to the product manual for more information. If the device is not found, check the connection status of the router or hub connected to the device. If there are two or more routers connected, it is recommended to set one router to hub mode to prevent IP conflicts.

4.3. Camera Device List

4.3.1. Search and Configure Device List

You can search for the desired device within the device list.

1) Click [List Search] or press Ctrl + F to open the search bar.



Drag a column here to group by this column.
(Column hide : Column right click / Column position change : Column drag and drop)

Model	Status	Name	IP mode	IP Address	MAC Address	Hos
XNO-6123R	Need PW	Unknown	DHCP	192.168. 1.213	00:09:18:FF:FF:FF	
PND-A9081RV	Need PW	Unknown	DHCP	192.168. 1.212	E4:30:22:E6:AE:57	
QNV-C8012	Need PW	Unknown	DHCP	192.168. 1.210	E4:30:22:E5:9A:36	

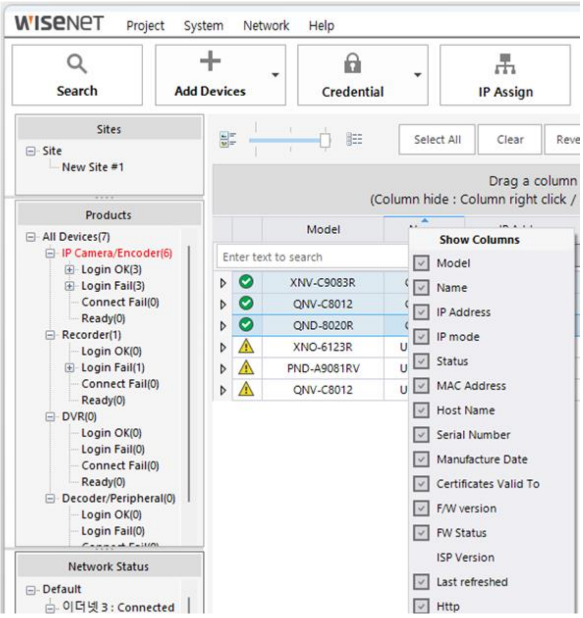
2) Enter text to search in the search bar.

3) Click the arrow (▲▼) next to the search bar to quickly search for items that contain the entered value.

4) Click the search options icon (⚙▾) to configure search options.

5) You can choose to show or hide specific columns in the device list.

- Right-click on any column.
- Check the checkbox for the columns you want to display in the device list.

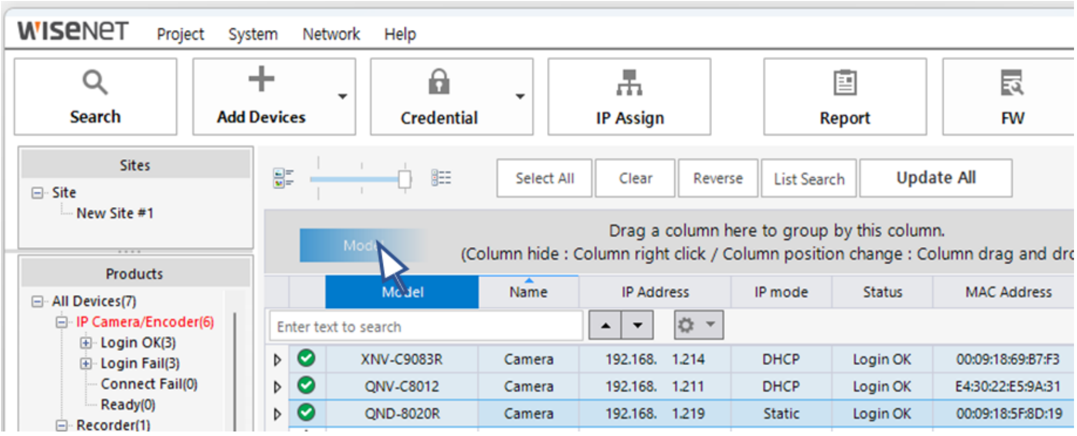


To change the column order, click and drag the desired column to the desired position while holding the mouse.

4.3.2. Group Device List

You can group the device list into desired groups for display.

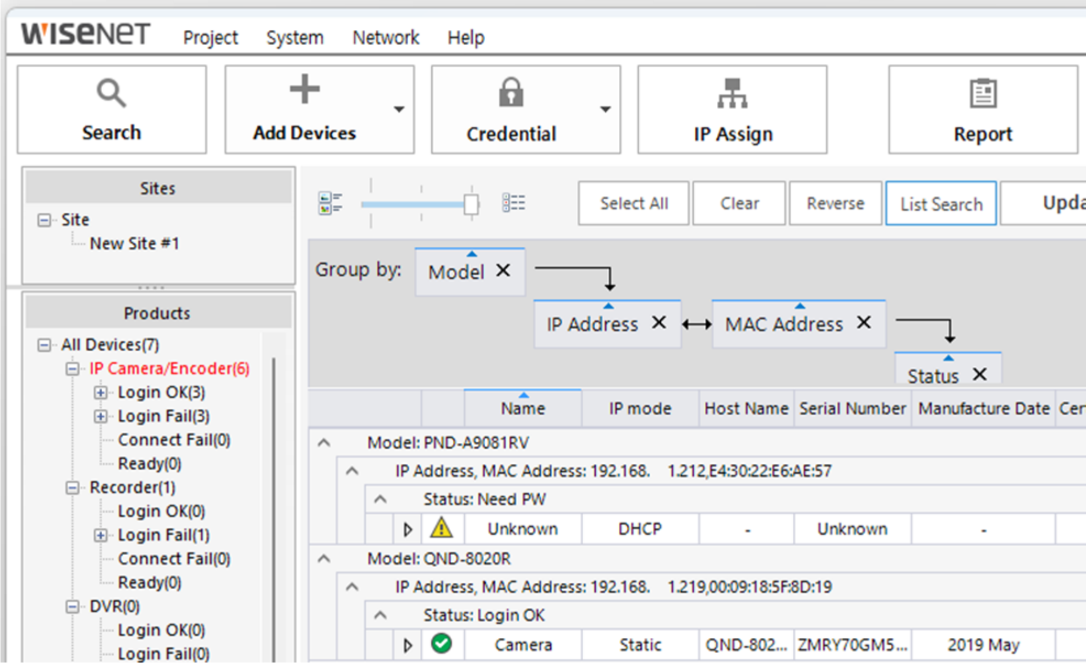
1) Select the desired column and drag it to the grouping area.



Drag a column here to group by this column.
(Column hide : Column right click / Column position change : Column drag and drc

Model	Name	IP Address	IP mode	Status	MAC Address
XNV-C9083R	Camera	192.168. 1.214	DHCP	Login OK	00:09:18:69:B7:F3
QNV-C8012	Camera	192.168. 1.211	DHCP	Login OK	E4:30:22:E5:9A:31
QND-8020R	Camera	192.168. 1.219	Static	Login OK	00:09:18:5F:8D:19

2) The device list based on the configured groups and levels will be displayed.



```
Name      IP mode  Host Name  Serial Number  Manufacture Date  Cer
Model: PND-A9081RV
  IP Address, MAC Address: 192.168.   1.212,E4:30:22:E6:AE:57
    Status: Need PW
      ⚠  Unknown   DHCP   -          Unknown        -
Model: QND-8020R
  IP Address, MAC Address: 192.168.   1.219,00:09:18:5F:8D:19
    Status: Login OK
      ✓  Camera    Static QND-802...  ZMRY70GM5...  2019 May
```

4.4. Login and IP Configuration

The Device Manager uses SUNAPI (HTTP(s) common protocol) for login and IP configuration.

During the device search process, if a device without a password is detected, a prompt will appear, allowing the user to set an initial password for the device.

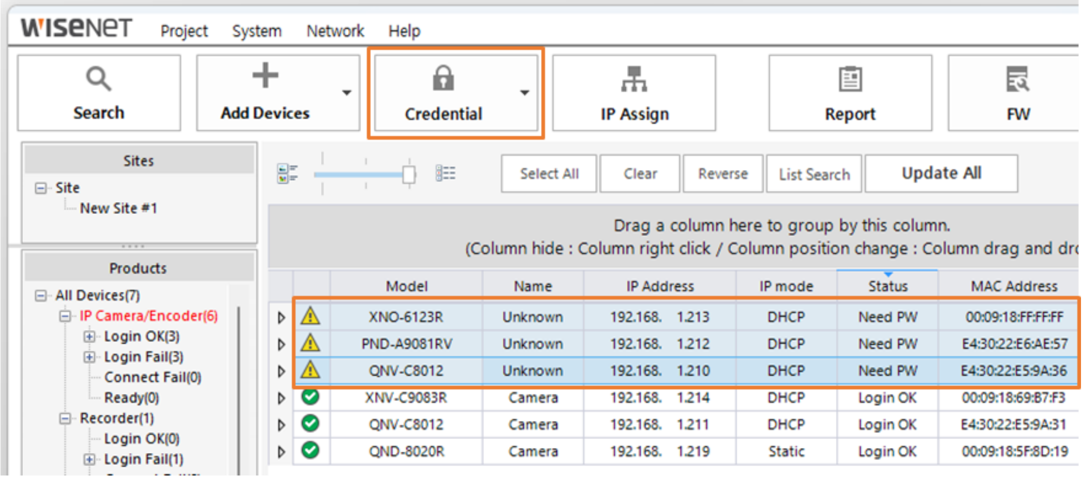
> **Note**
>
> To safeguard the password data, when transmitting information such as device details and passwords, it is encrypted using the unique RSA key of each device.

4.4.1. Login

To make direct changes to the configurations of a registered device from the Device Manager, the administrator password of the selected device must be entered and authenticated.

1) Select the device from the device list.

2) Click [Credential].



Drag a column here to group by this column.
(Column hide : Column right click / Column position change : Column drag and dr

Model	Name	IP Address	IP mode	Status	MAC Address
XNO-6123R	Unknown	192.168. 1.213	DHCP	Need PW	00:09:18:FF:FF:FF
PND-A9081RV	Unknown	192.168. 1.212	DHCP	Need PW	E4:30:22:E6:AE:57
QNV-C8012	Unknown	192.168. 1.210	DHCP	Need PW	E4:30:22:E5:9A:36
XNV-C9083R	Camera	192.168. 1.214	DHCP	Login OK	00:09:18:69:B7:F3
QNV-C8012	Camera	192.168. 1.211	DHCP	Login OK	E4:30:22:E5:9A:31
QND-8020R	Camera	192.168. 1.219	Static	Login OK	00:09:18:5F:8D:19

3) Enter the user ID and password, then click [Apply].

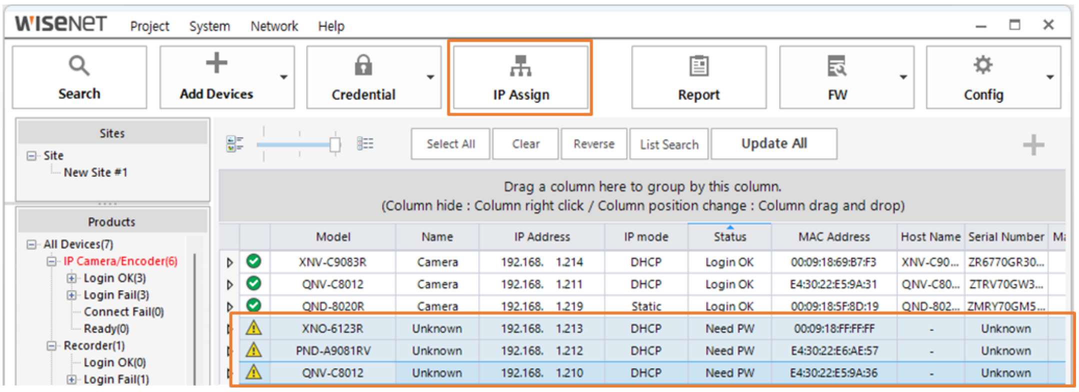
4) The login status is displayed in the [Result] section of each device.

4.4.2. IP Configuration

This feature allows you to set the IP address of the device. You can also set the IP addresses of multiple devices at once.

1) Select the device from the device list.

2) Click [IP Assign].



Drag a column here to group by this column.
(Column hide : Column right click / Column position change : Column drag and drop)

Model	Name	IP Address	IP mode	Status	MAC Address	Host Name	Serial Number
XNV-C9083R	Camera	192.168. 1.214	DHCP	Login OK	00:09:18:69:B7:F3	XNV-C90...	ZR6770GR30...
QNV-C8012	Camera	192.168. 1.211	DHCP	Login OK	E4:30:22:E5:9A:31	QNV-C80...	ZTRV70GW3...
QND-8020R	Camera	192.168. 1.219	Static	Login OK	00:09:18:5F:8D:19	QND-802...	ZMRY70GM5...
XNO-6123R	Unknown	192.168. 1.213	DHCP	Need PW	00:09:18:FF:FF:FF	-	Unknown
PND-A9081RV	Unknown	192.168. 1.212	DHCP	Need PW	E4:30:22:E6:AE:57	-	Unknown
QNV-C8012	Unknown	192.168. 1.210	DHCP	Need PW	E4:30:22:E5:9A:36	-	Unknown

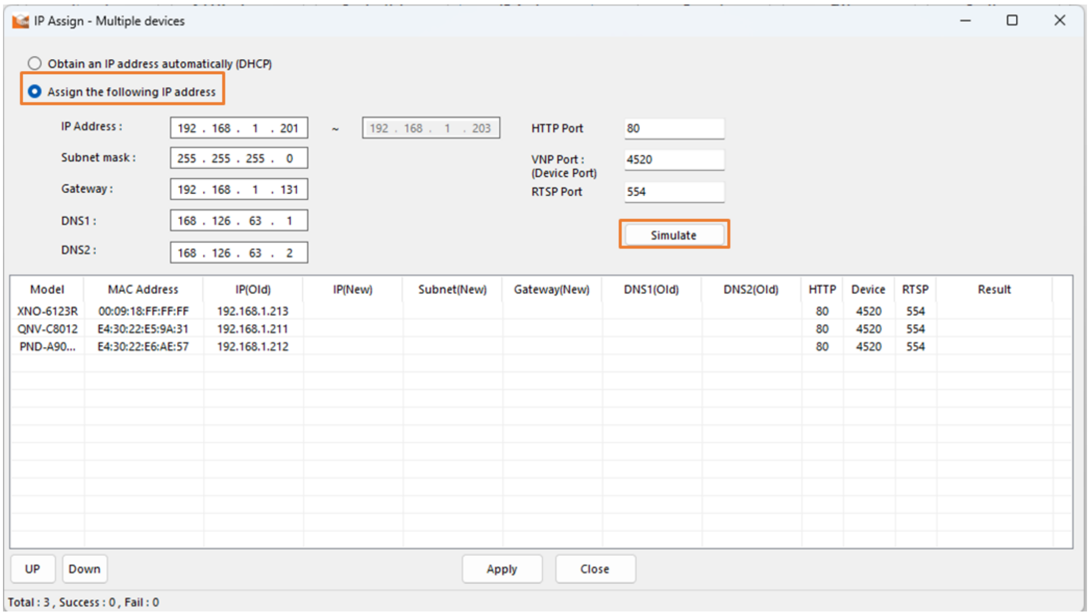
3) If you want the IP address to be automatically assigned through DHCP, select [Obtain an IP address automatically (DHCP)] in the [IP Assign – Single device] window, enter the port and DNS information, and click [Apply].

4) If you want to set a static IP address, select [Assign the following IP address] from the [IP Assign – Single device] window, enter the starting address of the IP address, provide port information, and then click [Apply].

5) To set IP addresses for multiple devices at once, select multiple devices from step 1, then click [IP Assign].

6) From the [IP Assign – Multiple devices] window, select [Assign the following IP address] and enter the starting address of the IP address, provide IP and Port information, and then click [Simulate].

7) After reviewing the IP address assigned to each device, click [Apply].



○ Obtain an IP address automatically (DHCP)

● Assign the following IP address

IP Address : 192 . 168 . 1 . 201 ~ 192 . 168 . 1 . 203

Subnet mask : 255 . 255 . 255 . 0

Gateway : 192 . 168 . 1 . 131

DNS1 : 168 . 126 . 63 . 1

DNS2 : 168 . 126 . 63 . 2

HTTP Port 80

VNP Port : (Device Port) 4520

RTSP Port 554

Model	MAC Address	IP(Old)	IP(New)	Subnet(New)	Gateway(New)	DNS1(Old)	DNS2(Old)	HTTP	Device	RTSP	Result
XNO-6123R	00:09:18:FF:FF:FF	192.168.1.213						80	4520	554	
QNV-C8012	E4:30:22:E5:9A:31	192.168.1.211						80	4520	554	
PND-A90...	E4:30:22:E6:AE:57	192.168.1.212						80	4520	554	

Total : 3 , Success : 0 , Fail : 0

4.5. Report

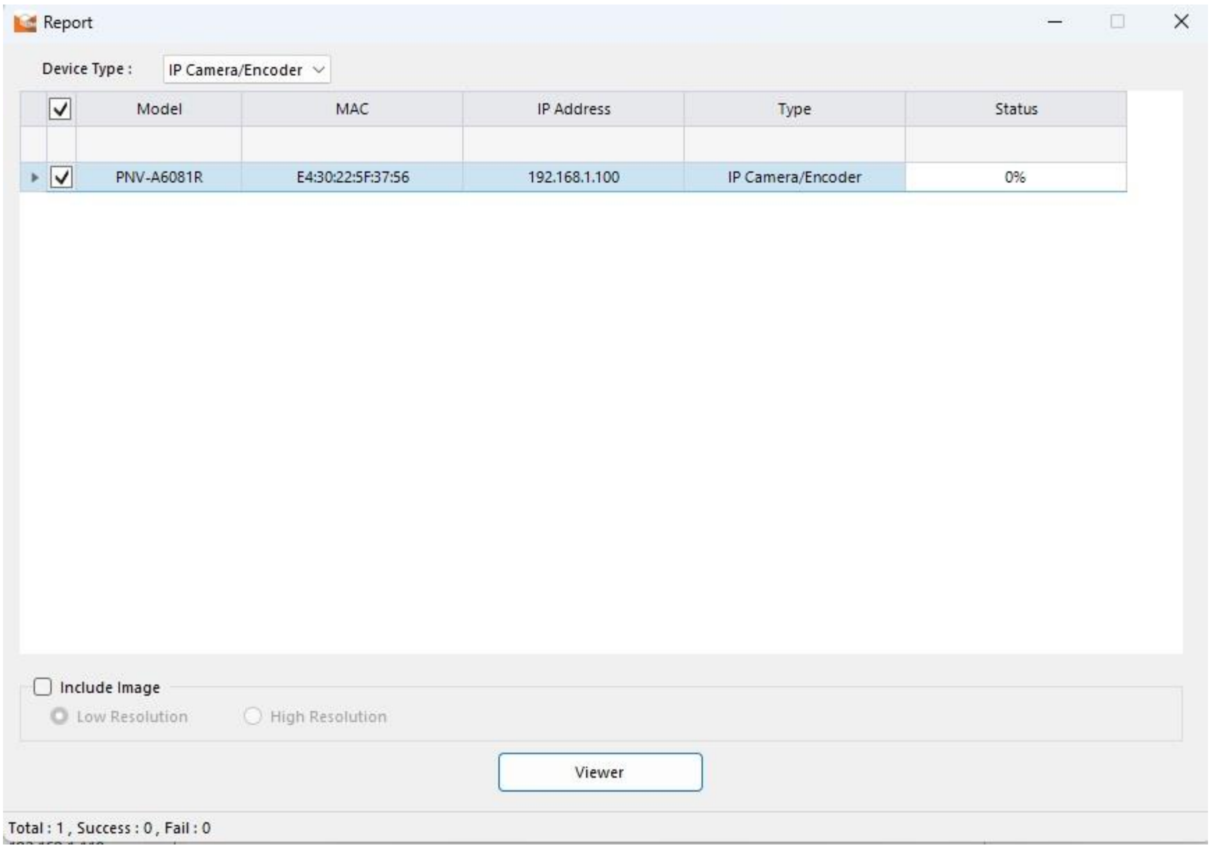
You can generate a file containing device information and save it in either "xls" or "csv" format.

SUNAPI (HTTP(s) common protocol) is used for collecting device information.

1) Select the device for which you want to generate the report from the device list.

2) Click [Report].

3) When the [Report] window appears, select the devices for which you want to generate the report and click [Viewer].



Report

Device Type : IP Camera/Encoder

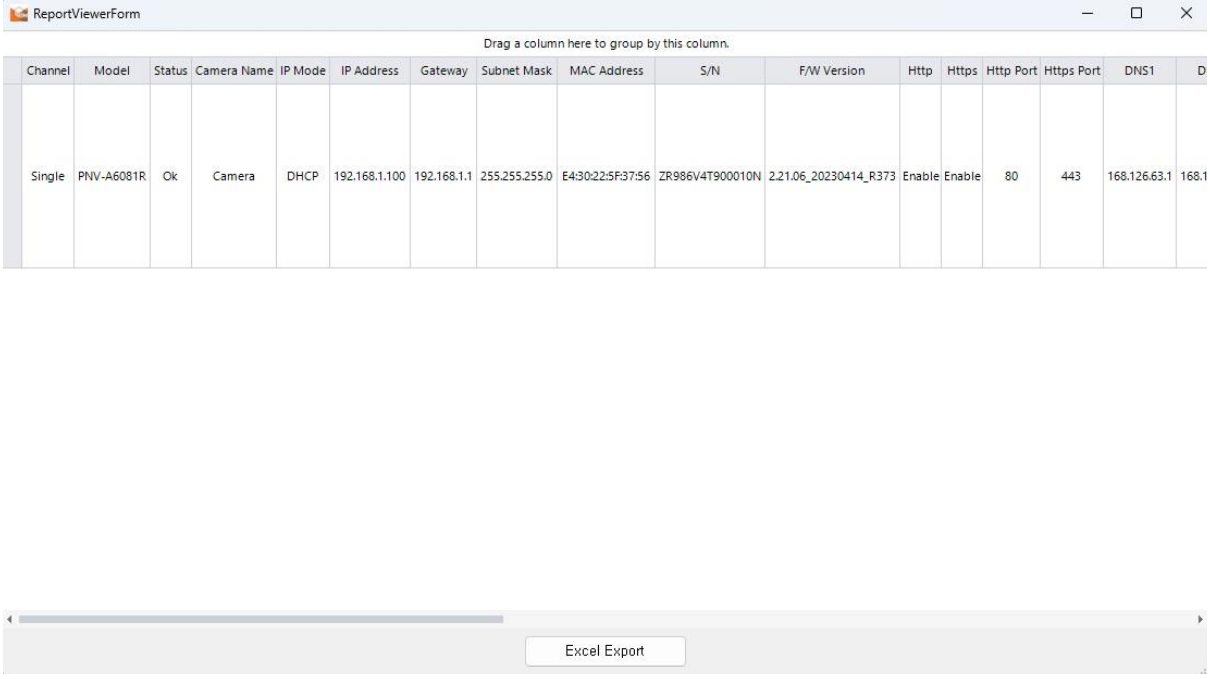
☑	Model	MAC	IP Address	Type	Status
☑	PNV-A6081R	E4:30:22:5F:37:56	192.168.1.100	IP Camera/Encoder	0%

□ Include Image

● Low Resolution ○ High Resolution

Total : 1 , Success : 0 , Fail : 0

4) After reviewing the device information, click [Excel Export].



ReportViewerForm

Drag a column here to group by this column.

Channel	Model	Status	Camera Name	IP Mode	IP Address	Gateway	Subnet Mask	MAC Address	S/N	F/W Version	Http	Https	Http Port	Https Port	DNS1	D
Single	PNV-A6081R	Ok	Camera	DHCP	192.168.1.100	192.168.1.1	255.255.255.0	E4:30:22:5F:37:56	ZR986V4T900010N	2.21.06_20230414_R373	Enable	Enable	80	443	168.126.63.1	168.1

5) In the [Save As] dialog box, select the folder location and file format, then click [Save].

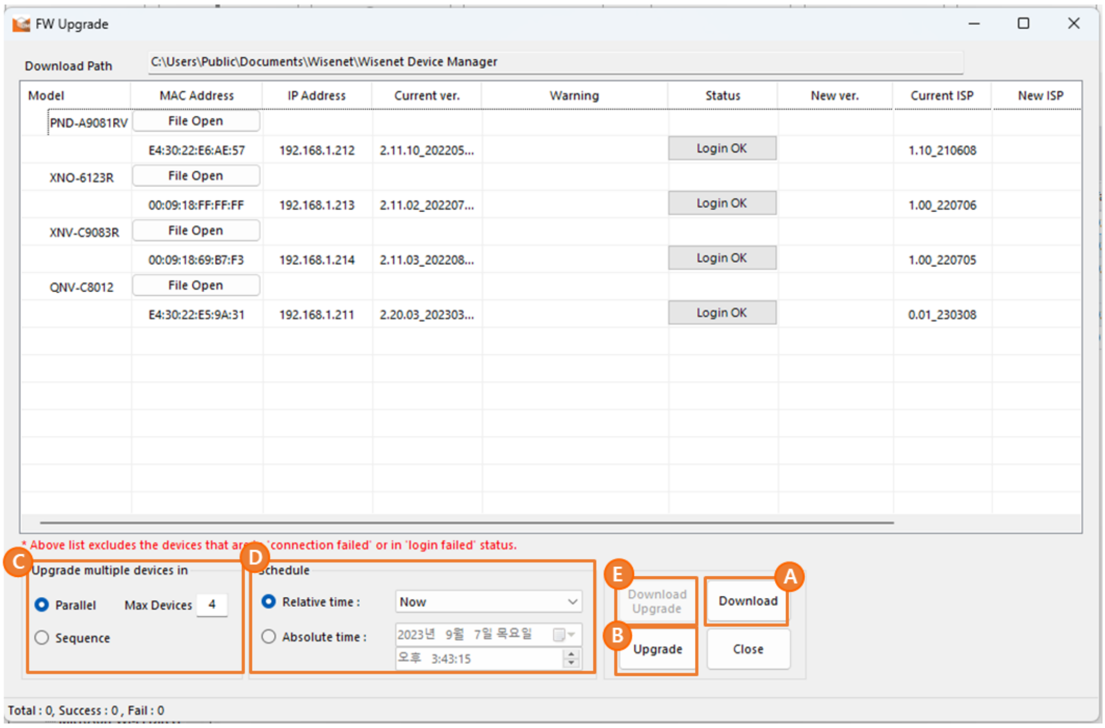
> **Note**
>
> If you want to include images, check the "Include Image" checkbox and then select [Low Resolution] or [High Resolution]. If you save the report in CSV format, images will not be included.

4.6. Firmware

You can check the firmware status of authorized devices and perform firmware updates.

SUNAPI (HTTP(s) common protocol) is used for device firmware upgrades.

1) Select the device for which you want to update the firmware from the device list.
2) Click [FW] > [FW Update].
3) From the [FW Upgrade] window, you can perform the following actions:



FW Upgrade

Download Path: C:\Users\Public\Documents\Wisenet\Wisenet Device Manager

Model	MAC Address	IP Address	Current ver.	Warning	Status	New ver.	Current ISP	New ISP
PND-A9081RV	File Open							
	E4:30:22:E6:AE:57	192.168.1.212	2.11.10_202205...		Login OK		1.10_210608	
XNO-6123R	File Open							
	00:09:18:FF:FF:FF	192.168.1.213	2.11.02_202207...		Login OK		1.00_220706	
XNV-C9083R	File Open							
	00:09:18:69:B7:F3	192.168.1.214	2.11.03_202208...		Login OK		1.00_220705	
QNV-C8012	File Open							
	E4:30:22:E5:9A:31	192.168.1.211	2.20.03_202303...		Login OK		0.01_230308	

* Above list excludes the devices that ar 'connection failed' or in 'login failed' status.

Upgrade multiple devices in

● Parallel Max Devices 4

○ Sequence

Schedule

● Relative time : Now

○ Absolute time : 2023년 9월 7일 목요일 오후 3:43:15

Total : 0, Success : 0 , Fail : 0

A. Download the firmware for the device.

   - A separate cloud server is used to support firmware download and is operated by an in-house network security management team.

B. If you have downloaded the firmware, proceed with the firmware upgrade.

C. If you want to upgrade multiple devices, choose from the following method:

   - Parallel: Upgrade up to 16 devices simultaneously. The number of devices in progress can be changed.
   - Sequence: Upgrade one device at a time in sequence.

D. Schedule the date and time to automatically execute the firmware upgrade:

   - Relative time: The firmware upgrade will be executed after the selected time.
   - Absolute time: The firmware upgrade will be executed at the selected date and time.

> **Note**
>
> If the firmware window is closed, the upgrade cannot be performed at the scheduled time. The firmware window must remain open.

E. Download the latest firmware and proceed with the upgrade immediately. To execute this, select [Sequence] from [Upgrade multiple devices in] box.

> **Note**
>
> You can also perform a manual upgrade using firmware downloaded from a different source. Install the firmware acquired from a separate path on the PC with the Device Manager. Then, use [Open File] to locate the folder where the firmware is installed to proceed with the upgrade.

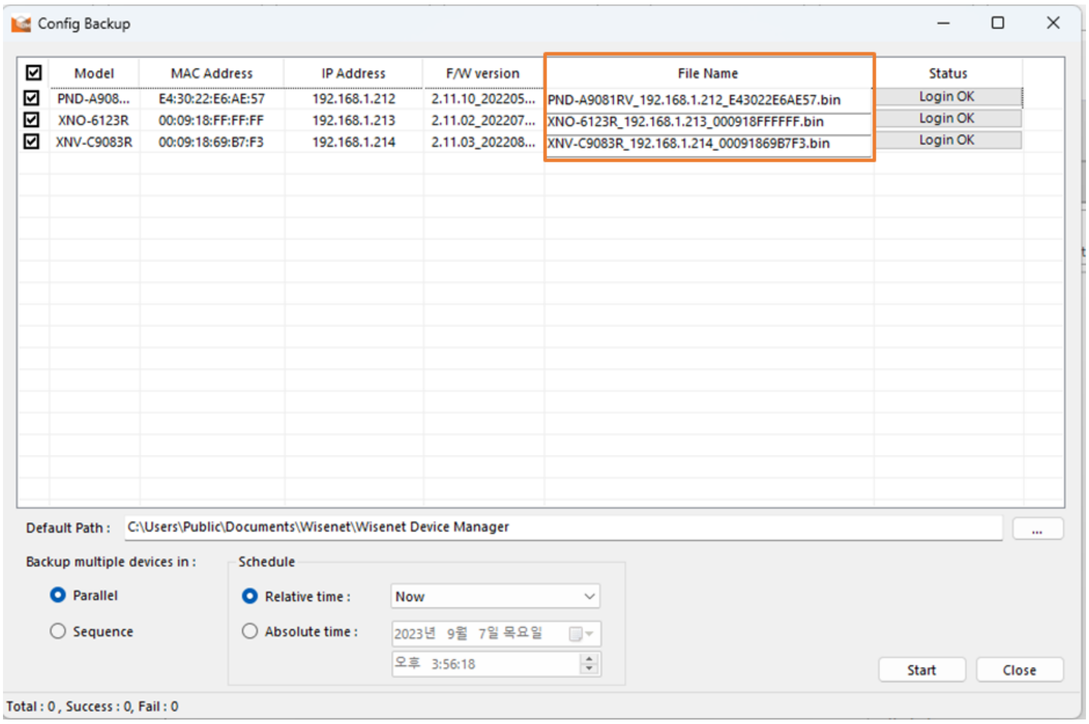
4.7. Backup and Restore Configuration

You can save or load device configuration information.

SUNAPI (HTTP(s) common protocol) is used for device configuration backup and restore.

Backup Configuration

1) Select the device you want to back up the configuration from the device list.
2) Click [Config] > [Config Backup].
3) The [Config Backup] window appears, and the backup file names of the devices are displayed.
4) After reviewing the backup file storage location, click [Start].



Config Backup

☑	Model	MAC Address	IP Address	F/W version	File Name	Status
☑	PND-A908...	E4:30:22:E6:AE:57	192.168.1.212	2.11.10_202205...	PND-A9081RV_192.168.1.212_E43022E6AE57.bin	Login OK
☑	XNO-6123R	00:09:18:FF:FF:FF	192.168.1.213	2.11.02_202207...	XNO-6123R_192.168.1.213_000918FFFFFF.bin	Login OK
☑	XNV-C9083R	00:09:18:69:B7:F3	192.168.1.214	2.11.03_202208...	XNV-C9083R_192.168.1.214_00091869B7F3.bin	Login OK

Default Path : C:\Users\Public\Documents\Wisenet\Wisenet Device Manager

Backup multiple devices in :
● Parallel
○ Sequence

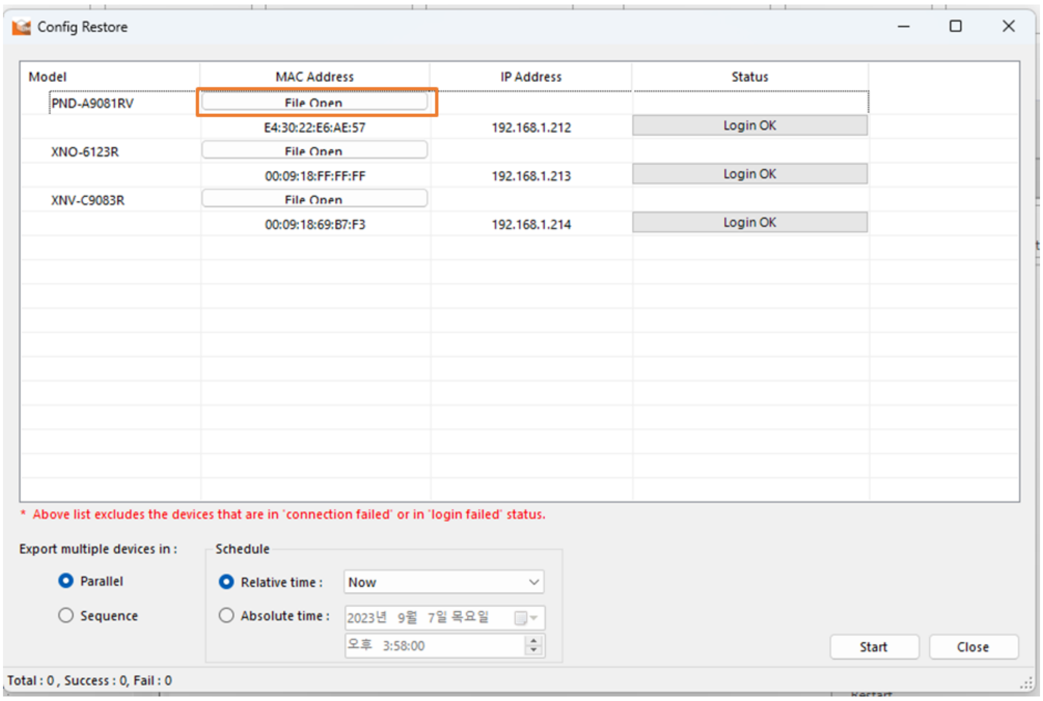
Schedule
● Relative time : Now
○ Absolute time : 2023년 9월 7일 목요일
오후 3:56:18

Total : 0 , Success : 0, Fail : 0

Restore Configuration

1) Select the device for which you want to restore the configuration from the device list.
2) Click [Config] > [Config Restore].

3) From the [Config Restore] window, select the device and click [File Open].



Model	MAC Address	IP Address	Status
PND-A9081RV	File Open		
	E4:30:22:E6:AE:57	192.168.1.212	Login OK
XNO-6123R	File Open		
	00:09:18:FF:FF:FF	192.168.1.213	Login OK
XNV-C9083R	File Open		
	00:09:18:69:B7:F3	192.168.1.214	Login OK

* Above list excludes the devices that are in 'connection failed' or in 'login failed' status.

Export multiple devices in :

● Parallel

○ Sequence

Schedule

● Relative time : Now

○ Absolute time : 2023년 9월 7일 목요일 오후 3:58:00

Total : 0 , Success : 0, Fail : 0

4) Choose the configuration file you want to apply.

Note

When backing up or restoring configuration for multiple devices, you can choose from the following method.

- Parallel: Backup or restore up to 16 devices simultaneously. The number of devices in progress can be changed.
- Sequence: Backup or restore one device at a time in sequence.

You can also schedule the date and time for configuration backup or restore to be executed:

- Relative time: The configuration backup or restore will be executed after the selected time.
- Absolute time: The configuration backup or restore will be executed at the selected date and time.

Note

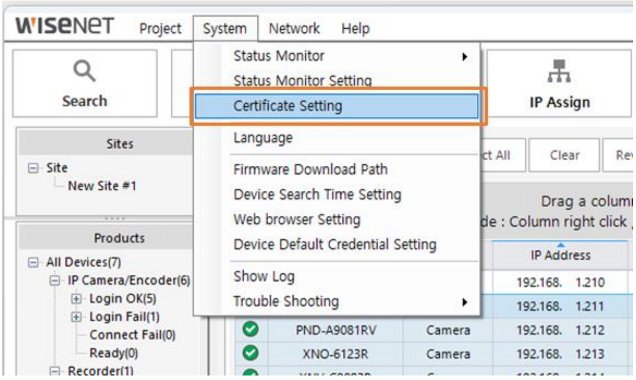
If the [Config Backup] or [Config Restore] window is closed, the backup or restore cannot be performed at the scheduled time. The [Config Backup] or [Config Restore] window must remain open.

4.8. Certificate Setting

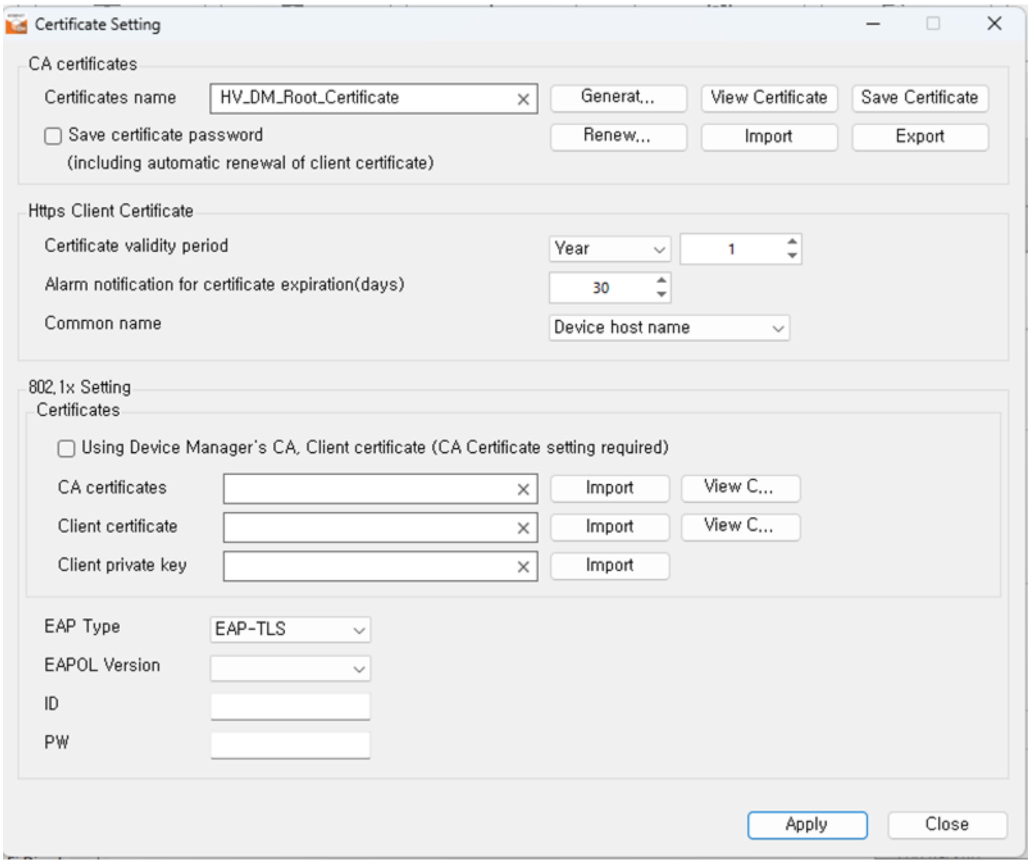
To open the [Certificate Setting] window, select [System] > [Certificate Setting].

Note

The certificate follows the ITU-T X509 v3 standard, which is part of the public key infrastructure (PKI). It uses the RSA and sha256 algorithms to encrypt signatures and keys and supports PKCS#1, PKCS#7, PKCS#8 and PKCS#12.



From the [Certificate Setting] window, you can set the certificates to be applied to HTTPS and 802.1x. The certificate setting is applied for each project.


Certificate Setting

CA certificates

Certificates name: HV_DM_Root_Certificate

□ Save certificate password
(including automatic renewal of client certificate)

Https Client Certificate

Certificate validity period: Year 1

Alarm notification for certificate expiration(days): 30

Common name: Device host name

802.1x Setting

Certificates

□ Using Device Manager's CA, Client certificate (CA Certificate setting required)

CA certificates:

Client certificate:

Client private key:

EAP Type: EAP-TLS

EAPOL Version:

ID:

PW:

4.8.1. CA Certificate

From the [CA Certificates] section in the [Certificate Setting] window, you can generate or renew a certificate or import certificate to continue using the existing certificate.

- **Generate Certificate**: Create a new certificate based on the provided password, nickname, and save configuration. If the certificate is successfully created, the name of the certificate will appear in the [Certificates name] input field.

- **View Certificate**: Review the information of the CA certificate that is currently applied.
- **Save Certificate**: Save the currently applied CA certificate in ".cer" or ".crt" file format.
- **Renew Certificate**: Renew the expiration date of the currently applied CA certificate.
- **Import Certificate**: Import the CA certificate in a ".pfx" or ".p12" file format.
- **Export Certificate**: Save the currently applied CA certificate in ".pfx" or ".p12" file format.

4.8.2. HTTPS Client Certificate

From the [HTTPS Client Certificate] section in the [Certificate Setting] window, you can configure the validity period and alarm notification for expiration and select the common name of the HTTPS client certificate.

- **Client Certificate Validity Period**: Set the validity period (up to 3 years) when creating a client certificate.
- **Alarm Notification for Certificate Expiration (Days)**: Display a reminder if the remaining validity period is less than the set days.
- **Common Name**: Select the naming method (Device IP address or Device Hostname) when creating the client certificate.

> Note
>
> You can import CA certificates, client certificates, and client keys. You can also specify additional settings related to them in advance.

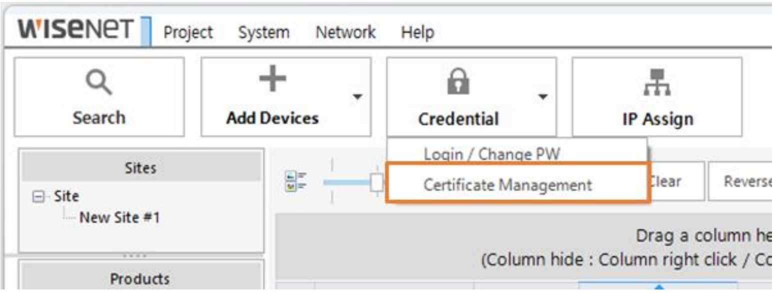
4.8.3. 802.1x Certificate Setting

From the [802.1x Setting] section in the [Certificate Setting] window, you can import CA certificates, client certificates, and client keys. You can also specify additional settings related to them in advance.

- You can use the CA and client certificates generated by the Device Manager. (In this case, a CA certificate setting is required.)
- You can import a CA or client certificate not issued by the Device Manager.
- You can import a client private key.
- You can select EAP-TLS, LEAP, or PEAPv0/MSCHAPv2 for EAP type.
- You can set the EAPOL Version (f1 or 2).
- You can enter the ID and password of the certificate.

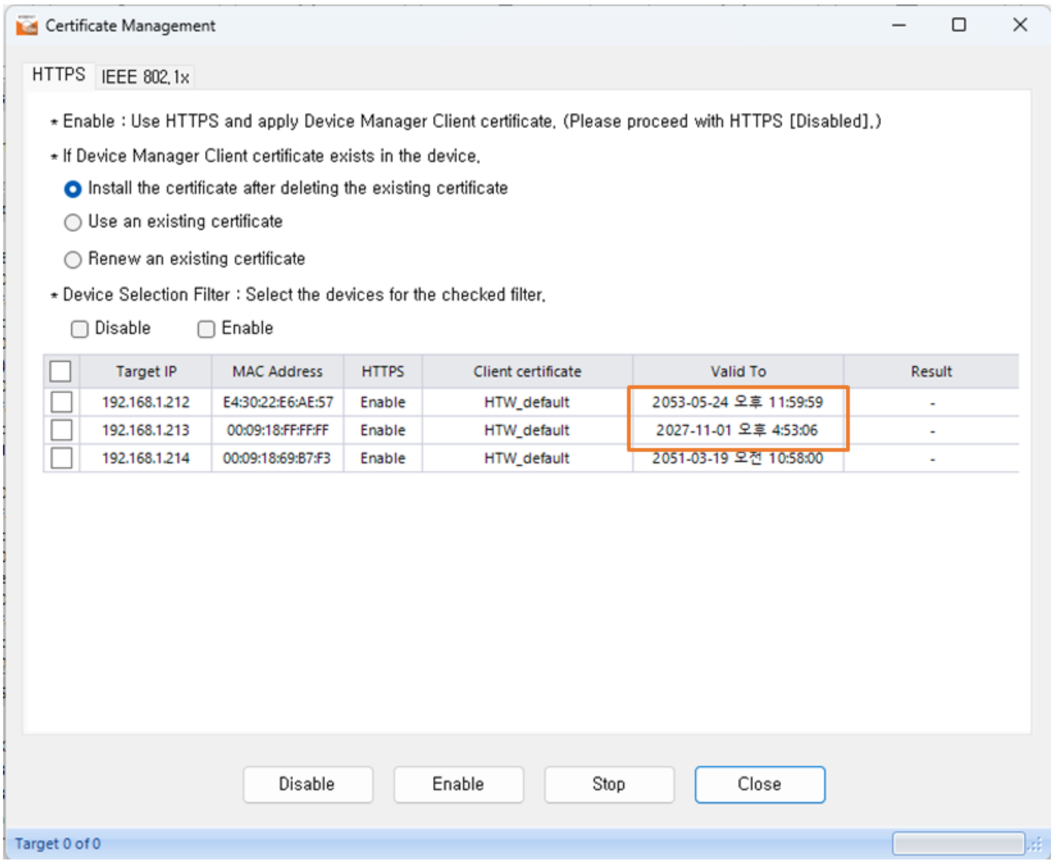
4.9. Certificate Management

To open the [Certificate Management] window, select [Credential] > [Certificate Management].



This feature allows you to configure the usage of HTTPS and 802.1x certificates and manage the validity period.

SUNAPI (HTTP(s) common protocol) is used for CA to manage client certificates.



- Enable : Use HTTPS and apply Device Manager Client certificate. (Please proceed with HTTPS [Disabled].)
- If Device Manager Client certificate exists in the device.

● Install the certificate after deleting the existing certificate

○ Use an existing certificate

○ Renew an existing certificate

- Device Selection Filter : Select the devices for the checked filter.

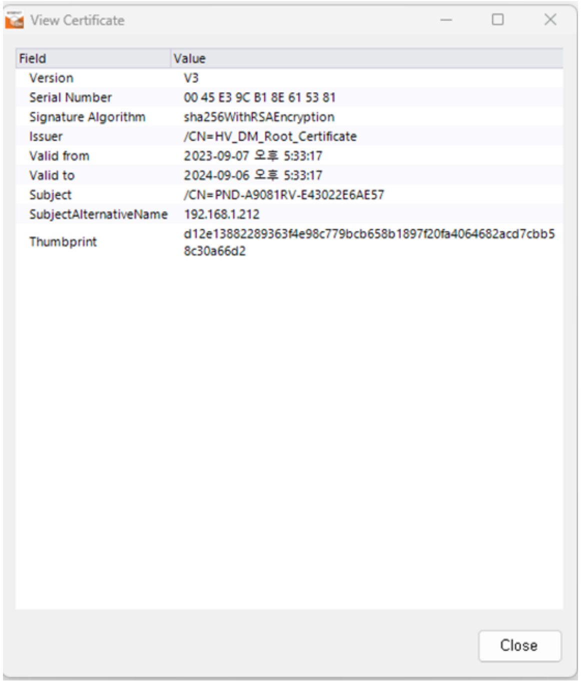
□ Disable □ Enable

□	Target IP	MAC Address	HTTPS	Client certificate	Valid To	Result
□	192.168.1.212	E4:30:22:E6:AE:57	Enable	HTW_default	2053-05-24 오후 11:59:59	-
□	192.168.1.213	00:09:18:FF:FF:FF	Enable	HTW_default	2027-11-01 오후 4:53:06	-
□	192.168.1.214	00:09:18:69:B7:F3	Enable	HTW_default	2051-03-19 오전 10:58:00	-

4.9.1. HTTPS Setting

From the [HTTPS] tab in the [Certificate Management] window, you can set the way Device Manager's client certificate is applied based on HTTPS.

- If Device Manager's client certificate exists within the device:
  - **Install the Certificate After Deleting Existing Certificate**: Remove the existing Device Manager client certificate and issue and install a new one.
  - **Use an Existing Certificate**: Continue using the existing Device Manager client certificate.
  - **Renew an Existing Certificate**: Renew the validity period of the existing Device Manager client certificate.
- **Device Selection Filter**: You can select multiple devices that are checked from the list at once. If the device requires individual configuration, select the left checkbox next to the device on the list. Double-click on the client certificate cell on the list, or right-click and select [View Client Certificate] to view the certificate information.



Field	Value
Version	V3
Serial Number	00 45 E3 9C B1 8E 61 53 81
Signature Algorithm	sha256WithRSAEncryption
Issuer	/CN=HV_DM_Root_Certificate
Valid from	2023-09-07 오후 5:33:17
Valid to	2024-09-06 오후 5:33:17
Subject	/CN=PND-A9081RV-E43022E6AE57
SubjectAlternativeName	192.168.1.212
Thumbprint	d12e13882289363f4e98c779bcb658b1897f20fa4064682acd7cbb58c30a66d2

Buttons in the [HTTPS] tab under the [Certificate Management] window.

- **Disable**: Disable HTTPS for the selected devices.
- **Enable**: Enable HTTPS and apply the client certificate for the selected devices.
- **Stop**: Stop all ongoing operations.
- **Close**: Close the [Certificate Management] window.

Note

> The CA certificate must be configured from the [Certificate Setting] to be able to use the HTTPS certificate management feature. For certain devices, you may not be able to check certificate information.

4.9.2. IEEE 802.1x Configuration

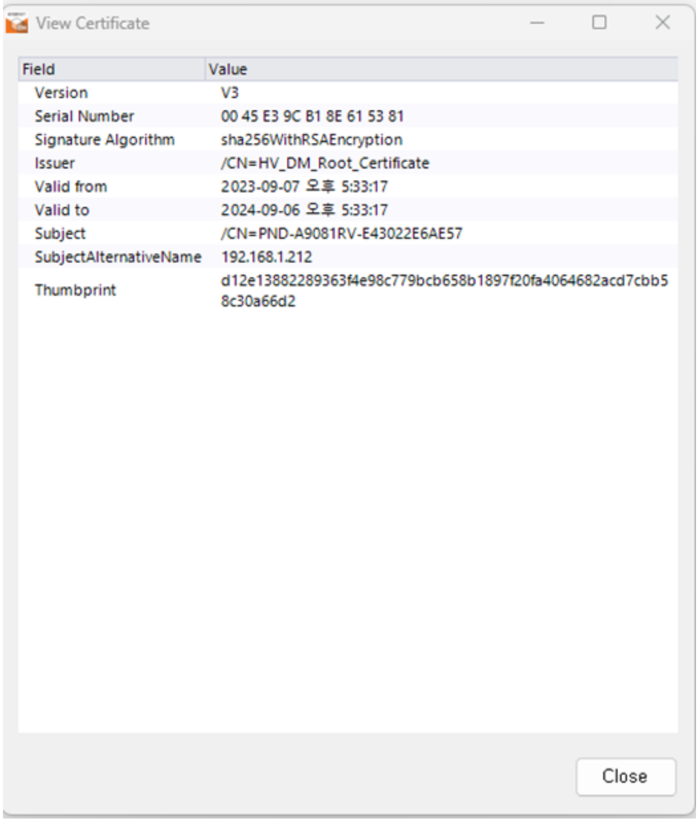
From the [IEEE 802.1x] tab in the [Certificate Management] window, you can set the way Device Manager's CA or client certificate is applied based on IEEE 802.1x.

- If Device Manager's client certificate exists within the device:

  The feature is enabled only when the [Using Device Manager's CA, Client Certificate (CA Certificate Setting Required)] option is selected from the [802.1x Setting] > [Certificates] section in the [Certificate Setting] window.

  - **Install the Certificate After Deleting Existing Certificate**: Remove the existing Device Manager certificate and issue and install a new one.
  - **Use an Existing Certificate**: Remove the existing Device Manager certificate and issue and install a new one.

- **Device Selection Filter**: You can select multiple devices that are checked from the list at once. Double-click on the client certificate cell on the list, or right-click and [View Client Certificate] or [View CA Certificate] to view the certificate information.



Field	Value
Version	V3
Serial Number	00 45 E3 9C B1 8E 61 53 81
Signature Algorithm	sha256WithRSAEncryption
Issuer	/CN=HV_DM_Root_Certificate
Valid from	2023-09-07 오후 5:33:17
Valid to	2024-09-06 오후 5:33:17
Subject	/CN=PND-A9081RV-E43022E6AE57
SubjectAlternativeName	192.168.1.212
Thumbprint	d12e13882289363f4e98c779bcb658b1897f20fa4064682acd7cbb58c30a66d2

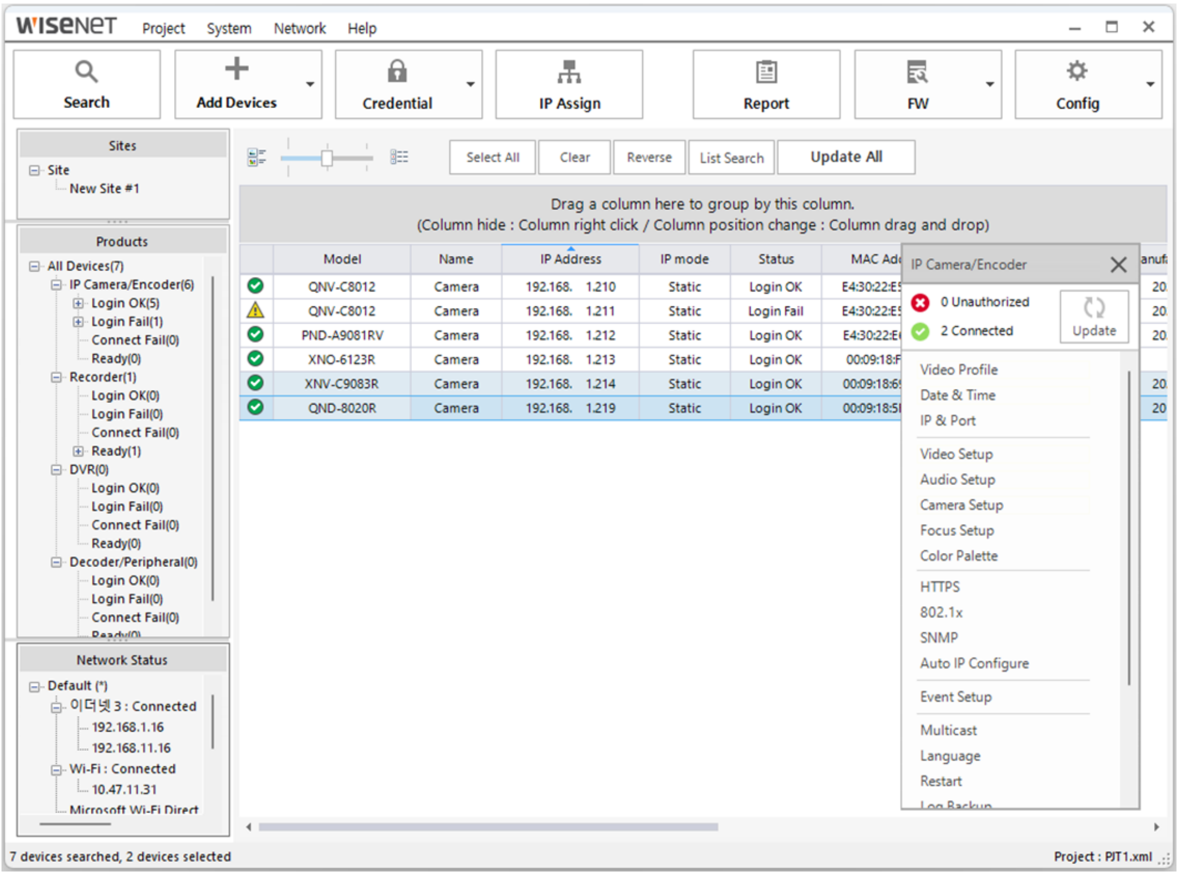
Buttons in the [IEEE 802.1x] tab under the [Certificate Management] window.

- **Disable**: Disable 802.1x for the selected devices.
- **Enable**: Enable 802.1x and apply the certificate for the selected devices.
- **Stop**: Stop all ongoing operations.
- **Close**: Close the [Certificate Management] window.

> **Note**
>
> When using the Device Manager certificate, you cannot use the same client certificate simultaneously with HTTPS. For certain devices, you may not be able to check certificate information.

4.10. Device Setup

When a device is selected from the device list, clicking the (+) button at the top reveals the device setup menu supported by the device. The items in the setup menu may vary depending on the device.



Drag a column here to group by this column.
(Column hide : Column right click / Column position change : Column drag and drop)

	Model	Name	IP Address	IP mode	Status	MAC Ad	anuf
✓	QNV-C8012	Camera	192.168. 1.210	Static	Login OK	E4:30:22:E	20
⚠	QNV-C8012	Camera	192.168. 1.211	Static	Login Fail	E4:30:22:E	20
✓	PND-A9081RV	Camera	192.168. 1.212	Static	Login OK	E4:30:22:E	20
✓	XNO-6123R	Camera	192.168. 1.213	Static	Login OK	00:09:18:F	
✓	XNV-C9083R	Camera	192.168. 1.214	Static	Login OK	00:09:18:6	20
✓	QND-8020R	Camera	192.168. 1.219	Static	Login OK	00:09:18:5	20

7 devices searched, 2 devices selected

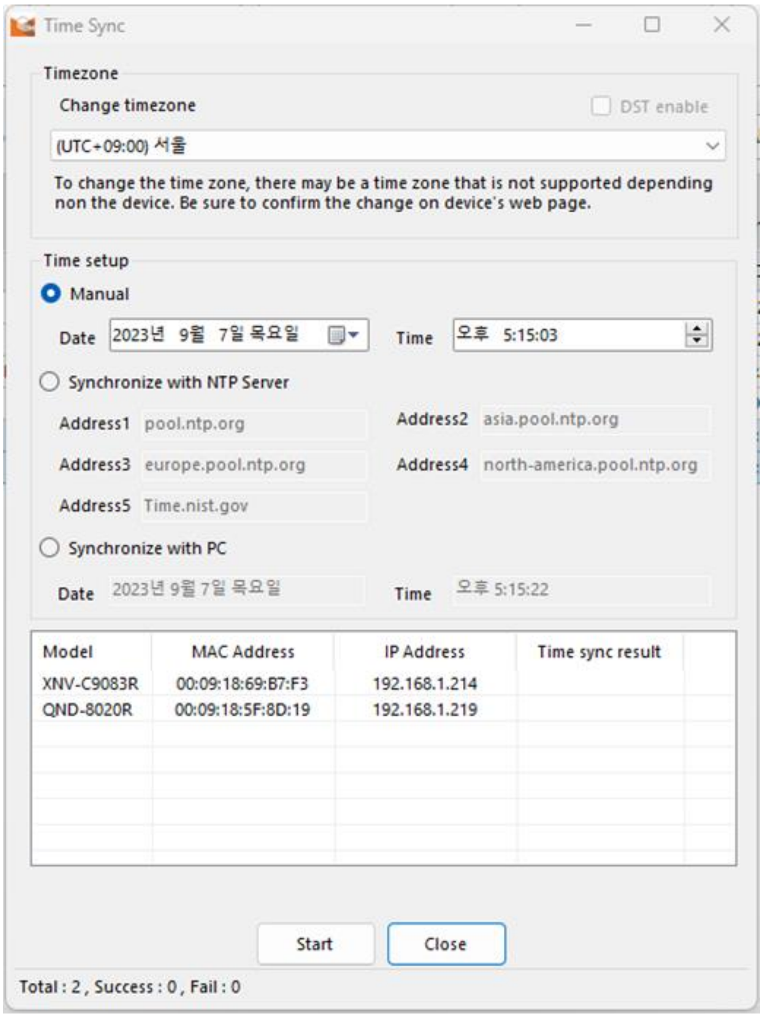
Project : PJT1.xml

4.10.1. Video Profile

From the video profile, items such as codecs, frame rates, resolutions, and bitrates for the device can be configured. You can also add, delete, or modify profiles. Available options may differ depending on the device.

4.10.2. Date & Time

Configure the date and time of the device. Time information can be configured for multiple devices at the same time. Available options include:



Timezone

Change timezone ☐ DST enable

(UTC+09:00) 서울

To change the time zone, there may be a time zone that is not supported depending non the device. Be sure to confirm the change on device's web page.

Time setup

● Manual

Date 2023년 9월 7일 목요일 Time 오후 5:15:03

○ Synchronize with NTP Server

Address1 pool.ntp.org Address2 asia.pool.ntp.org

Address3 europe.pool.ntp.org Address4 north-america.pool.ntp.org

Address5 Time.nist.gov

○ Synchronize with PC

Date 2023년 9월 7일 목요일 Time 오후 5:15:22

Model	MAC Address	IP Address	Time sync result
XNV-C9083R	00:09:18:69:B7:F3	192.168.1.214	
QND-8020R	00:09:18:5F:8D:19	192.168.1.219	

Total : 2 , Success : 0 , Fail : 0

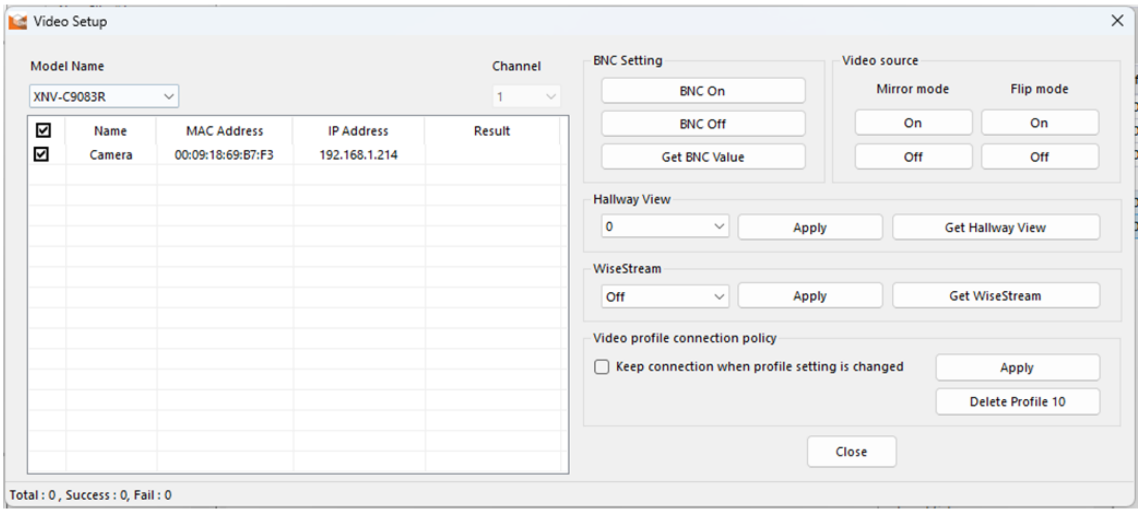
- Timezone: Set based on standard time zones.
- Manual: Manually input date and time information for the device.
- Synchronize with NTP Server: Synchronize date and time through an NTP server.
- Synchronize with PC: Synchronize the date and time with the PC where Device Manager is installed.

4.10.3. IP & Port

View the device IP and other information and set the hostname. The input field is disabled for devices that do not support the hostname setting.

4.10.4. Video Setup

Configure video input, output, compression, and more. Available options may vary depending on the device.



Video Setup

Model Name: XNV-C9083R

Channel: 1

☑	Name	MAC Address	IP Address	Result
☑	Camera	00:09:18:69:B7:F3	192.168.1.214	

Video source — Mirror mode: On / Off; Flip mode: On / Off

Hallway View: 0

WiseStream: Off

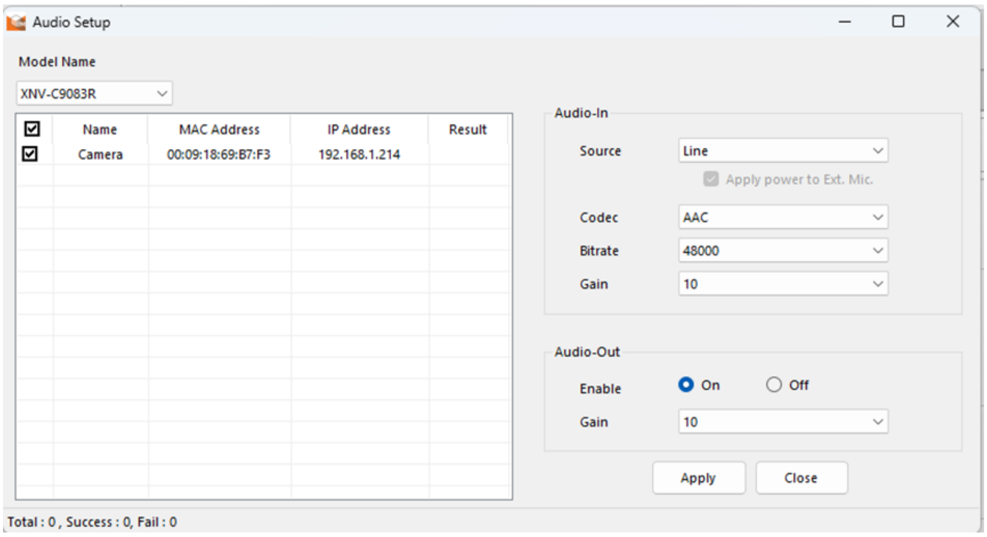
Video profile connection policy: □ Keep connection when profile setting is changed

Total : 0 , Success : 0, Fail : 0

- BNC Setting: Set analog video (BNC) output for the camera.
- Video Source: Set flip or mirror mode for the video.
- Hallway View: Rotate the video to adjust the monitoring area to fit the hallway.
- WiseStream: Adjust the level of video compression.

4.10.5. Audio Setup

Configure audio input and output for the device. Available options may vary depending on the device.



Audio Setup

Model Name: XNV-C9083R

☑	Name	MAC Address	IP Address	Result
☑	Camera	00:09:18:69:B7:F3	192.168.1.214	

Audio-In

Source: Line

☑ Apply power to Ext. Mic.

Codec: AAC

Bitrate: 48000

Gain: 10

Audio-Out

Enable: ● On ○ Off

Gain: 10

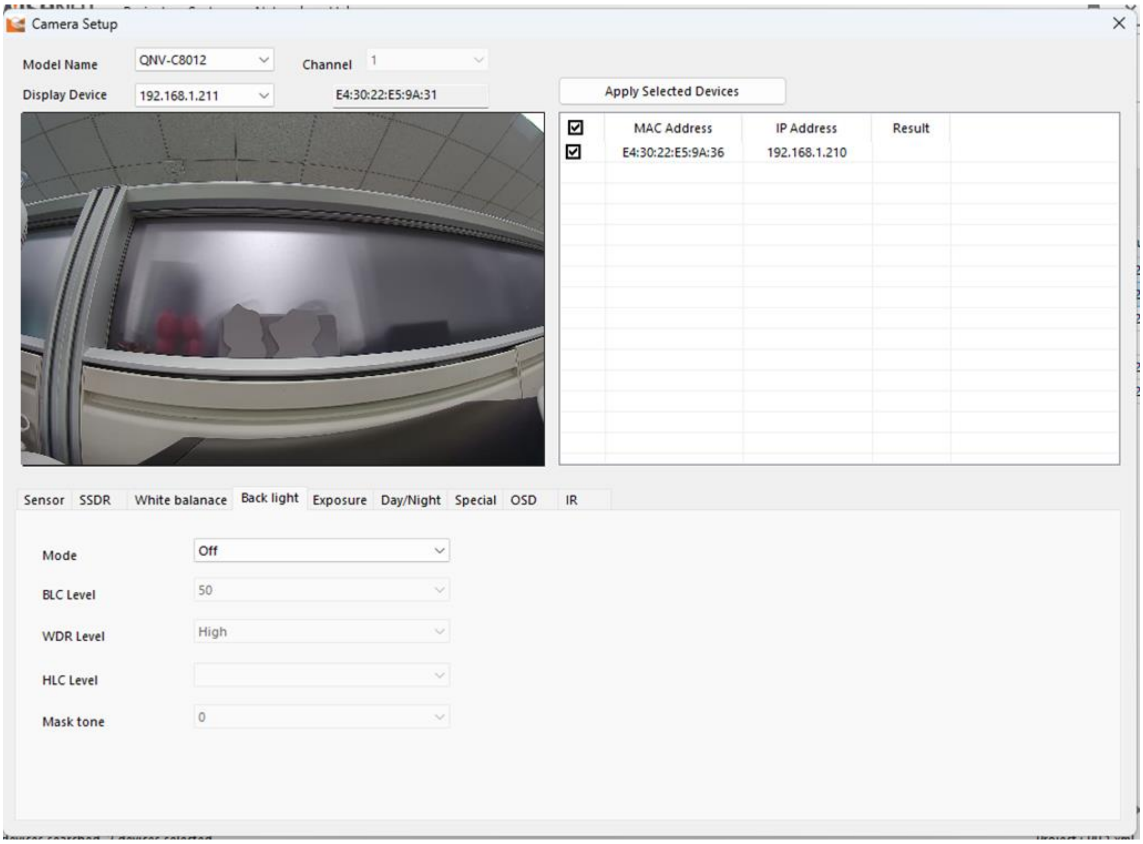
Total : 0 , Success : 0, Fail : 0

- Audio-in: Set the audio input method, choosing from Internal MIC, External MIC, or Line options.
- Codec: Set the audio codec, choosing from G.711, G.726, or AAC options.

- Gain: Set the amplification value for audio input, ranging from 1 to 10. The higher the value, the greater the amplification.
- Audio-out: Enable or disable audio output.

4.10.6. Camera Setup

Adjust the camera settings to fit the installed environment. Enabled features and available options may vary depending on the device.



Model Name: QNV-C8012

Channel: 1

Display Device: 192.168.1.211 — E4:30:22:E5:9A:31

☑	MAC Address	IP Address	Result
☑	E4:30:22:E5:9A:36	192.168.1.210	

Mode: Off

BLC Level: 50

WDR Level: High

HLC Level:

Mask tone: 0

- Sensor: Set the sensor mode (frames per second) for capturing video.
- SSDR: Configure the SSDR feature to balance the overall brightness in high-contrast lighting conditions by enhancing the brightness in darker areas. Increasing the level will further brighten the dark areas.
- White Balance: Correct the image based on white color to ensure the colors look natural regardless of the lighting conditions.
- Back Light: Compensate the backlight in an environment with a contrast between bright and dark areas to ensure visibility on both sides. Settings such as BLC, WDR, and HLC levels can be adjusted.
- Exposure: Modify exposure levels based on the installed environment of the device. Settings such as brightness, minimum and maximum shutter speed, anti-flicker, SSNR level, and iris focal length can be configured.

- Day/Night: Change video output between color and black-and-white based on the installed environment of the device. Mode, duration, dwell time, and alarm input can be configured.
- Special: Settings such as sharpness level, gamma, color level, fog calibration, and DIS can be configured.
- OSD: Display the title or date/time on the video screen and set display positions.
- IR: Select and set levels for IR LED mode.

4.10.7. Focus Setup

Configure the focus of the device. The availability of this feature may vary depending on the device.

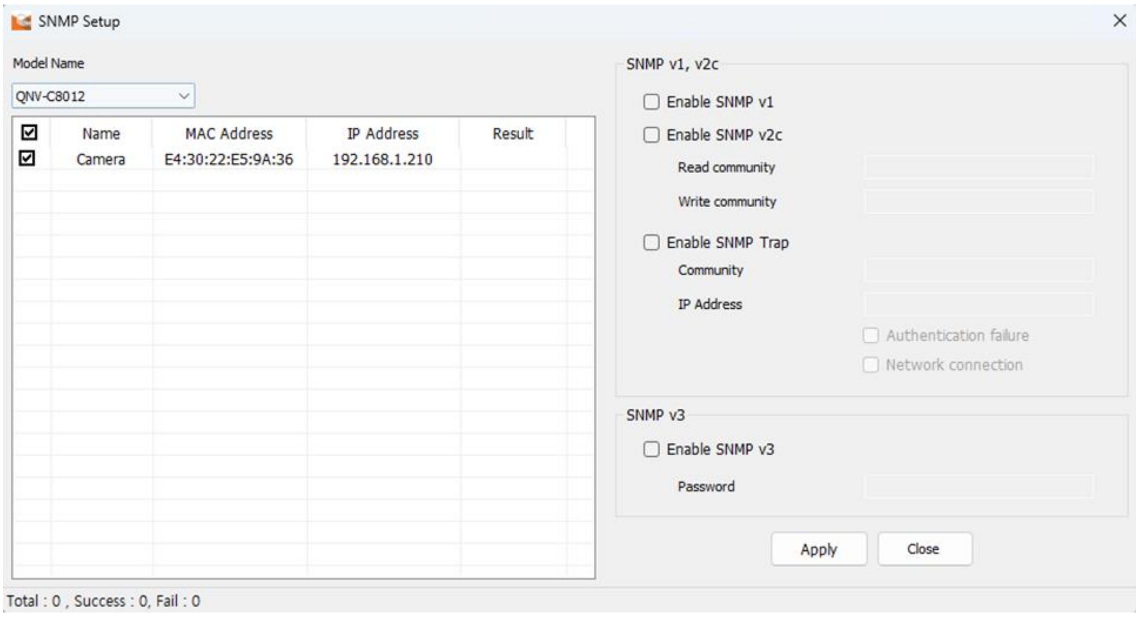
- Focus Initialize: The focus setting is initialized.
- Simple Focus: The focus is automatically adjusted.

4.10.8. Color Palette

Configure the color palette of the thermal camera. This feature is only available for thermal cameras.

4.10.9. SNMP

Set the SNMP protocol for the device. This enables remote monitoring and management by the system or network administrator. SNMP v1, v2, and v3 options are available.



Model Name: QNV-C8012

☑	Name	MAC Address	IP Address	Result
☑	Camera	E4:30:22:E5:9A:36	192.168.1.210	

☐ Enable SNMP v1

☐ Enable SNMP v2c

☐ Enable SNMP Trap

☐ Authentication failure

☐ Network connection

☐ Enable SNMP v3

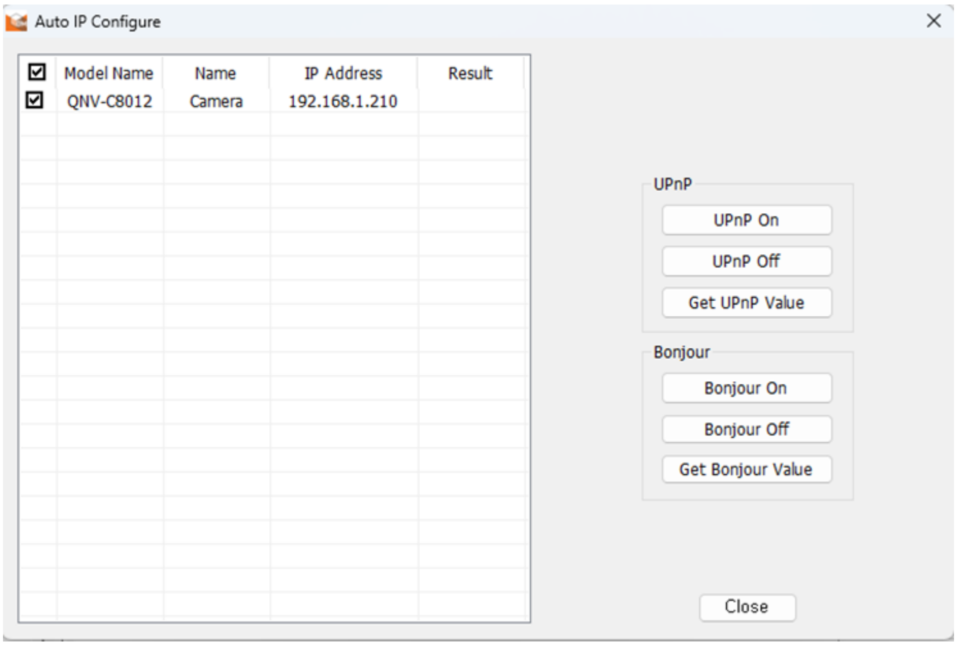
Total : 0 , Success : 0, Fail : 0

- SNMP v1: Basic feature with minimal security functions.
- SNMP v2: Data and authentication security algorithms are added, and bandwidth utilization is more efficient than SNMP v1. Selecting this option will activate read and write community, allowing input of respective community names.

- SNMP Trap: Send important events and statuses to the management system. This option will activate the community, IP address, and event occurrence condition (authentication failure and link connection).
- SNMP v3: Encrypted packets are used to prevent unauthorized access to data. User passwords can be set by selecting the option.

4.10.10. Auto IP Configuration

Automatically configure the device’s connection and discoverable IP. You can choose between the UPnP and Bonjour protocols.



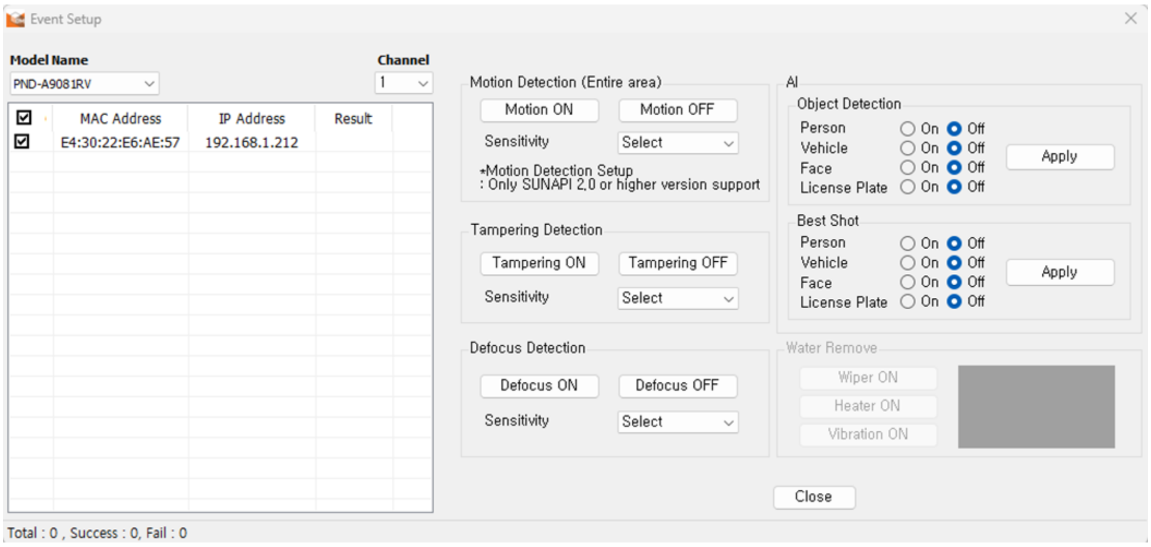
Auto IP Configure

☑	Model Name	Name	IP Address	Result
☑	QNV-C8012	Camera	192.168.1.210	

- UPnP (Universal Plug and Play): Search devices automatically from clients and operating systems that support UPnP. Devices connected to the network are displayed on Windows OS that supports UPnP.
- Bonjour: Search devices automatically from clients and operating systems that support Bonjour. On Mac OS that supports Bonjour, devices connected to the network are displayed on the Safari web browser bookmark.

4.10.11. Event Setup

Configure features related to event detection. The configured settings apply to the entire screen.



Model Name: PND-A9081RV

Channel: 1

☑	MAC Address	IP Address	Result
☑	E4:30:22:E6:AE:57	192.168.1.212	

Motion Detection (Entire area)

Sensitivity: Select

*Motion Detection Setup
: Only SUNAPI 2.0 or higher version support

Tampering Detection

Sensitivity: Select

Defocus Detection

Sensitivity: Select

AI

Object Detection

Person	○ On	● Off
Vehicle	○ On	● Off
Face	○ On	● Off
License Plate	○ On	● Off

Best Shot

Person	○ On	● Off
Vehicle	○ On	● Off
Face	○ On	● Off
License Plate	○ On	● Off

Water Remove

Total : 0 , Success : 0, Fail : 0

- Motion Detection: Trigger the event when motion is detected and adjust the sensitivity level. Higher sensitivity will result in better detection of events even in environments with unclear distinctions between background and objects.
- Tampering Detection: Trigger the event when the screen is covered or the camera position changes.
- Defocus Detection: Trigger the event when the camera's focus is blurred.
- AI: Trigger the object detection event when the object specified by the user is detected. Types of objects (person, vehicle, face, and license plate) and the best shot feature can be selected.
- PTZ Water Remove: Enable the wiper function of the PTZ camera.

4.10.12. Multicast

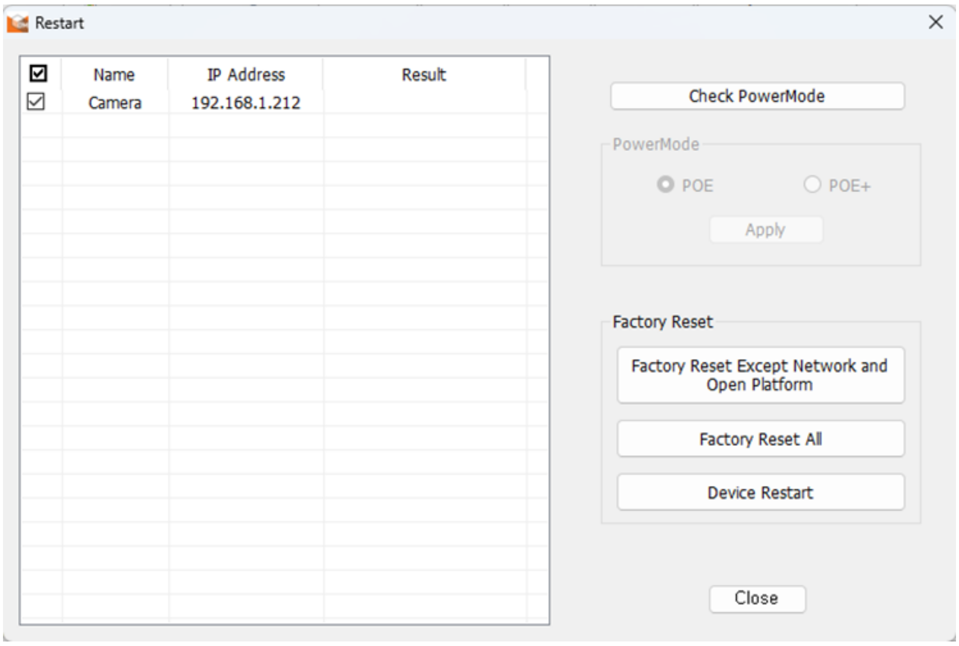
Configure multicast settings with this feature. You can turn the feature on or off and set the IP Address and Port.

4.10.13. Language

This feature allows you to set the web viewer language.

4.10.14. Restart

You can set power mode, perform a factory reset, and restart the device.

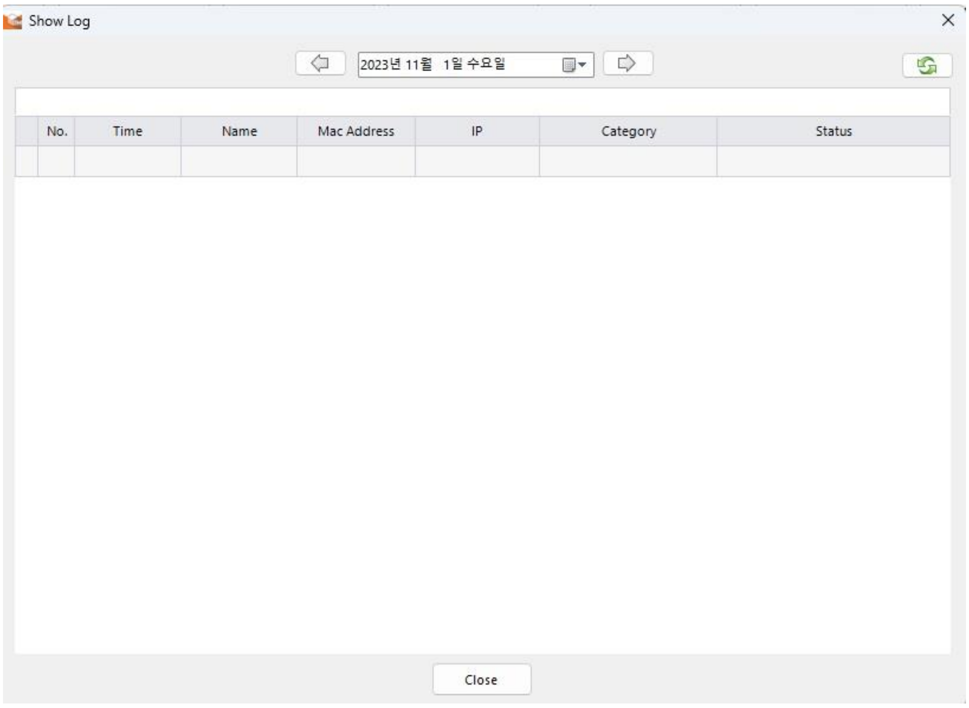


☑	Name	IP Address	Result
☑	Camera	192.168.1.212	

PowerMode: ● POE ○ POE+

4.10.15. Show Log

Each device's system, event, and access log information can be viewed.

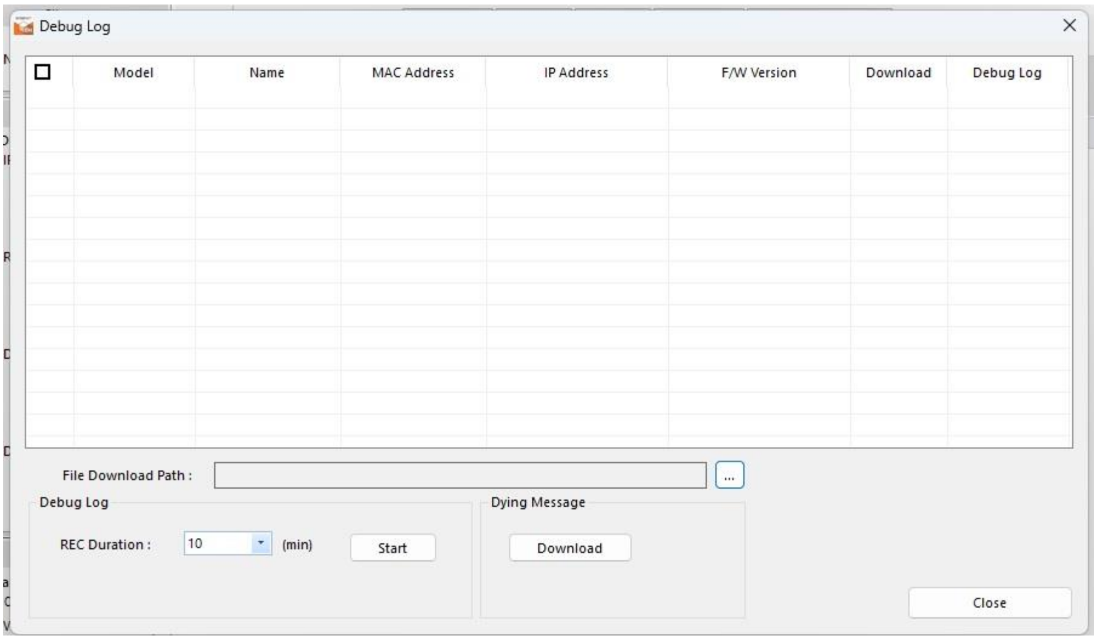


2023년 11월 1일 수요일

No.	Time	Name	Mac Address	IP	Category	Status

4.10.16. Debug Log

Selected device’s debug log can be collected, which has specific operation. It can be also downloaded as csv file format, with supporting selection of downloading path. Recording duration is minimum 10 minutes and up to 60 minutes, by 10 minutes gradually.



Debug Log

□	Model	Name	MAC Address	IP Address	F/W Version	Download	Debug Log

File Download Path :

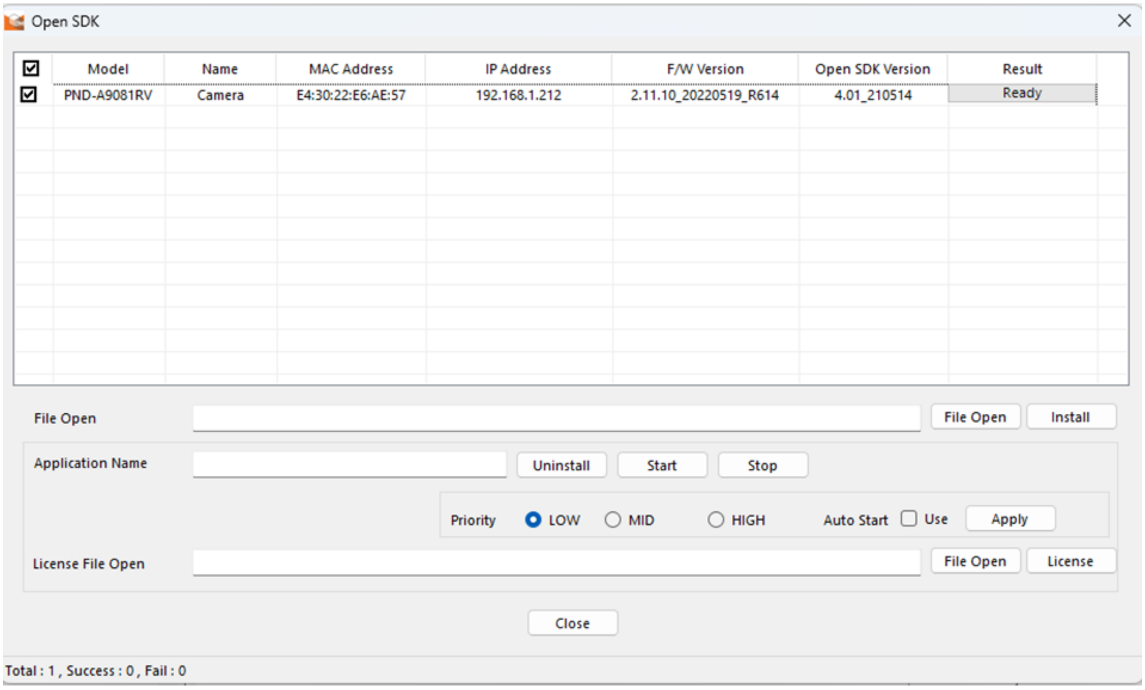
Debug Log

REC Duration : 10 (min)

Dying Message

4.10.17. Open Platform

You can install, uninstall, start, or stop the open platform application on the device.



Open SDK

☑	Model	Name	MAC Address	IP Address	F/W Version	Open SDK Version	Result
☑	PND-A9081RV	Camera	E4:30:22:E6:AE:57	192.168.1.212	2.11.10_20220519_R614	4.01_210514	Ready

File Open

Application Name

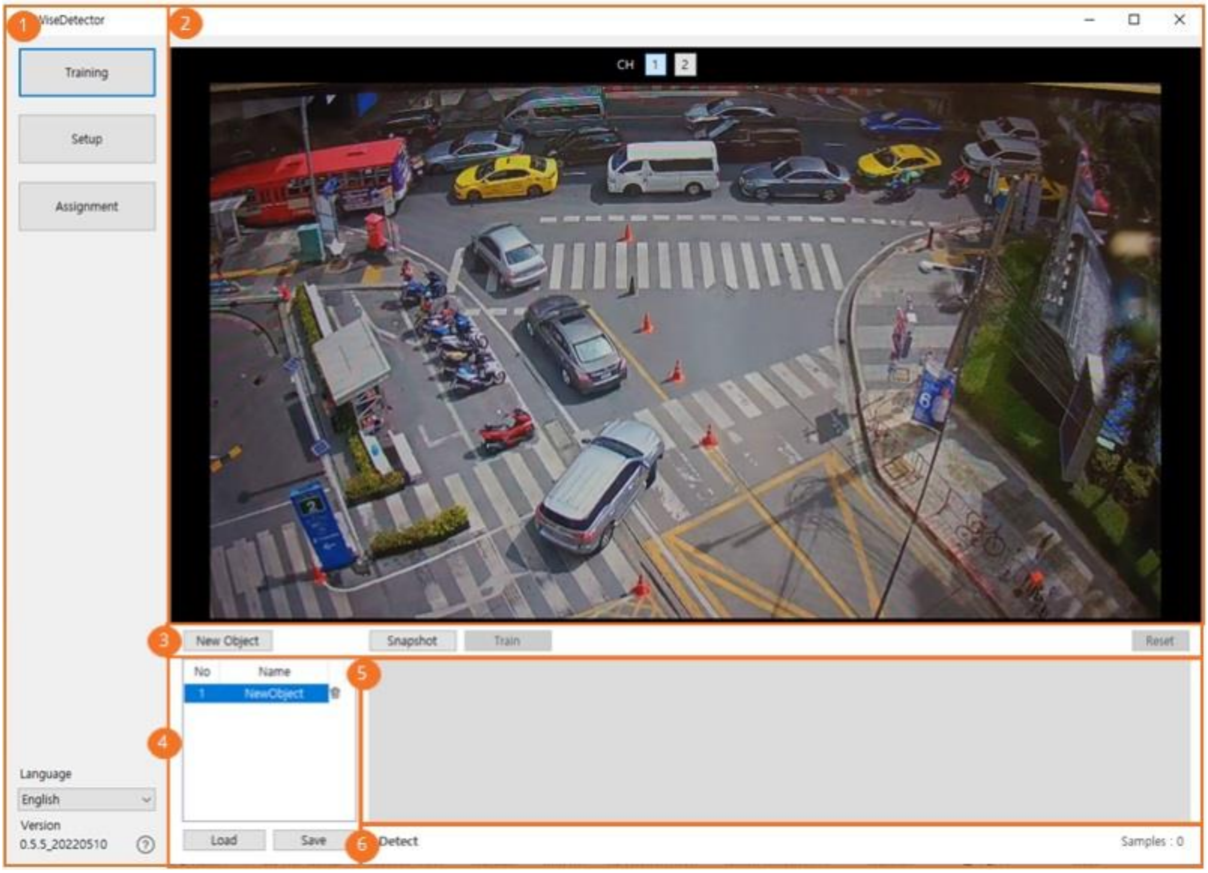
Priority ● LOW ○ MID ○ HIGH Auto Start □ Use

License File Open

Total : 1 , Success : 0 , Fail : 0

4.10.18. WiseDetector

WiseDetector is a new feature designed to help cameras detect objects after the users select the objects they want and train the camera to detect them.



① Menu: View program features and version

② View video: Display the connected camera video

③ Training features button: Provide features about training

④ Manage Objects: Display the object list and management features

⑤ Training Images: Display training sample images

⑥ Display Count: Display several samples and the number of detected objects

5. Conclusion

Device Manager is an intuitive program that allows users to efficiently manage and monitor multiple devices simultaneously in various locations without the burden of configuring devices individually. The ability to group devices according to their intended purposes further enhances user convenience by allowing them to manage the devices collectively in the system.

Hanwha Vision continuously updates the Device Manager to ensure seamless compatibility and configuration for the newly released lineup each year. There are also plans to provide ongoing support to facilitate the configuration and management of various devices in the future.

Hanwha Vision Co., Ltd.
13488 Hanwha Vision R&D Center,
6 Pangyo-ro 319-gil, Bundang-gu, Seongnam-si, Gyeonggi-do
TEL 070.7147.8771-8
FAX 031.8018.3715
www.HanwhaVision.com