WISeNeT Mutual Authentication Guide for Devices User Guide

Contents

WISeNeT

WISeNeT Mutual Authentication Guide for Devices

Hanwha Techwin devices are equipped with mutual authentication functions to ensure secure communication between devices. This guide provides information on how to set up mutual authentication between devices.

What is mutual authentication?

Mutual authentication is a secure process in which the server and client authenticate each other before encrypted communication takes place. This is achieved by providing a device certificate and authentication function to prove their identity.

Mutual authentication is a two-way authentication. It is actually a secure process in which the server and client authenticate each other before encrypted communication takes place.
To this end, in the network environment, both the server and the client must be able to provide a device certificate and authentication function to prove their identity.

Hanwha Techwin's latest devices are equipped with a device certificate and provide a mutual authentication function. This provides the ability to restrict or check invalid server or client connections.

- **How to check supported models**

  To check the model equipped with the device certificate
  - https://www.hanwha-security.com > Product > Product specification > Network > Security > Device Certificate (Hanwha Techwin Root CA, preinstalled)

Server authentication is supported from NVR (Intel-based) and SSM Appliance*SSM v2.10.7 or later products, and client authentication is supported from WN7 X series model.

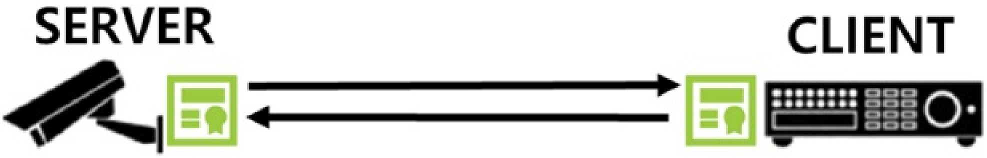
Mutual authentication between Camera and Video recorder

Follow the steps below to set up mutual authentication between Camera and Video recorder:

1. Connect the camera where the device certificate is installed and the video storage.
2. In the camera, set HTTPS and mutual authentication mode.
3. In the video storage device, register the camera with manual registration and set mutual authentication mode.
4. Check the authentication result on the video storage set live screen for camera authentication result and in the camera web browser based on the camera access client IP address for video storage authentication result.

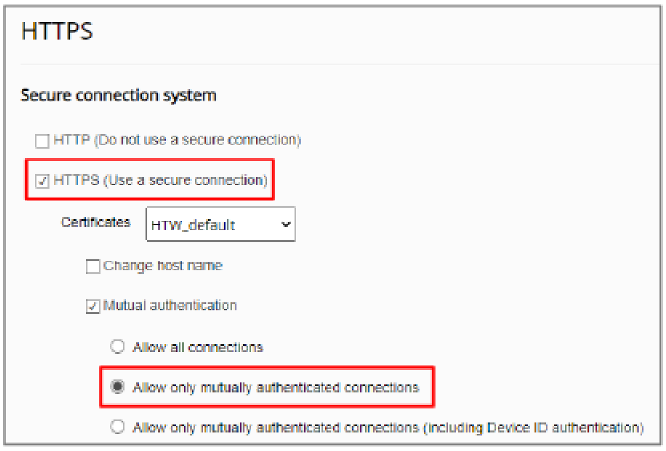
How to connect and set up

Connect the camera where the device certificate is installed and the video storage.



Camera setup

1. The camera sets HTTPS and mutual authentication mode as follows.
   - Check "HTTPS"
   - Select certificates as HTW-default
   - Check "Mutual Authentication" & select "Allow only mutually authenticated connections".



HTTPS

Secure connection system

☐ HTTP (Do not use a secure connection)

☑ HTTPS (Use a secure connection)

Certificates: HTW_default

☐ Change host name

☑ Mutual authentication

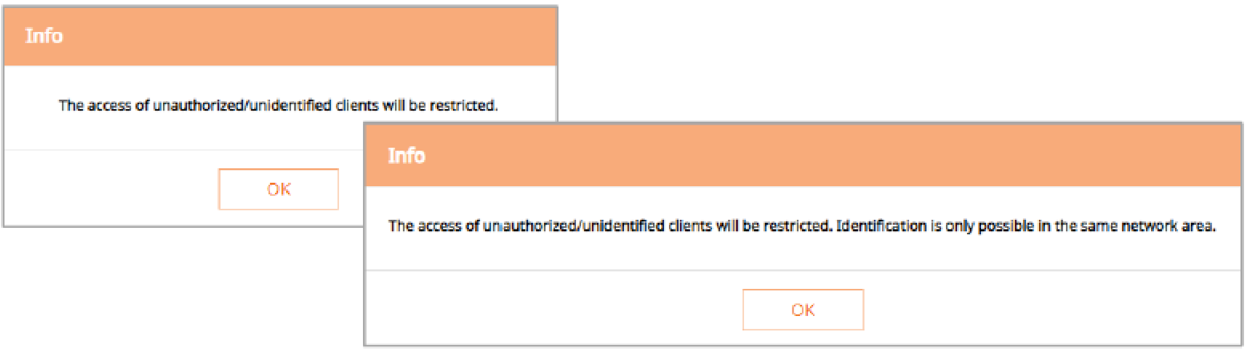
○ Allow all connections

● Allow only mutually authenticated connections

○ Allow only mutually authenticated connections (including Device ID authentication)

- Mutual authentication options(Server: Camera / Client: Video storage, SSM)
  1. **Allow all connections**
     The server allows encrypted communication with the client regardless of whether or not the authentication of the certificate delivered from the client is successful. However, whether the authentication was successful or not can be checked based on the IP of the client connected to the server.
  2. **Allow only mutually authenticated connections**
     The server determines whether or not to allow the client to access the server according to the success of the authentication of the certificate received from the client. At this time, authentication checks whether the client's certificate is a certificate issued by Hanwha and whether the validity period has expired.
     When authentication fails, encrypted communication between the server and the client is terminated.
  3. **Allow only mutually authenticated connections (including Device ID authentication)**
     The server determines whether or not to allow the client to access the server according to whether the authentication of the certificate delivered from the client is successful. At this time, authentication checks whether the client's certificate is a certificate issued by Hanwha and whether the validity period has expired. Also make sure it matches the client's MAC address. If authentication fails, the encrypted communication between the server and the client is terminated.

Mutual authentication after releasing HTTP mode If you select ② or ③ options, web browser access becomes impossible, and connection is possible after factory reset of the camera.



Info

The access of unauthorized/unidentified clients will be restricted.

OK

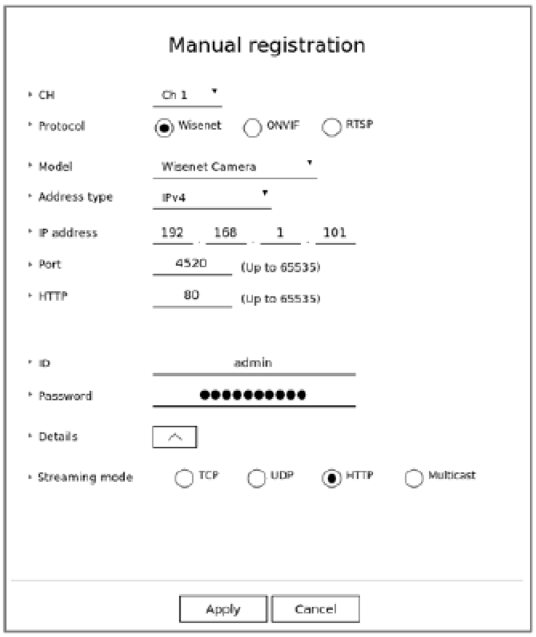
Info

The access of unauthorized/unidentified clients will be restricted. Identification is only possible in the same network area.

OK

Video storage setup

1. When registering a camera in the storage device, set as follows.
   - Only Manual registration is supported with Mutual Authentication.



Manual registration

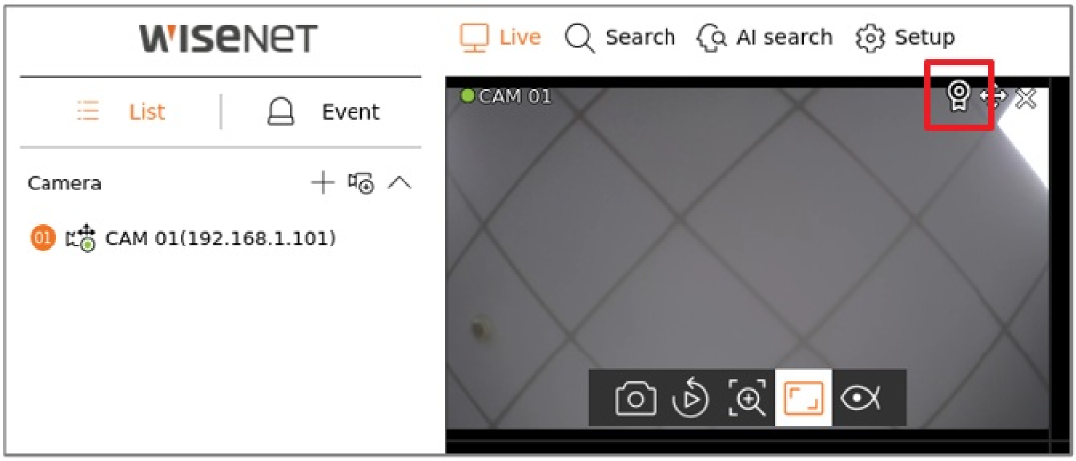
- CH: Ch 1
- Protocol: ● Wisenet ○ ONVIF ○ RTSP
- Model: Wisenet Camera
- Address type: IPv4
- IP address: 192 . 168 . 1 . 101
- Port: 4520 (Up to 65535)
- HTTP: 80 (Up to 65535)
- ID: admin
- Password: ●●●●●●●●●●●
- Details
- Streaming mode: ○ TCP ○ UDP ● HTTP ○ Multicast

  - **Protocol:** Wisenet
  - **HTTP:** 80
  - **Streaming mode:** HTTP

Device authentication result

- **Camera authentication result**

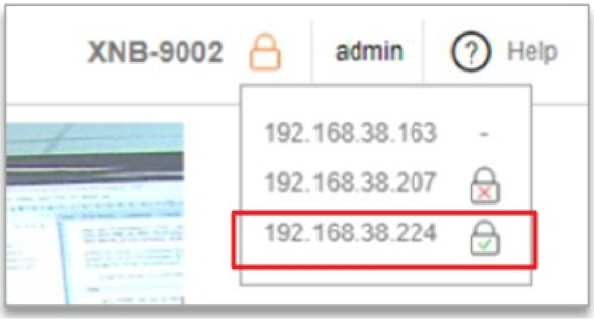
  You can check the camera authentication result on the video storage set live screen as follows.



- **Video storage authentication result**

  The authentication result for the video storage device can be checked in the camera web browser based on the camera access client IP address.

  - When set to “Only allow mutually authenticated connections” mode, encrypted communication is possible only with clients equipped with device certificates. It is impossible to check the storage device authentication result through a web browser, and success or failure can be determined because the encrypted communication between the camera and the storage device has not been terminated. However, if you want to temporarily check the authentication result through a web browser for convenience, you can check the authentication result on the web browser screen as follows if you additionally set the HTTP mode in the camera.
    - In case of web browser access through HTTP mode, it is not encrypted communication, so be careful about security.



No lock(-): No certificate (HTTP mode)

Red lock( ): Certificates that do not support device authentication (authentication failed)

Green lock( ): Certificate that supports device authentication (authentication successful

- In case of connection to a storage device that supports device authentication (192.168.38.224), the success of mutual authentication is confirmed through the green lock.
- In case of connection to a storage device that does not support device authentication (192.168.38.207), check the failure of mutual authentication through a red lock.
- In case of web browser access without certificate (192.068.38.163), there is no lock mark

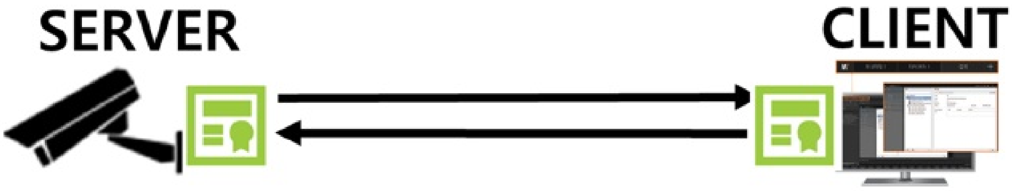
Mutual authentication between Camera and SSM Appliance

Follow the steps below to set up mutual authentication between Camera and SSM Appliance:

1. Connect the camera where the device certificate is installed and the SSM Appliance.
2. In the camera, set HTTPS and mutual authentication mode.
3. In the SSM Appliance, add the camera with mutual authentication mode.
4. Check the authentication result on the SSM Appliance.

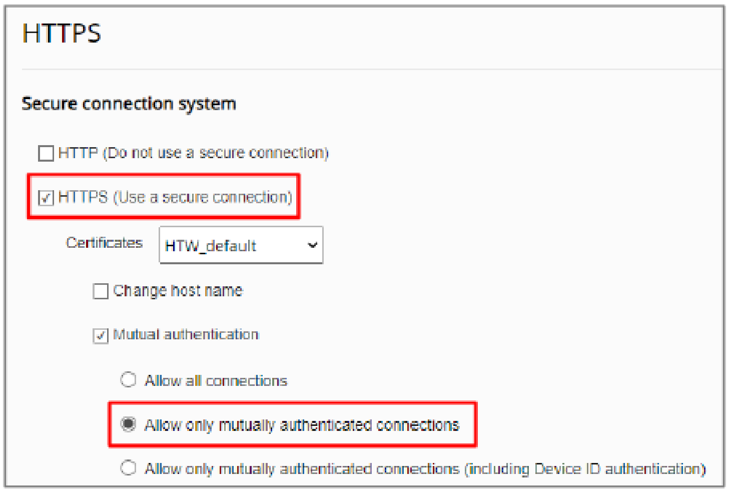
How to connect and set up

Connect the camera where the device certificate is installed and SSM Appliance.



Camera setup

1. The camera sets HTTPS and mutual authentication mode as follows.
    - Check “HTTPS”
    - Select certificates as HTW-default
    - Check “Mutual Authentication” & select “Allow only mutually authenticated connections”



HTTPS

Secure connection system

□ HTTP (Do not use a secure connection)

☑ HTTPS (Use a secure connection)

Certificates: HTW_default

□ Change host name

☑ Mutual authentication

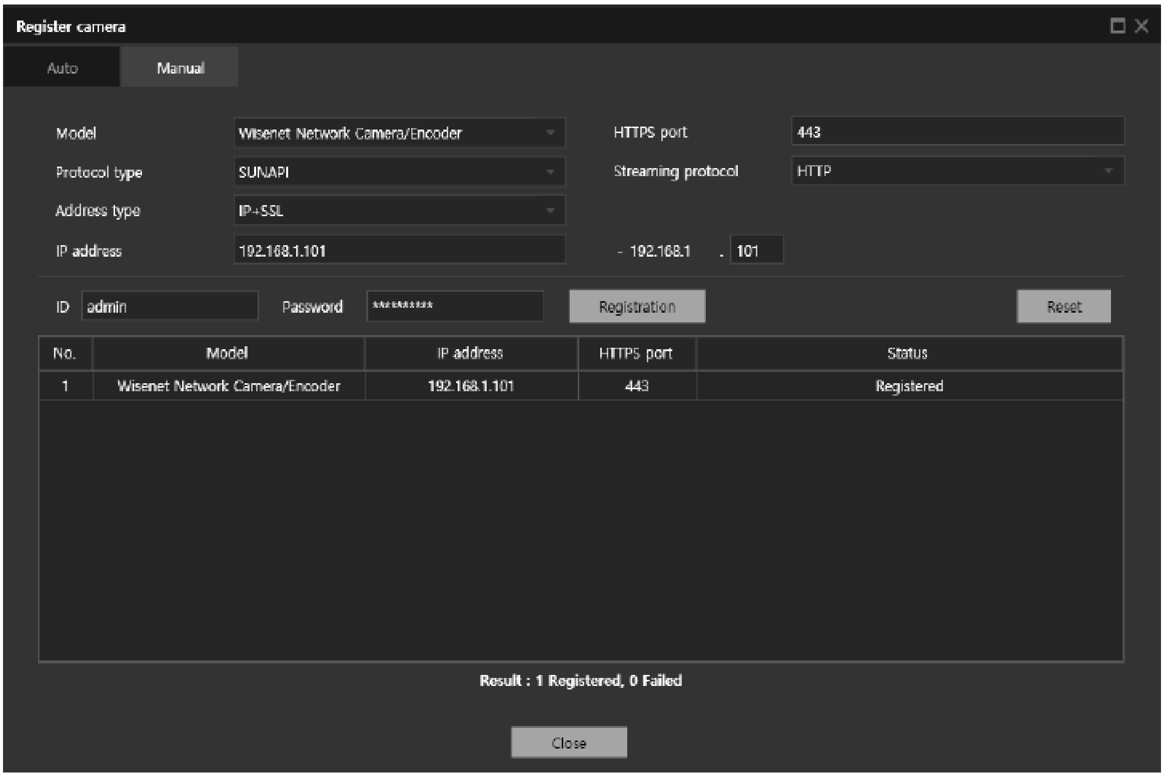
○ Allow all connections

● Allow only mutually authenticated connections

○ Allow only mutually authenticated connections (including Device ID authentication)

SSM Appliance setup

1. When registering a camera manually in SSM Appliance, set as follows.
   - If the mutual authentication option used for registration is changed during camera authentication, re-registration is required. If it is not changed, it can be omitted.
     1. **Protocol:** SUNAPI
     2. **Network:** IP + SSL
     3. **HTTPS:** 443
     4. **Streaming Protocol:** HTTP



Register camera

Auto | Manual

Model	Wisenet Network Camera/Encoder	HTTPS port	443
Protocol type	SUNAPI	Streaming protocol	HTTP
Address type	IP+SSL		
IP address	192.168.1.101	- 192.168.1	. 101

ID: admin Password: ********* Registration Reset

No.	Model	IP address	HTTPS port	Status
1	Wisenet Network Camera/Encoder	192.168.1.101	443	Registered

Result : 1 Registered, 0 Failed

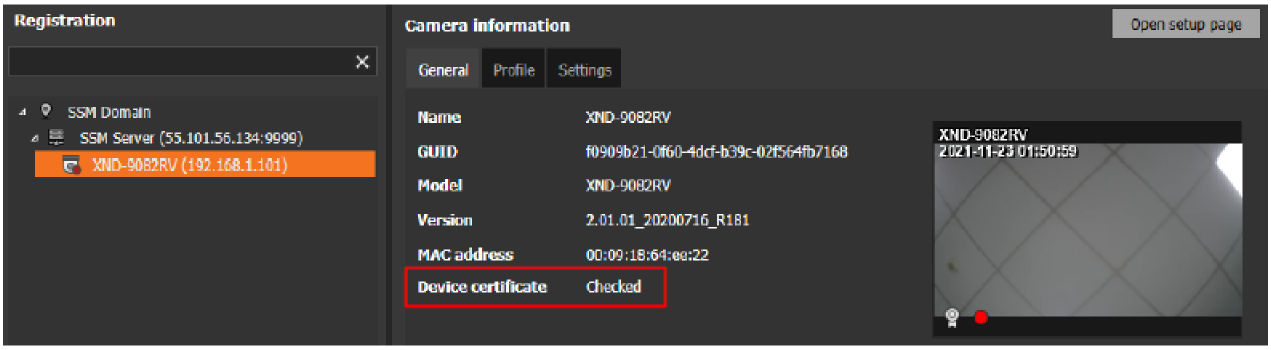
Close

Device authentication result

- **Camera authentication result**

  “SSM Appliance > Camera information > General” Check the camera authentication result on the menu screen.

  When the camera authentication is successful, the device certificate is displayed as verified.



Camera information

Name XND-9082RV

GUID f0909b21-0f60-4dcf-b39c-02f564fb7168

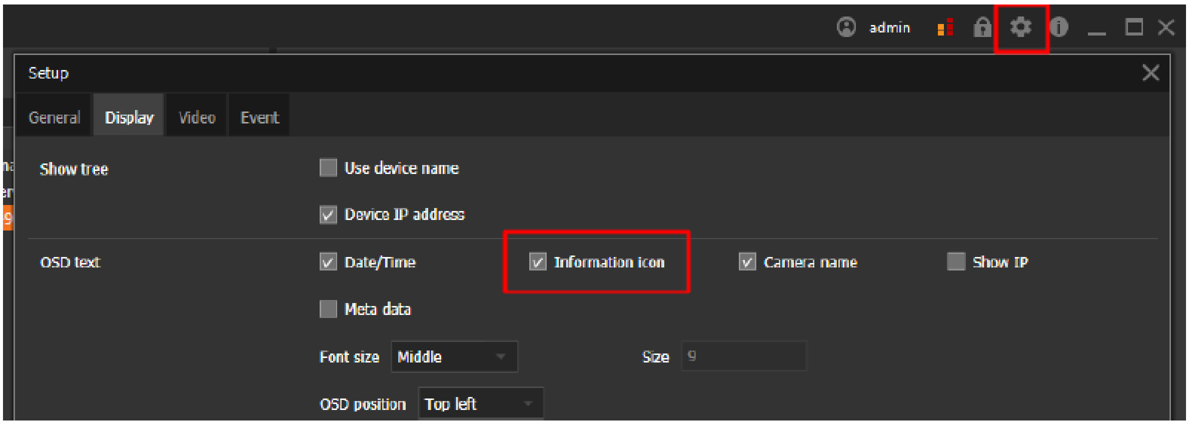
Model XND-9082RV

Version 2.01.01_20200716_R181

MAC address 00:09:18:64:ee:22

Device certificate Checked

- If the device certificate icon is not visible, set as follows.
  - Setup > Display > OSD text > Information Icon



Show tree ☐ Use device name

☑ Device IP address

OSD text ☑ Date/Time ☑ Information icon ☑ Camera name ☐ Show IP

☐ Meta data

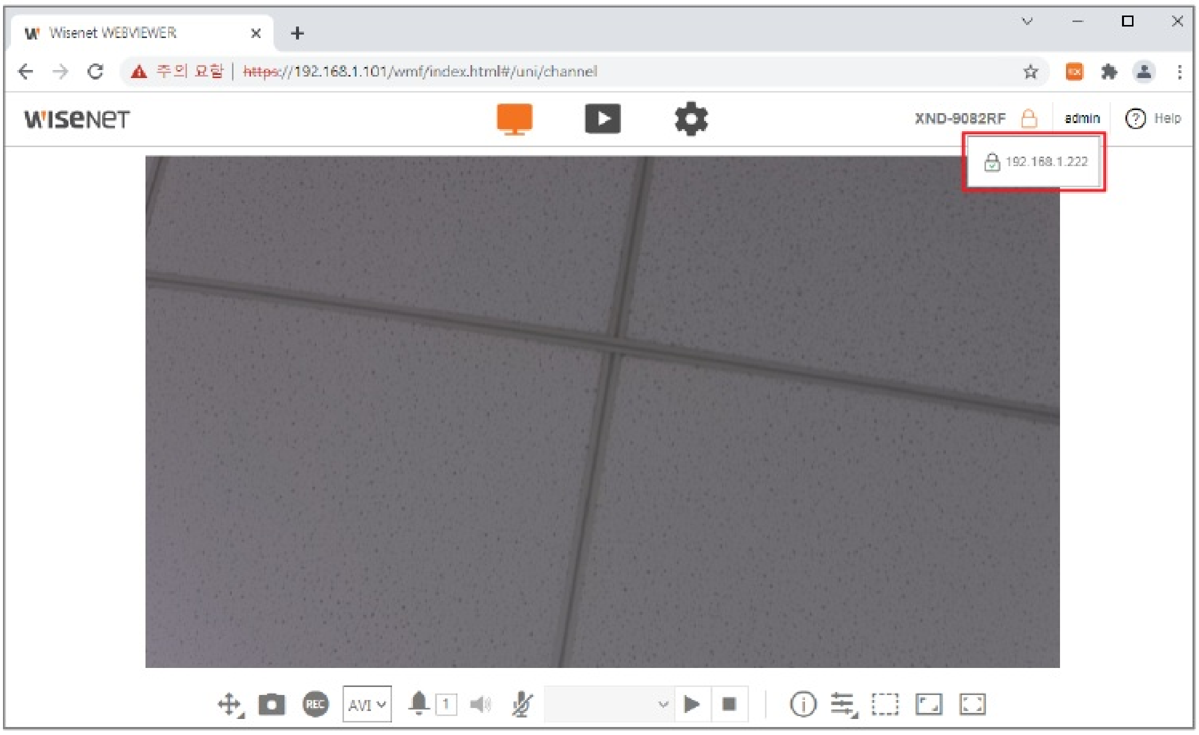
Font size Middle Size 9

OSD position Top left

- **SSM Appliance authentication result**

  The authentication result for SSM Appliance can be checked in the camera web browser based on the client IP address connected to the camera.

  - However, authentication results through a web browser can be checked only when HTTP mode is additionally set in the camera.
  - In case of web browser access through HTTP mode, it is not encrypted communication, so be careful about security.



No lock (-): No certificate (HTTP mode)

Red lock ( ): Certificates that do not support device authentication (authentication failed)

Green lock ( ): Certificate that supports device authentication (authentication successful)

- In case of SSM Appliance connection (192.168.1.222) that supports device authentication, the success of mutual authentication is confirmed through the green lock.

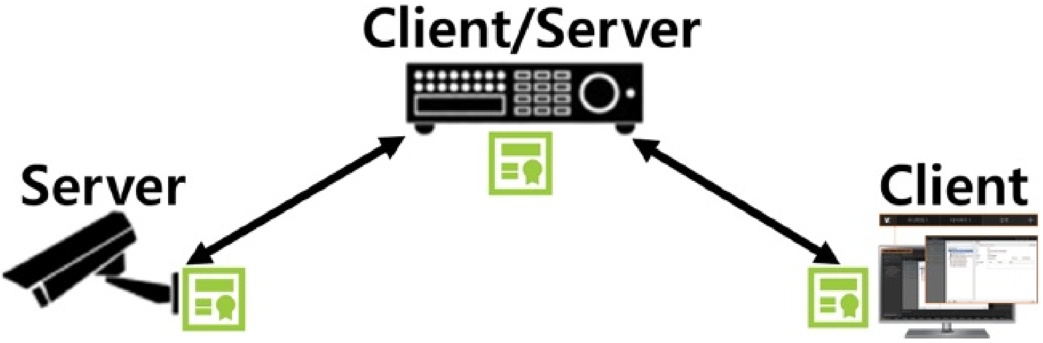
Mutual authentication between Video recorder and SSM Appliance

Follow the steps below to set up mutual authentication between Video recorder and SSM Appliance:

1. Connect the Video recorder and SSM Appliance.
2. In the Video recorder, set HTTPS and mutual authentication mode.
3. In the SSM Appliance, set mutual authentication mode.
4. Check the authentication result on the SSM Appliance.

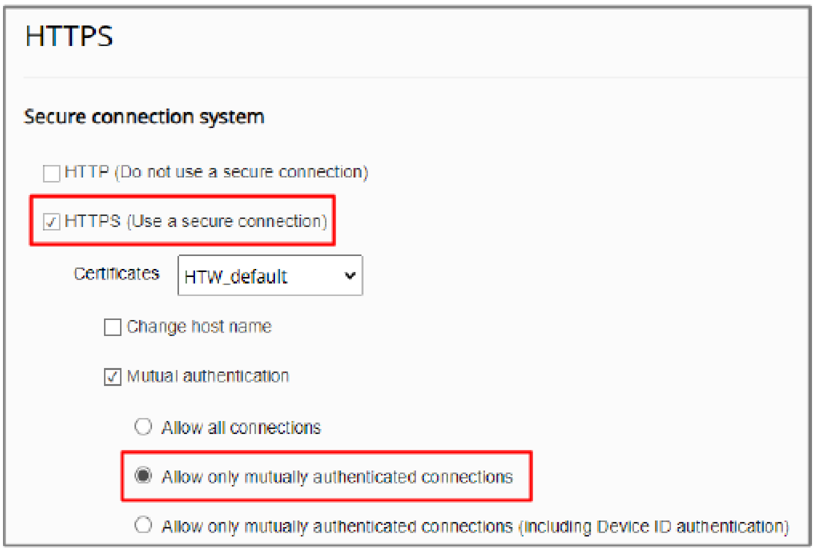
How to connect and set up

Connect the camera, storage device and SSM Appliance where the device certificate is installed.



Camera setup

1. The camera sets HTTPS and mutual authentication mode as follows.
    - Check “HTTPS”
    - Select certificates as HTW-default
    - Check “Mutual Authentication” & select “Allow only mutually authenticated connections”



HTTPS

Secure connection system

☐ HTTP (Do not use a secure connection)

☑ HTTPS (Use a secure connection)

Certificates: HTW_default

☐ Change host name

☑ Mutual authentication

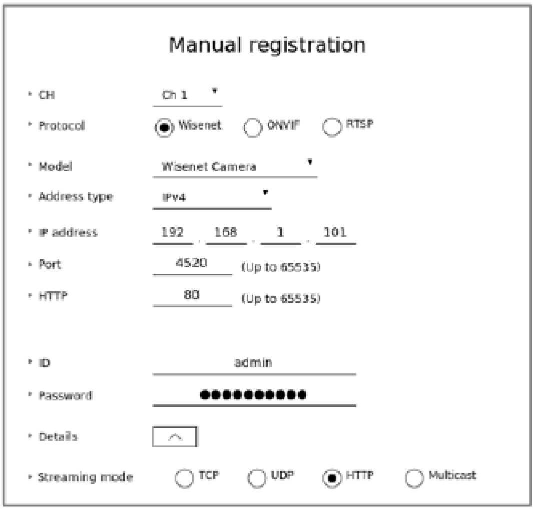
○ Allow all connections

● Allow only mutually authenticated connections

○ Allow only mutually authenticated connections (including Device ID authentication)

Video storage setup

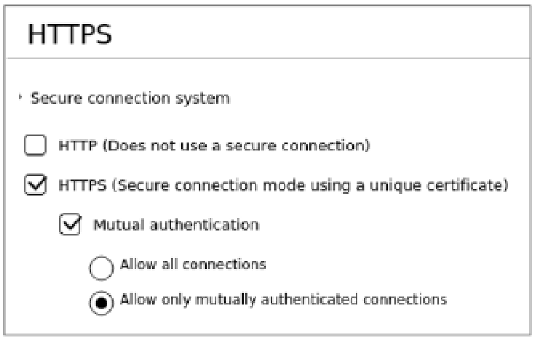
1. When registering a camera in the video storage, set as follows.
   - Only Manual registration is supported with Mutual Authentication



Manual registration

- CH: Ch 1
- Protocol: ● Wisenet ○ ONVIF ○ RTSP
- Model: Wisenet Camera
- Address type: IPv4
- IP address: 192 . 168 . 1 . 101
- Port: 4520 (Up to 65535)
- HTTP: 80 (Up to 65535)
- ID: admin
- Password: ●●●●●●●●●●
- Details
- Streaming mode: ○ TCP ○ UDP ● HTTP ○ Multicast

   - **Protocol:** Wisenet
   - **HTTP:** 80
   - **Streaming mode:** HTTP
2. The video storage security connection method is set as follows.



HTTPS

- Secure connection system

□ HTTP (Does not use a secure connection)

☑ HTTPS (Secure connection mode using a unique certificate)

☑ Mutual authentication

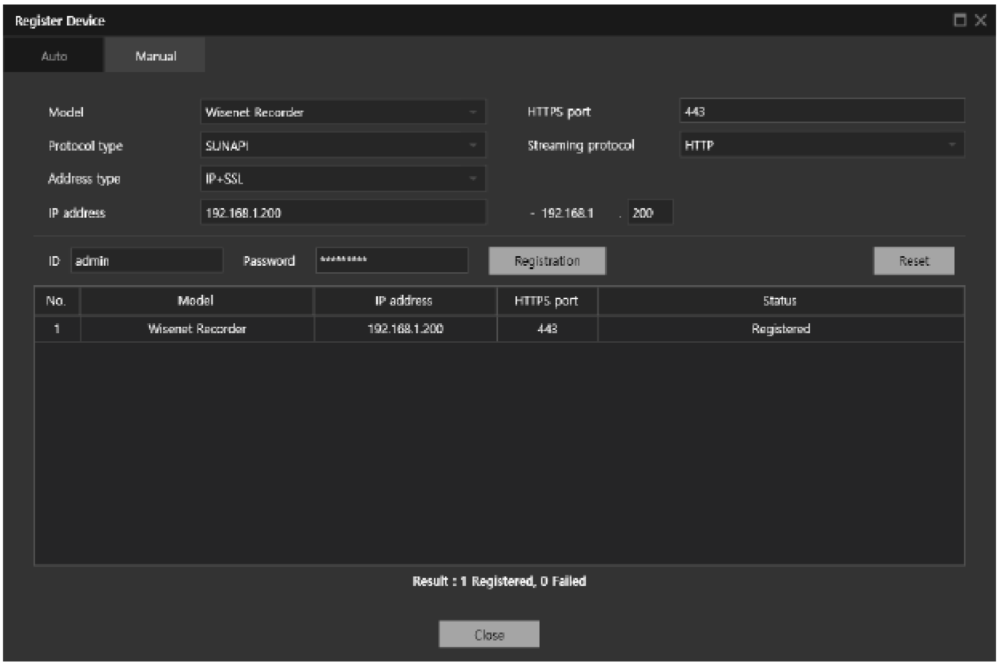
○ Allow all connections

● Allow only mutually authenticated connections

   - Check “HTTPS”
   - Check “Mutual Authentication” & select “Allow only mutually authenticated connections

SSM Appliance setup

1. When registering a video storage manually in SSM Appliance, set as follows.
   - **Protocol type:** SUNAPI
   - **Address type:** IP+SSL
   - **HTTPS port:** 443
   - **Streaming protocol:** HTTP



Model: Wisenet Recorder

Protocol type: SUNAPI

Address type: IP+SSL

IP address: 192.168.1.200

HTTPS port: 443

Streaming protocol: HTTP

- 192.168.1 . 200

ID: admin

Password: *********

No.	Model	IP address	HTTPS port	Status
1	Wisenet Recorder	192.168.1.200	443	Registered

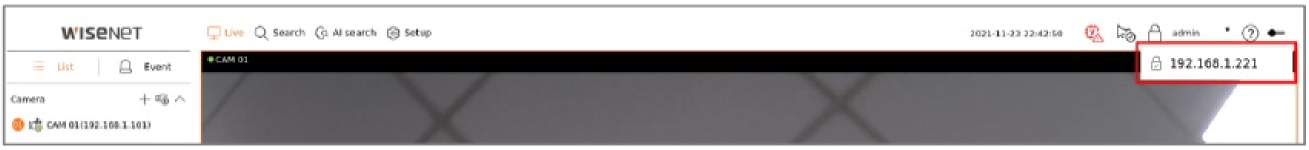
Result : 1 Registered, 0 Failed

Device authentication result

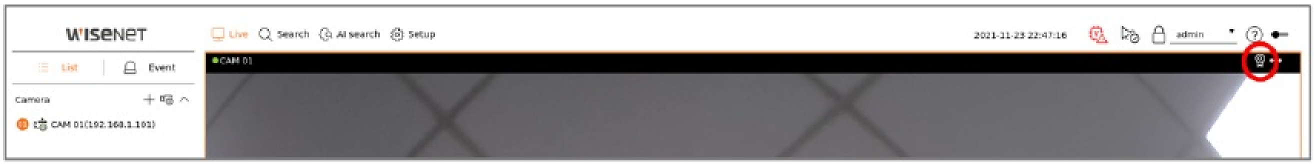
SSM Appliance authentication result

Check the SSM Appliance authentication result on the video storage set screen.

- The authentication result can be checked based on the client IP address connected to the video storage.

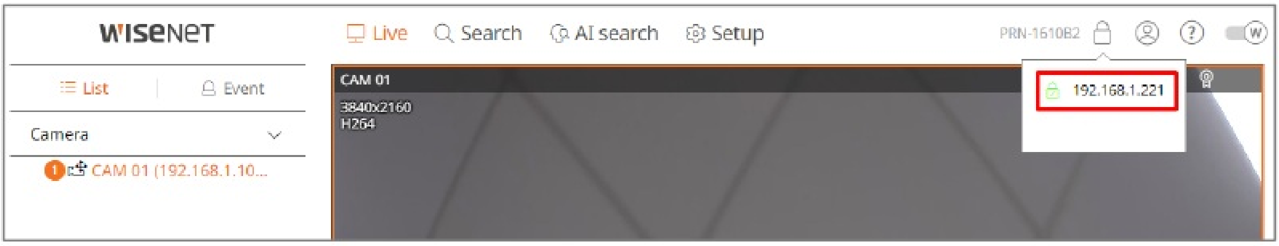


On the video storage set screen, you can also check the authentication result of the camera registered in the video storage.



You can also check the SSM Appliance authentication result on the video storage web browser screen.

- For convenience, if you want to temporarily check the authentication result through a web browser, you can additionally set the HTTP mode in the storage device to check the authentication result on the web browser screen as follows.
- In case of web browser access through HTTP mode, it is not encrypted communication, so be careful about security.



No lock (-): When video transmission is not using HTTPS (TCP/UDP/Multicast mode)

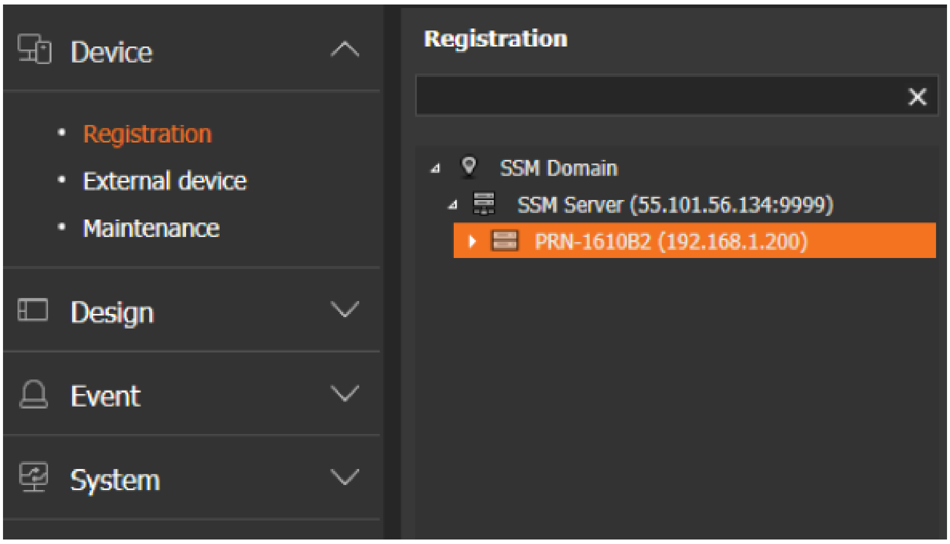
Red lock ( ): Certificates that do not support device authentication (authentication failed)

Green lock ( ): Certificate that supports device authentication (authentication successful

- For SSM Appliance (192.168.1.221) that supports device authentication, check the success of mutual authentication through a green lock.
- There is no lock mark for client access that does not use video transmission using HTTPS.

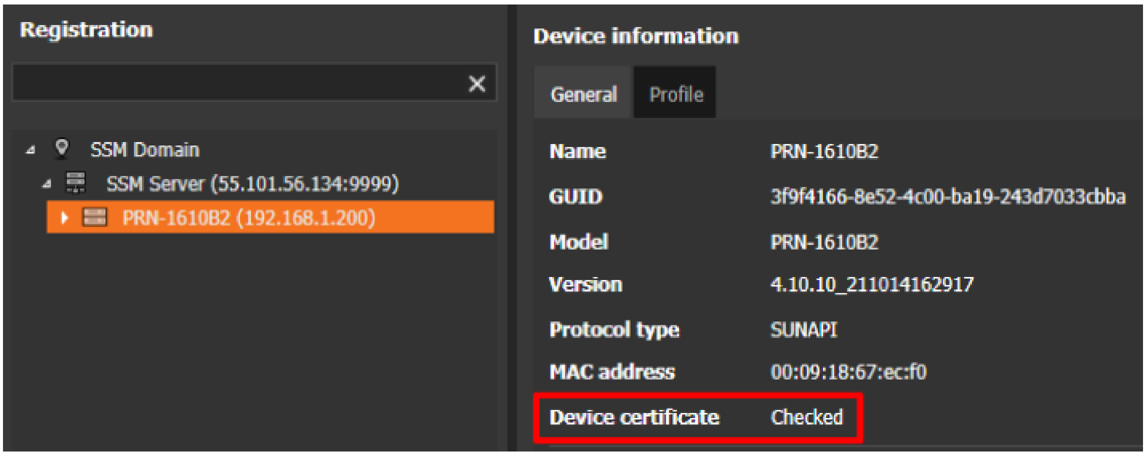
Video storage authentication result

Check if the storage device is normally registered in the SSM Appliance.



Check the device certificate in the device information of the registered video storage.

- When the video storage authentication is successful, “Device certificate Checked” is displayed.



Name	PRN-1610B2
GUID	3f9f4166-8e52-4c00-ba19-243d7033cbba
Model	PRN-1610B2
Version	4.10.10_211014162917
Protocol type	SUNAPI
MAC address	00:09:18:67:ec:f0
Device certificate	Checked

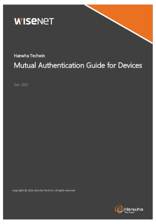
Note: Server authentication is supported from NVR (Intel-based) and SSM Appliance*SSM v2.10.7 or later products, and client authentication is supported from WN7 X series model.

For more information on supported models with device certificate, refer to the product specification page on

Hanwha Techwin website.

Hanwha Techwin Co., Ltd
13488 Hanwha Techwin R&D Center,
6 Pangyoro 319-gil, Bundang-gu, Seongnam-si, Gyeonggi-do
TEL (82) 70.7147.8771-8
FAX (82) 31.8018.3715
http://www.hanwha-security.com

Documents / Resources

	WISeNeT Mutual Authentication Guide for Devices [pdf] User Guide Mutual Authentication Guide for Devices, Mutual Authentication, Guide for Devices

References

- Hanwha Vision - Global Vision Solution Provider
- Hanwha Vision - Security Global Leader