



Hanwha Techwin

# Mutual Authentication Guide for Devices

Dec. 2021

Copyright © 2021 Hanwha Techwin. All rights reserved



# Contents

---

- What is mutual authentication?
- Mutual authentication between Camera and Video recorder
- Mutual authentication between Camera and SSM Appliance
- Mutual authentication between Video recorder and SSM Appliance

## What is mutual authentication?

---

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, refer to the location below.

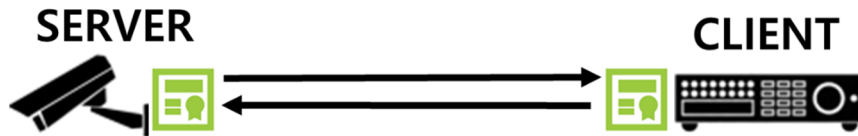
■ <https://www.hanwha-security.com> > Product > Product specification > Network > Security > Device Certificate (Hanwha Techwin Root CA, pre-installed)

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

# Mutual authentication between Camera and Video recorder

## 1. 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.

# Mutual authentication between Camera and Video recorder

## ③ Allow only mutually authenticated connections (including Device ID authentication)

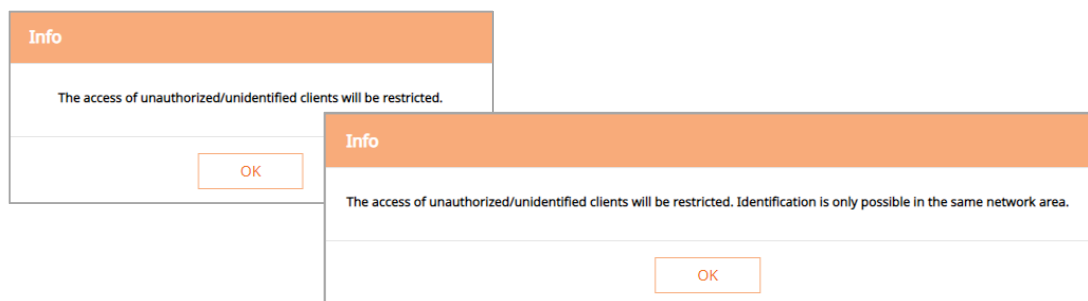
The server determines whether or not to allow the client to access the server according to whether the authentication of the certificate delivered from the client is successful.

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.

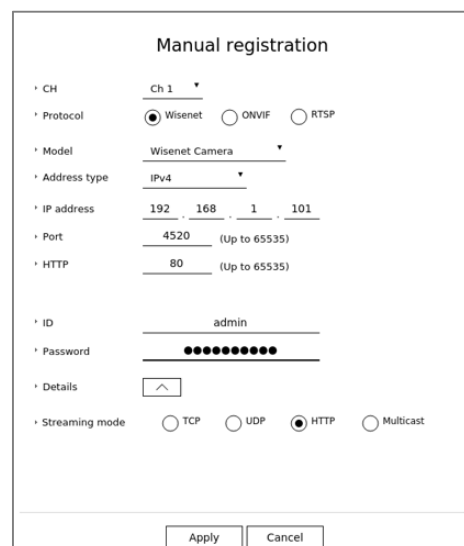


## ■ Video storage setup

1) When registering a camera in the storage device, set as follows.

※ Only Manual registration is supported with Mutual Authentication

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

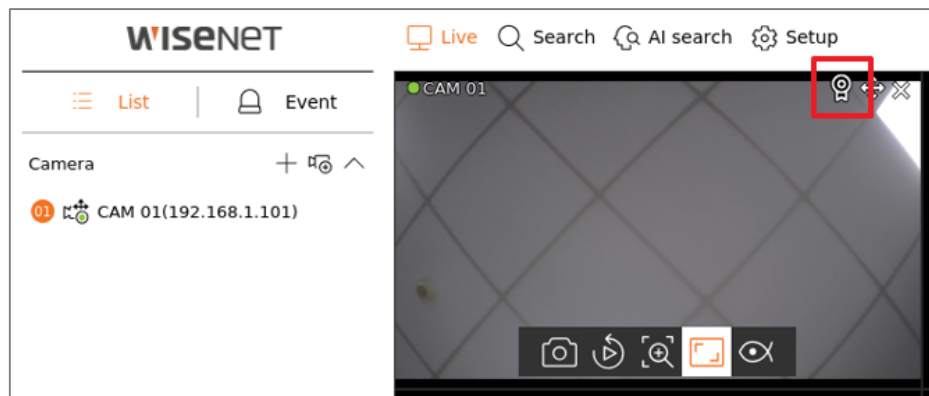


# Mutual authentication between Camera and Video recorder

## 2. 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.

# Mutual authentication between Camera and Video recorder

---



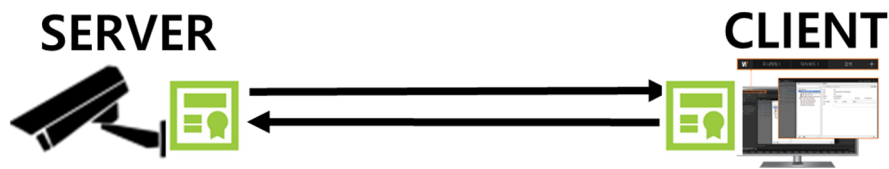
- └ No lock(-): No certificate (HTTP mode)
- Red lock(🔒): Certificates that do not support device authentication (authentication failed)
- Green lock(🔓): Certificate that supports device authentication (authentication successful) └

- 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

## 1. 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"

The screenshot shows a configuration window titled 'HTTPS'. Under the 'Secure connection system' section, there are two options: 'HTTP (Do not use a secure connection)' which is unchecked, and 'HTTPS (Use a secure connection)' which is checked and highlighted with a red rectangle. Below this, there is a 'Certificates' dropdown menu set to 'HTW\_default'. Further down, there is a 'Change host name' checkbox which is unchecked. Under the 'Mutual authentication' section, which is checked, there are three radio button options: 'Allow all connections' (unchecked), 'Allow only mutually authenticated connections' (checked and highlighted with a red rectangle), and 'Allow only mutually authenticated connections (including Device ID authentication)' (unchecked).

※ See page 3 for mutual authentication options.

### ■ 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.

- Protocol: **SUNAPI**
- Network: **IP + SSL**
- HTTPS: **443**
- Streaming Protocol: **HTTP**



# Mutual authentication between Camera and SSM Appliance

**Register camera**

Auto Manual

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

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

## 2. 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.

**Registration**

SSM Domain  
SSM Server (55.101.56.134:9999)  
XND-9082RV (192.168.1.101)

**Camera information**

General Profile Settings

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

Open setup page

※ If the device certificate icon is not visible, set as follows.

- Setup > Display > OSD text > Information Icon

Setup

General Display Video Event

Show tree  
Use device name  
Device IP address  
OSD text  
Date/Time  
Meta data  
Information icon  
Camera name  
Show IP

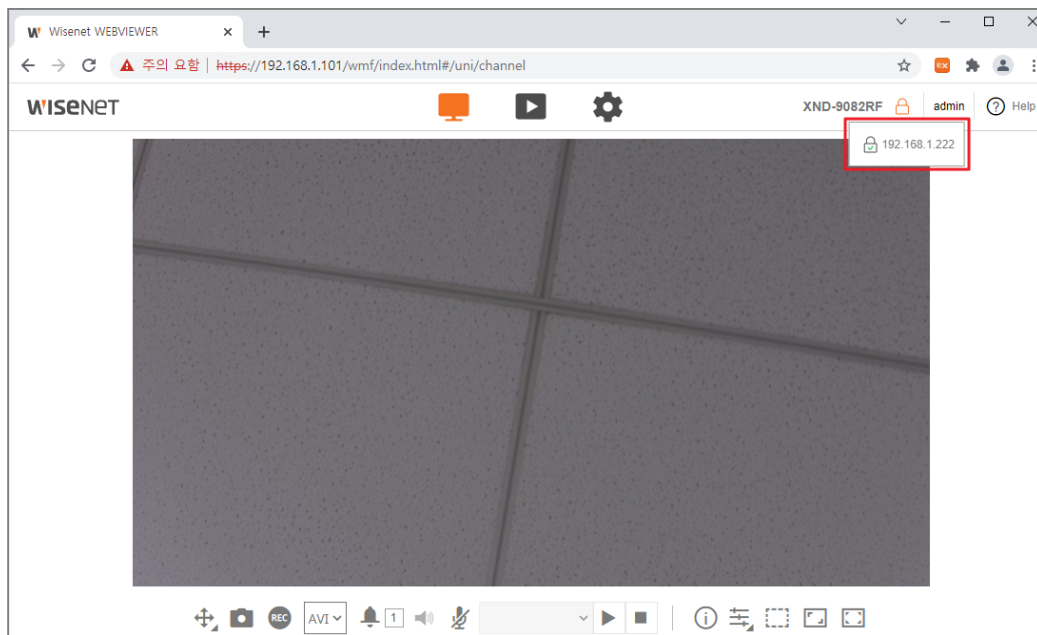
Font size: Middle Size: 9  
OSD position: Top left

# Mutual authentication between Camera and SSM Appliance

## ■ 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)

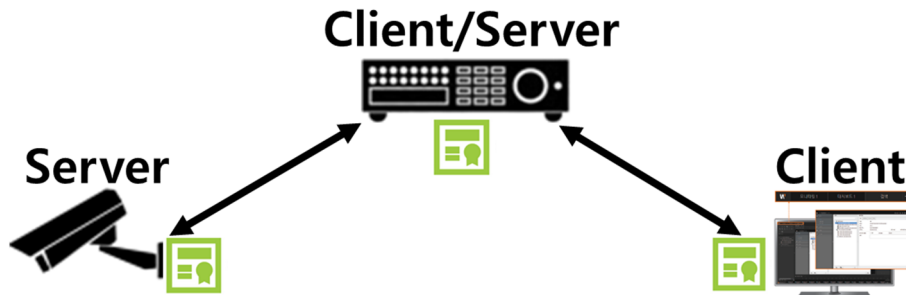
Green lock (🟢): Certificate that supports device authentication (authentication successful)

- 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

## 1. 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"

The screenshot shows the 'HTTPS' configuration window. Under the 'Secure connection system' section, the 'HTTPS (Use a secure connection)' checkbox is checked and highlighted with a red box. Below this, the 'Certificates' dropdown menu is set to 'HTW\_default'. Further down, the 'Mutual authentication' checkbox is checked. Under this, the radio button for 'Allow only mutually authenticated connections' is selected and highlighted with a red box. The other options, 'HTTP (Do not use a secure connection)', 'Change host name', 'Allow all connections', and 'Allow only mutually authenticated connections (including Device ID authentication)', are unselected.

※ See page 3 for mutual authentication options.

# Mutual authentication between Video recorder and SSM Appliance

## ■ Video storage setup

1) When registering a camera in the video storage, set as follows.

※ Only Manual registration is supported with Mutual Authentication

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

The image shows a 'Manual registration' form. It includes fields for CH (Ch 1), Protocol (Wisenet selected), Model (Wisenet Camera), Address type (IPv4), IP address (192.168.1.101), Port (4520), HTTP (80), ID (admin), Password (masked), Details (expandable), and Streaming mode (HTTP selected).

2) The video storage security connection method is set as follows.

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

The image shows the 'HTTPS' settings form. It includes a 'Secure connection system' section with options for HTTP (Does not use a secure connection) and HTTPS (Secure connection mode using a unique certificate). Under HTTPS, there is a 'Mutual authentication' checkbox which is checked, and two sub-options: 'Allow all connections' and 'Allow only mutually authenticated connections' (selected).

## ■ 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**

The image shows the 'Register Device' window with the 'Manual' tab selected. It displays fields for Model (Wisenet Recorder), Protocol type (SUNAPI), Address type (IP+SSL), IP address (192.168.1.200), HTTPS port (443), Streaming protocol (HTTP), ID (admin), and Password (masked). There are 'Registration' and 'Reset' buttons. Below the form is a table showing the registration result:

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

At the bottom, it says 'Result : 1 Registered, 0 Failed' and has a 'Close' button.

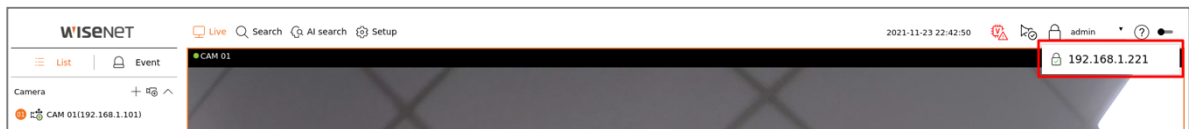
# Mutual authentication between Video recorder and SSM Appliance

## 2. Device authentication result

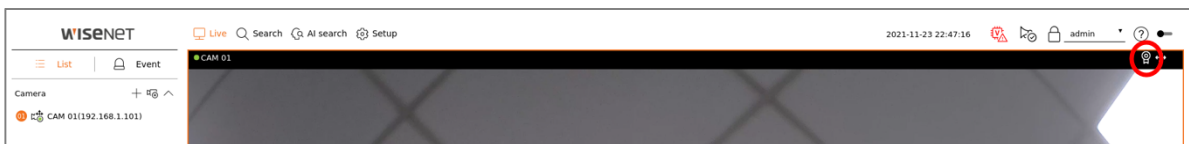
### ■ SSM Appliance authentication result

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.

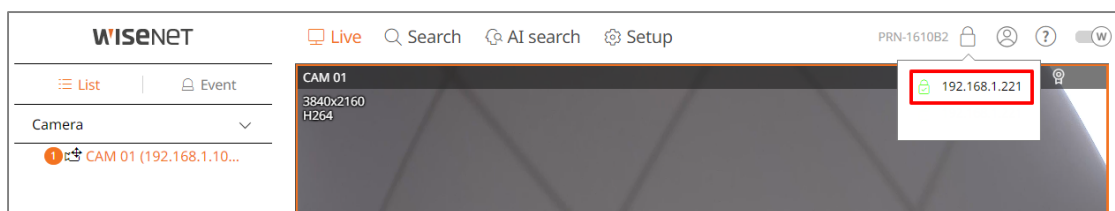


On the video storage set screen, you can also check the authentication result of the camera registered in the video storage.



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)

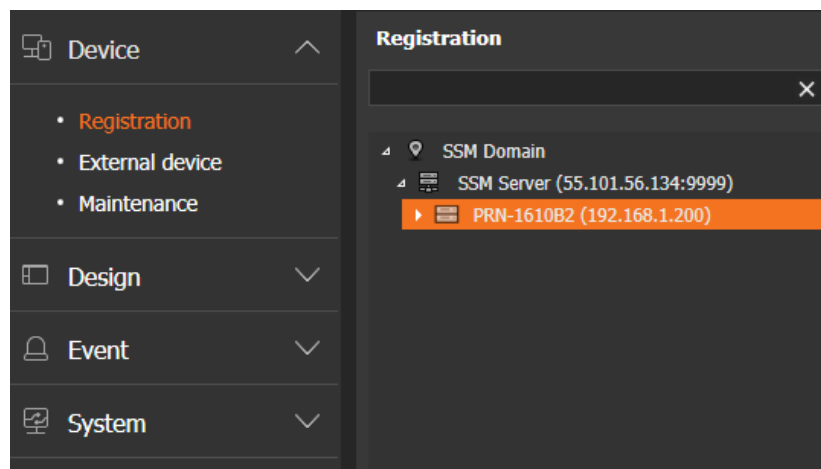
Green lock (🔓): Certificate that supports device authentication (authentication successful)

## Mutual authentication between Video recorder and SSM Appliance

- 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.

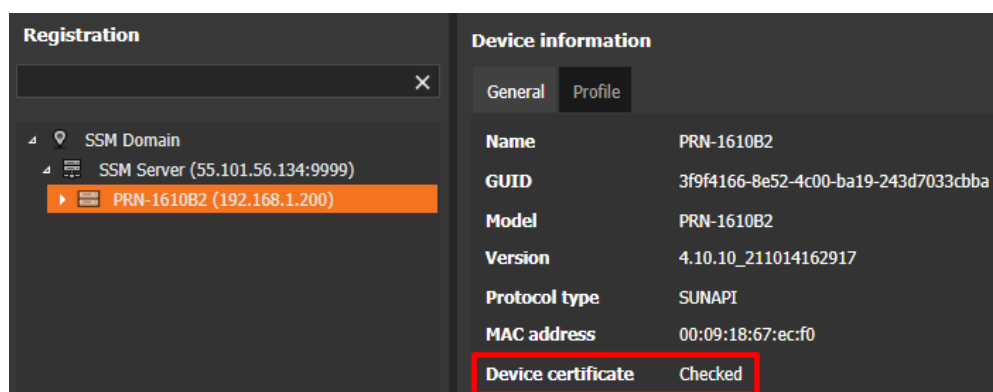
### ■ Video storage authentication result

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.



# WISENET

## 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>

Copyright © 2021 Hanwha Techwin Co., Ltd. All rights reserved

