Hanwha Vision

IP Controller

User Manual

NHP-P100
NHP-P200

CE

IP Controller

User Manual

❖ **Design and specifications are subject to change without prior notice.**
You can download the latest version from the Hanwha Vision web site. (www.HanwhaVision.com)

❖ **The initial administrator ID is "admin" and the password should be set when logging in for the first time.**
Please change your password every three months to safely protect personal information and to prevent the damage of the information theft.
Please, take note that it's a user's responsibility for the security and any other problems caused by mismanaging a password.

IMPORTANT SAFETY INSTRUCTIONS

Read these operating instructions carefully before using the unit.

Follow all the safety instructions listed below.

Keep these operating instructions handy for future reference.

1) Read these instructions.
2) Keep these instructions.
3) Heed all warnings.
4) Follow all instructions.
5) Do not use this apparatus near water.
6) Clean the contaminated area on the product surface with a soft, dry cloth or a damp cloth.
(Do not use a detergent or cosmetic products that contain alcohol, solvents or surfactants or oil constituents as they may deform or cause damage to the product.)
7) Do not block any ventilation openings, Install in accordance with the manufacturer's instructions.
8) Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
9) Do not defeat the safety purpose of the polarized or grounding- type plug. A polarized plug has two blades with one wider than the other. A grounding type plug has two blades and a third grounding prong. The wide blade or the third prong are provided for your safety. if the provided plug does not fit into your outlet, consult an electrician for replacement of the obsolete outlet.
10) Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
11) Only use attachments/accessories specified by the manufacturer.
12) Use only with the cart, stand, tripod, bracket, or table specified by the manufacturer, or sold with the apparatus. When a cart is used, use caution when moving the cart/apparatus combination to avoid injury from tip-over.

13) Unplug this apparatus during lightning storms or when unused for long periods of time.
14) Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.

Standards Approvals

FC CE

- Any changes or modifications in construction of this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

- This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
- This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules.
These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.
This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.
- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CAUTION

- This product is intended to be supplied by a UL Listed Power Supply Unit marked "Class 2" or "LPS" or "PS2" and rated from PoE.
  - **NHP-P100**: PoE+, 53V @ Max 0.48A, 12VDC @ Max 2.08A / 24VDC IN @ Max 1.04A
  - **NHP-P200**: PoE++, 55V @ Max 0.78A, 12VDC @ Max 3.5A / 24VDC IN @ Max 1.75A
- The ITE is to be connected only to PoE networks without routing to the outside plant.
The wired LAN hub providing power over the Ethernet (PoE) in accordance with IEEE 802.3bt (NHP-P200) or IEEE 802.3at (NHP-P100) shall be a UL Listed device with the output evaluated as a Limited Power Source as defined in UL60950-1 or PS2 as defined in UL62368-1.
- Battery
  - Batteries(battery pack or batteries installed) shall not be exposed to excessive heat such as sunshine, fire or the like.
  - The battery cannot be replaced.
  - Prohibition of battery abuse
    - Do not install and use the wrong type of battery.
    - Do not leave the battery in a mechanically crush or cut it because it can explode.
    - Do not leave the battery in a high temperature environment.
    - Do not leave the battery in a low-pressure environment.

PRODUCT USER MANUAL DESCRIPTION

This document is a user manual for IP Controller. Before using this product, please read this document carefully in order to use it properly.

- This user manual explains how to use the product based on the defaults and default screens of this product.
- The content of this manual is subject to change depending on the product software updates and the company policies. It is subject to partial changes without prior notification to users.

TARGET AUDIENCE

This user manual contains contents for users of IP Controller.

HOW TO USE THE PRODUCT

Users of this product can perform remote monitoring and efficient access control through a web-based open platform application.

Before using this product, check if the latest version of this software is installed. Go to Hanwha Vision's website (www.HanwhaVision.com) to check the software version and download necessary files.

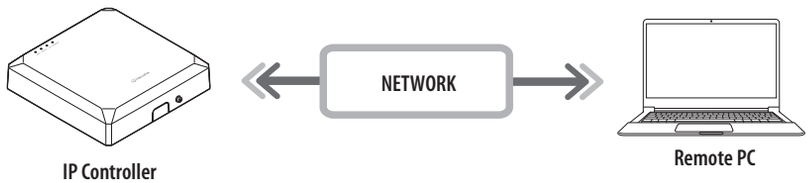
TABLE OF CONTENTS

overview

starting web viewer

WHAT IS WEB VIEWER?

A web viewer allows remote access to devices via a PC browser, enabling real-time monitoring and configuration changes.



SYSTEM REQUIREMENTS

The following lists the minimum suggested hardware and operating system requirements needed to run the Web Viewer.

- Supported browsers: Google Chrome™, Microsoft Edge®
- Supported OS: Works on all of the Windows, Linux, and Mac environments given the platform-independent nature of the web.
- This product has been tested and verified in the following environments:
  - Google Chrome™ 131 (Windows® 10 and Windows® 11)
  - Google Chrome™ 135 (macOS 14.6)
  - Microsoft Edge® 132 (Windows® 10 and Windows® 11)

CHECKING THE IP ADDRESS

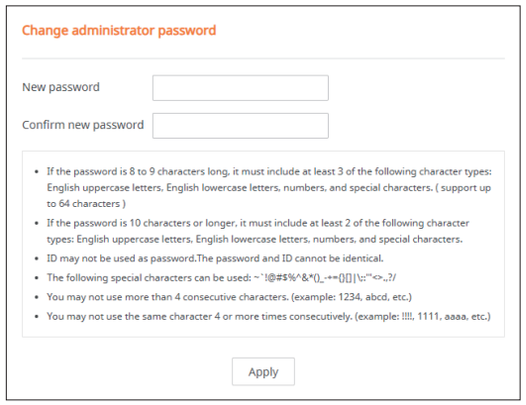
The IP address of the IP Controller required to access the web viewer can be verified in Wisenet Device Manager. To install Wisenet Device Manager, visit the Hanwha website (www.HanwhaVision.com) and download it from the "**Support** > **Tools**" menu.

1. Run Wisenet Device Manager.
2. Click <**Search**> to display the connected device list.
3. Verify the IP address of the IP Controller on the list.

SETTING THE PASSWORD

When accessing the web viewer for the first time or after a factory reset, you must set a password for the IP Controller.

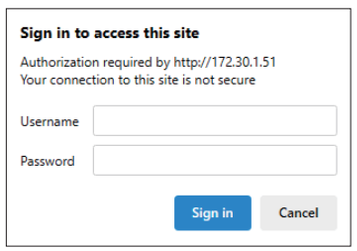
1. Open a web browser and enter the IP address of the IP Controller in the address bar.
2. Enter the administrator account password and click <**Apply**>.
   Refer to the password setup rules.



■ Make sure to memorize your password or record it so you don't forget it.

CONNECTING THE WEB VIEWER

1. Open a web browser and enter the IP address of the IP Controller in the address bar. The Sign in page appears.
2. Enter the <**Username**> and <**Password**>, then click <**Sign in**>.
   - **Username**: Enter "**admin**".
   - **Password**: Enter the password that has been set.



3. Once logged in, the main screen of the Setup Viewer will be displayed.

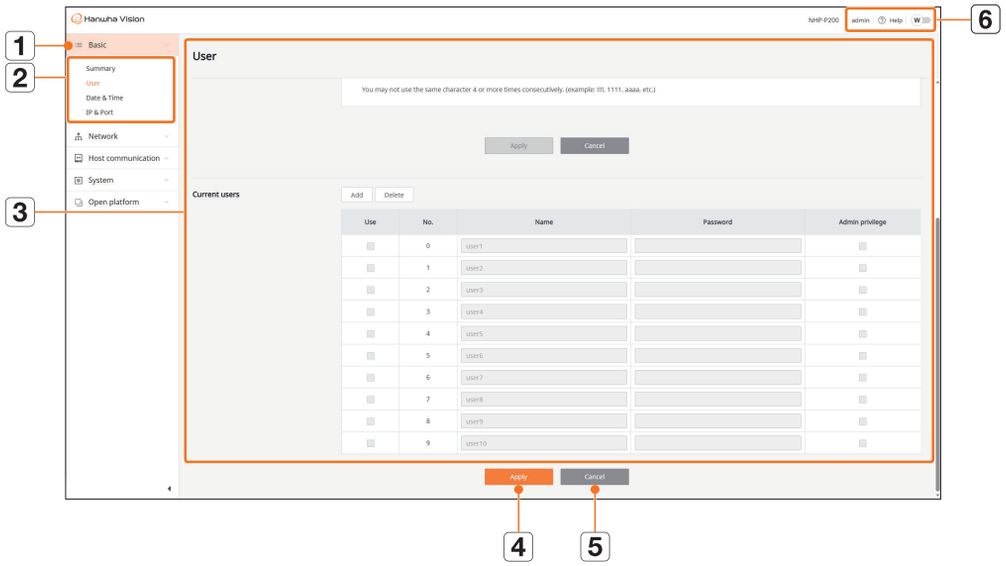
■ Please change your password every three months to safely protect personal information and to prevent the damage of the information theft. Please, take note that it's a user's responsibility for the security and any other problems caused by mismanaging a password.

■ You can change the administrator password in the "**Basic** > **User**" menu.

setup viewer

You can configure default system settings, networks, host operation mode, and open platforms. You can also back up, restore, and reset software upgrades and configuration information.

CONFIGURING SETUP VIEWER



Item		Description
1	Top menu list	Configure the settings or select a parent item to change the existing settings.
2	Sub-menu list	Among the sub-menus of selected parent menu, select a desired item to set.
3	Detailed Menu	Click desired item's input field to change and enter a desired value.
4	Apply	Apply the modified settings.
5	Cancel	Revert to the settings used before the change.
6	admin	Display the user's ID.
	Help	Display the help pop-up window.
	W	Change the color theme of the web viewer to white or black.

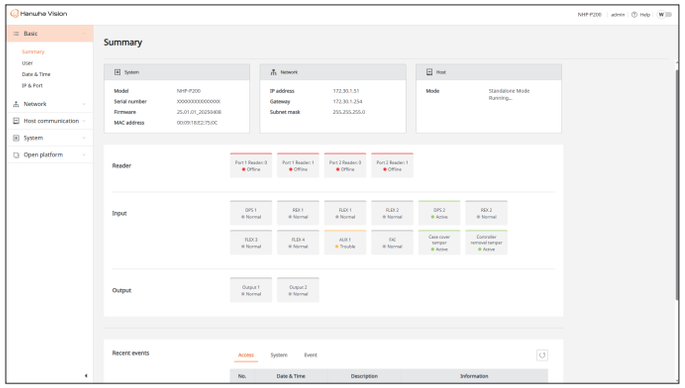
BASIC

You can check device information and status, and manage users.

Summary

You can check product information, networks, and host operation mode. You can also check the status and information of input and output devices connected to the IP Controller.

Basic > Summary



- **System**: Display the product's model name, serial number, firmware version, and MAC address.
- **Network**: Display the product's IP address, gateway, and subnet mask information.
- **Host**: Display the system's operation mode.
  - **Standalone mode**: Operate by installing and using EntryGuard.
  - **Cloud mode**: Operate by installing and using OnCAFE.
- **Reader**: Display the status of the reader connected to the IP Controller.
  - **Active**: The reader is operating normally.
  - **Offline**: No reader is connected.
  - **Trouble**: A reader is connected but not operating normally.
    If the reader is in OSDP mode and a <**Reader tamper**> event occurs, the status will change to <**Trouble**>.
- **Input**: Display the status of input devices connected to the IP Controller.
  - **Active**: Configured as <**Normally Open**> and the input device's contacts are open by default.
  - **Normal**: Configured as <**Normally Closed**> and the input device's contacts are closed by default.
  - **Trouble**: The input is configured as <**Supervised**> or there is a problem such as disconnection with the input circuit.
  - **Disabled**: Configured as an unused input.
  - **Unavailable**: The input is not possible because the reader protocol is set to Wiegand mode or two inputs cannot be used for one door.
- **Output**: Display the status of the output device connected to the IP Controller.
  - **Active**: The output is not in the <**Normally Closed**> state. The output is configured as <**Normally Closed**> by default.
  - **Normal**: The output is in the <**Normally Closed**> state.
- **Recent events**: Display up to five recent events by type.
  - You can view event logs via HTTPS.

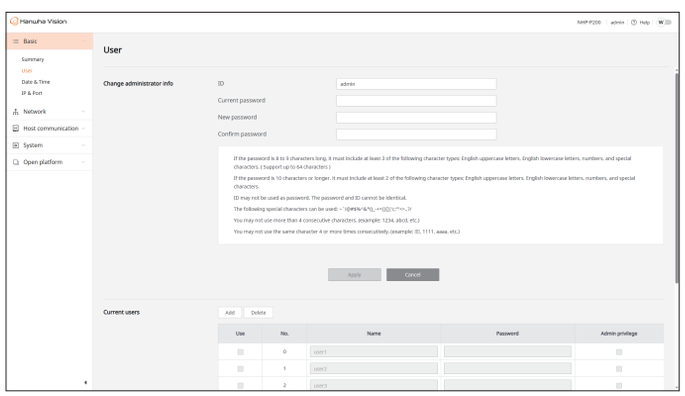
User

You can change the administrator's ID and password, and add or delete users. The administrator can configure and use all menu items and features. The administrator cannot be deleted, and a new administrator cannot be added.

Changing Administrator Information

You can change the administrator's ID and password.

Basic > User > Change administrator info



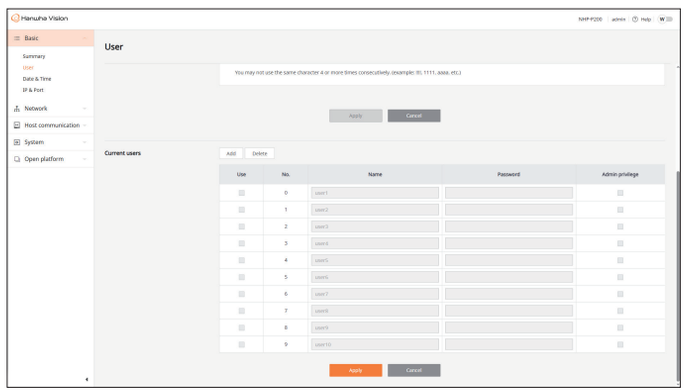
- **ID**: Enter the administrator ID that you want to change. You will be automatically logged out when the ID is changed.
- **Current password**: Enter the current password.
- **New password**: Enter a new password.
- **Confirm password**: Re-enter the new password.

- The default administrator ID is <**admin**>, and you will be required to set a password at the initial login.
- Please follow the instructions on the screen for to set up the password.
- Please change your password every three months to safely protect your personal information and prevent damage from information theft. Please, take note that it's a user's responsibility for the security and any other problems caused by mismanaging a password.

Changing User Information

You can add or delete users. You can also grant administrator authority to a specific user.

Basic > User > Current users

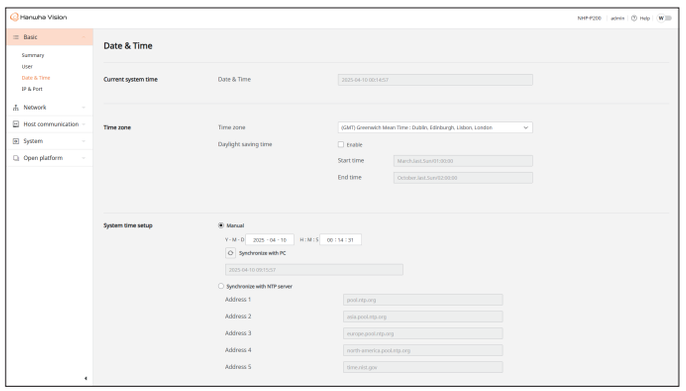


- **Add**: You can add up to 10 users.
- **Delete**: Select the user to delete in the user list and click <**Delete**>.
- **Admin privilege**: You can grant administrator authority to a specific user.
  If <**Admin privilege**> is not checked when adding a user, the user will not have configuration authority and will only be able to check the <**Summary**> page in the Setup viewer.

Date & Time

You can check or change the current date, time, and time related settings.

Basic > Date & Time



- **Current system time**: Display the current date and time.
- **Time zone**: Configure the time zone for the region where the product is installed.
- **Daylight saving time**: To use daylight saving time, check <**Enable**>. The start and end times of the current time zone will be automatically adjusted by one hour.
- **System time setup**: You can configure the system time.
  - **Manual**: You can configure the date and time manually. Changing the date and time will adjust both <**Time zone**> and <**Daylight saving time**>.
  - **Synchronize with PC**: After changing the date and time, click < ↻ > to synchronize with the time of the PC running the web viewer.
  - **Synchronize with NTP server**: You can synchronize the current date and time of the product with the NTP server. Manual time adjustment is not possible.
    You can configure up to five NTP servers using URL or IPv4 addresses.

IP & Port

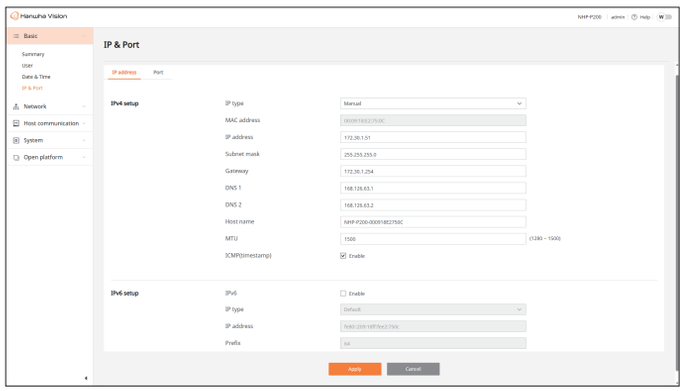
You can set the network connection route and protocol.

Setting a Network Connection

You can select the IPv4 network connection type and configure the connection settings.

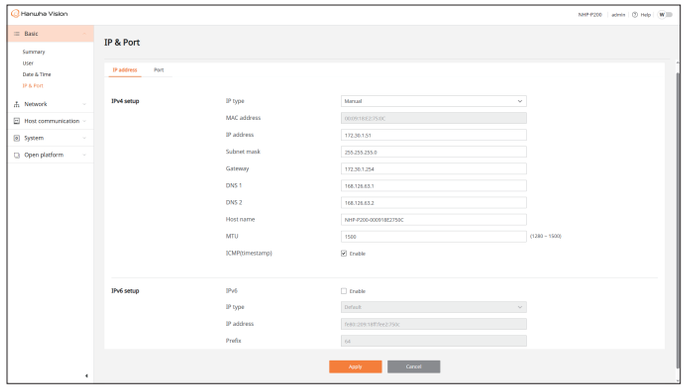
■ The network setup method varies depending on whether a router is used and the connection type, so check the connection mode before setting it up.

Basic > IP & Port > IP address > IPv4 setup



- **IP type**: Select <**Manual**> to connect the product as follows.
  - Select <**Manual**> when connecting to the Internet via a fixed IP or dedicated line, or connecting the product with remote users in a local network.
  - Select <**Manual**> when connecting the product to a router attached to a cable model, or connecting the product to a router in a local network.
  - Configure the settings for <**IP address**>, <**Subnet mask**>, <**Gateway**>, <**DNS 1**>, <**DNS 2**>, <**Host name**>, <**MTU**>, and <**ICMP(timestamp)**>.
    - Ensure that the IP address is within the fixed IP range provided by the router, and the subnet and gateway match the values provided by the router.
    - **E.g.** If the DHCP server is configured with start and end addresses of 192.168.0.100 and 192.168.0.200, the IP address must be configured outside this range, such as 192.168.0.2–192.168.0.99 or 192.168.0.201–192.168.0.254.
- **IP type**: Select <**DHCP**> when directly connecting the product to a cable modem, DHCP modem, or optical LAN.
  - Configure the settings for <**DNS 1**>, <**DNS 2**>, <**Host name**>, <**MTU**>, and <**ICMP(timestamp)**>.
  - You can check <**Enable**> under <**DNS setting by DHCP**> to automatically obtain DNS by DHCP.

Basic > IP & Port > IP address > IPv6 setup

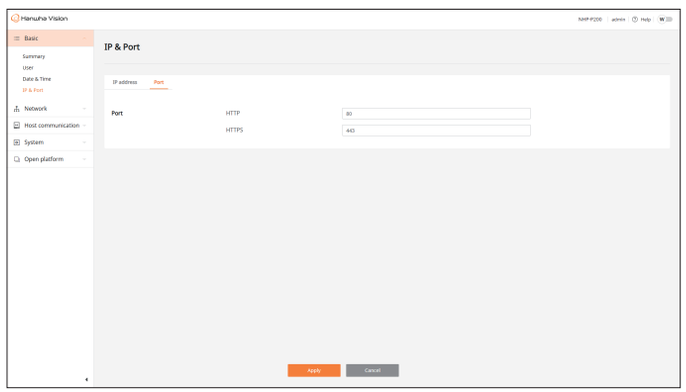


- **IPv6**: To use IPv6 settings, check <**Enable**>.
- **IP type**: Select the network connection type.
  - **Default**: <**IP address**> is the address configured with the MAC address of the product. It cannot be changed by users.
  - **Manual**: Configure <**IP address**>, <**Prefix**>(1~128), and <**Gateway**>.
  - **DHCP**: <**IP address**> is the address obtained through DHCP. It cannot be changed by users.

Setting Port

You can select the IPv4 network connection type and configure the connection settings.

Basic > IP & Port > Port



- **HTTP**: Enter the port value for the HTTP web viewer. The default value is 80, and it can be set between 1024 and 65535.
- **HTTPS**: Enter the port value for the HTTPS web viewer. The default value is 443, and it can be set between 1024 and 65535.
  - HTTPS is an enhanced version of the HTTP web communication protocol. If security is important when accessing the web viewer, enable the HTTPS port.

- Ports 3702, 4520, and 49152 cannot be configured.

NETWORK

You can configure features related to DDNS usage, security, and authentication for network connection.

DDNS

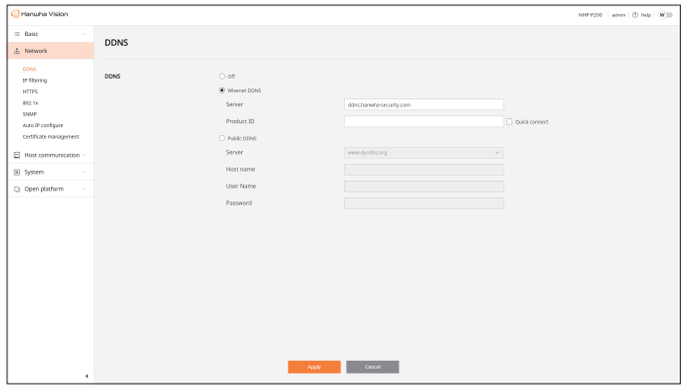
Remote users can access the product using a DDNS address in a dynamic IP environment.

Setting Wisenet DDNS

When using the Wisenet DDNS (Dynamic Domain Name Server) service, you can access the product by entering the registered product ID.

For Wisenet DDNS setup, first sign up for the Wisenet DDNS service provided by Hanwha Vision.

Network > DDNS > Wisenet DDNS

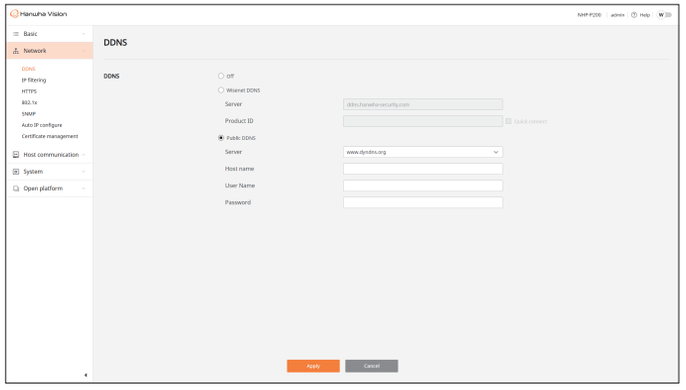


- **Wisenet DDNS**: Check this option to use Wisenet DDNS.
- **Server**: Enter the server name registered to Wisenet DDNS.
  - The server name can contain up to 63 characters, and can include letters, numbers, and special characters (- ./ _).
- **Product ID**: Enter the product ID registered to Wisenet DDNS.
  - The product ID can contain up to 31 characters, and can include letters, numbers, spaces, and special characters (~ ` ! @ $ ^ ( ) _ - | { } [ ] ; , . / ?).
- **Quick connect**: If using a router that supports UPnP, check <**Quick connect**> to automatically assign a port.

Configuring Public DDNS

When using the public DDNS (Dynamic Domain Name Server) service, you can access the product by entering the registered hostname, user name, and password.

Network > DDNS > Public DDNS



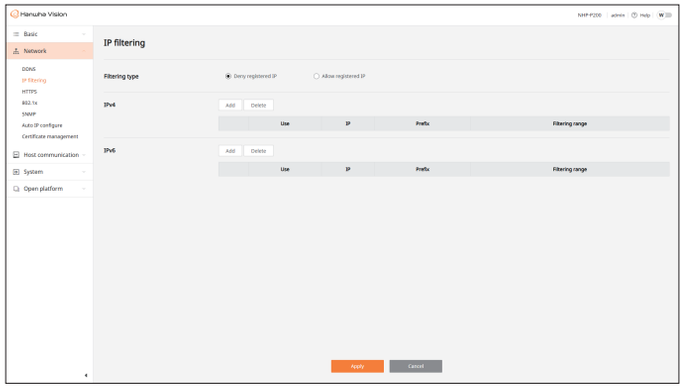
- **Public DDNS**: Check this option to use the public DDNS.
- **Server**: Select the DDNS site in use.
- **Host name**: Enter the hostname registered to the selected DDNS site.
- **User name**: Enter the username registered to the selected DDNS site.
- **Password**: Enter the password registered to the selected DDNS site.

■ The hostname, username, and password can contain up to 31 characters and can include letters, numbers, spaces, and special characters (~ ` ! @ $ ^ ( ) _ - | { } [ ] ; , . / ?).

IP filtering

You can create a list to restrict or allow access for specific IP addresses.

Network > IP filtering



- **Filtering type**: Select the filtering type.
  - **Deny registered IP**: Restrict access for registered IP addresses.
  - **Allow registered IP**: Allow access for registered IP addresses.
- **Add**: You can register IP addresses for filtering. Click <**Add**>, then enter the <**IP**> and <**Prefix**> to register.
  - When adding an IP address to allow access, add the IP address of the currently connected PC first.
  - For <**Prefix**>, you can enter 1-32 for IPv4 and 1-128 for IPv6.
  - Once the <**IP**> and <**Prefix**> are entered, the IP address range is displayed under <**Filtering range**>.
- **Delete**: You can delete a registered IP address. Select the IP address to delete from the registered IP list and click <**Delete**>.

HTTPS

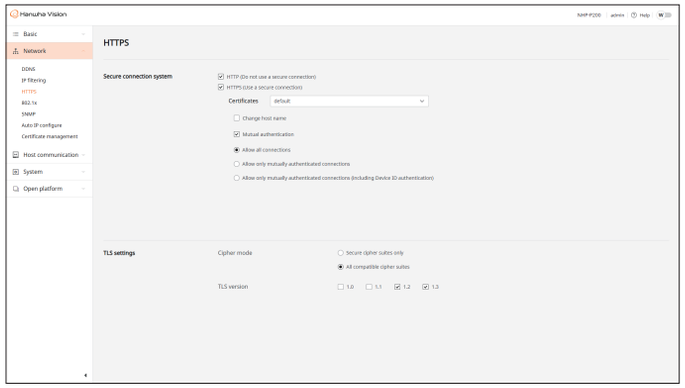
You can select a secure connection system or install certificates. You can also configure settings for TLS encrypted communications.

Setting Secure Connection Mode

Considering the security level, you can select a secure connection mode appropriate to the usage environment.

HTTPS (HyperText Transfer Protocol Secure) is a more secure version of HTTP. It uses TLS (Transport Layer Security) to encrypt/decrypt user page requests and exchange data.

Network > HTTPS > Secure connection system



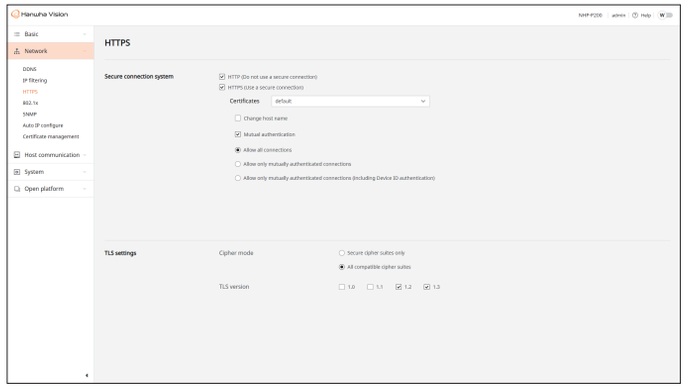
- **HTTP (Do not use a secure connection)**: Transfer data without encryption.
- **HTTPS (Use a secure connection)**: Uses a device certificate provided by the product for a secure connection.
  - An HTTPS connection is recommended if the product is connected to the external Internet or is installed in an environment where security is important.
- **Certificates**: If <**HTTPS (Use a secure connection)**> is selected, the <**Certificates**> menu is displayed.
- **Change host name**: Ensure that <**Host name**> under the "**Basic** > **IP & Port** > **IP address**" menu matches the CN value of the product certificate.
- **Mutual authentication**: Mutual authentication may be required to enhance security.
  - **Allow all connections**: You can allow access to the product without mutual authentication.
  - **Allow only mutually authenticated connections**: You can allow access to the product only when mutual authentication is successful.
  - **Allow only mutually authenticated connections (including device ID authentication)**: You can allow access to the product only when mutual authentication, including verification of the device ID (MAC address), is successful. However, this only operates in the same network environment.

- Select either HTTP or HTTPS for a secure connection system, or select both modes simultaneously.
- If the certificate is invalid, the web server may not function correctly. In this case, the system will internally attempt to restart the web server three times. If the attempts fail, the system will delete the certificate and change the secure connection mode to default (HTTP).
- If the device certificate within HTTPS is deselected, the hostname and mutual authentication setting will automatically reset to the default values.
- In cloud mode, HTTPS is enabled by default and cannot be turned off.

Setting TLS

You can select the Cipher mode or TLS version to use for encrypted communication.

Network > HTTPS > TLS settings



- **Cipher mode**: Provide cipher suites by combining algorithms used for TLS encrypted communications, such as key exchange, authentication, and encryption.
  - **Secure cipher suites only**: Use only highly secure cipher suites.
  - **All compatible cipher suites**: Select this option for backward compatibility. However, there may be vulnerabilities as it includes all cipher suites regardless of the security level.
- **TLS version**: You can select the TLS protocol version for encrypted communications.
  - If <**Cipher mode**> is set to <**Secure cipher suites only**>, only <**1.2**> or <**1.3**> can be selected.
  - When switching <**Cipher mode**> to <**Secure cipher suites only**> under <**All compatible cipher suites**>, <**1.0**> and <**1.1**> will automatically be deselected.
  - You can select multiple versions simultaneously.

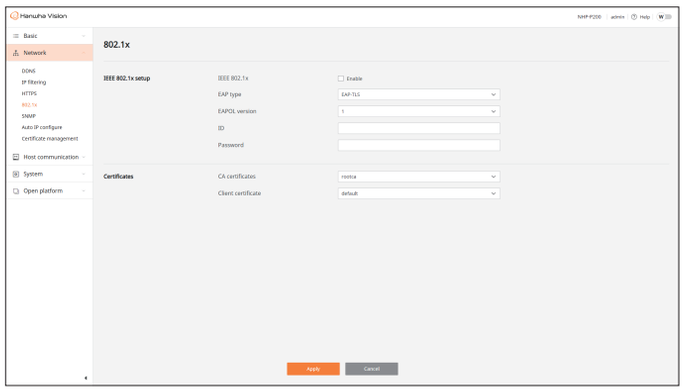
802.1x

You can enable or disable the 802.1x protocol for network connection and install certificates.

802.1x prevents hacking, viruses, and information leakage in network data transmission with an authentication system between servers and clients.

802.1x can be used to block the unauthorized client access and increase security by allowing only authenticated users to communicate.

Network > 802.1x



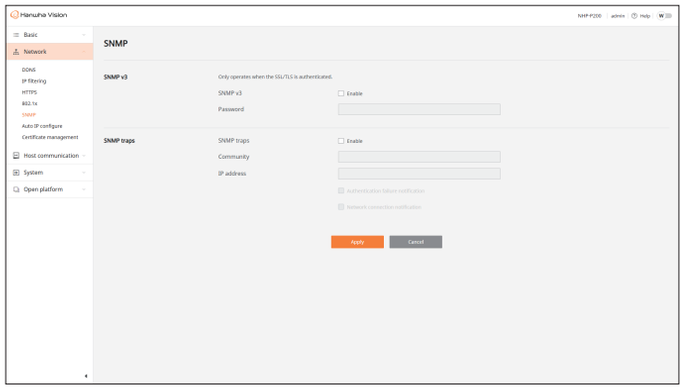
- **IEEE 802.1x**: To use IEEE 802.1x settings, check <**Enable**>.
- **EAP type**: Select the authentication type.
  - **EAP-TLS**: Requires a CA certificate, client certificate, and key installation.
  - **LEAP**: Certificates are not used.
  - **PEAPv0/MSCHAv2**: Requires the installation of a CA certificate.
- **EAPOL version**: Select the EAPOL version for the protocol.
  - Communications may not function properly for some switch hubs if version <**2**> is used. In this case, select the default EAPOL version <**1**>.
- **ID**: Enter the ID of the account configured on the authenticated server.
  - For **EAP-TLS** authentication, you can use a random ID.
- **Password**: Enter the password of the account configured on the authenticated server.
  - For **EAP-TLS** authentication, passwords are used only when an encrypted client private key is used.
- **CA certificate**: A list of certificates containing public keys is displayed. Select the certificate to use.
  CA certificate require the server to have the server certificate and key file installed.
- **Client certificate**: A list of certificates containing client authentication keys is displayed. Select the certificate to use.

- The ID and password can contain up to 30 characters, and can include letters, numbers, and special characters (` ~ ! @ # $ % ^ * ( ) _ | + - = ? { } [ ] / : ; & " ' < > ,).
- If connected to a port that does not use the 802.1x feature, the network is accessible regardless of the product's 802.1x settings.
- Authentication will fail if there is no communication between the switch hub and the server during the authentication attempt.
- Authentication will fail if the product's time is set outside the certificate's validity period.
- To set up an 802.1x environment, a RADIUS server must be used. In addition, the switch hub connected to the server must be a device that supports 802.1x.
- If the times of the server, switch hub, and product do not match, communication between the devices may fail.
- Both the CA certificate and client certificate must be installed to use 802.1x.

SNMP

The SNMP protocol allows system or network administrators to remotely monitor and configure the network devices.

Network > SNMP



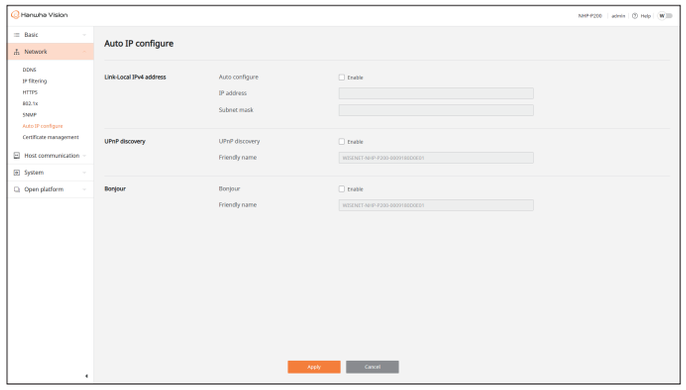
- **SNMP v3**: Only operates when the SSL/TLS is authenticated. To use <**SNMP v3**>, check <**Enable**>.
  - **Password**: Set the initial user password.
    - The password can contain up to 8-16 characters. The following characters cannot be used: ` & | ; $ { } < > \r \n.
- **SNMP traps**: SNMP traps are used to send important events and statuses to the management system. To use <**SNMP traps**>, check <**Enable**>.
  - **Community**: Enter the name of the trap community to receive messages.
  - **IP address**: Enter the IP address to send messages.
  - **Authentication failure notification**: If the community information is incorrect, events will be sent to the entered IP address.
  - **Network connection notification**: If a disconnected network is reconnected, events will be sent to the entered IP address.

- SNMP setup can only be activated by authorized users when necessary.

Auto IP configure

You can automatically search for and connect to the product in a local network, the Bonjour protocol, or an operating system using UPnP.

Network > Auto IP configure

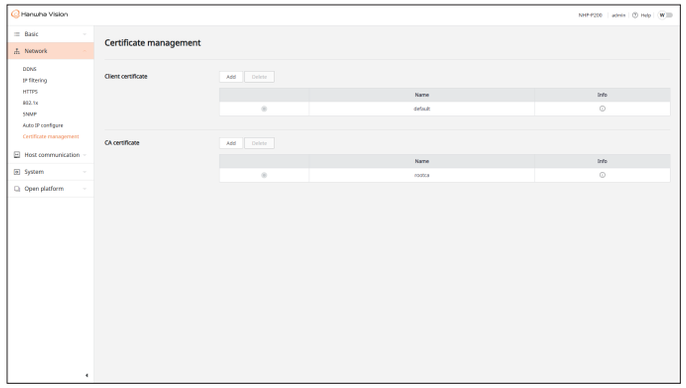


- **Auto configure**: An <**IP address**> and <**Subnet mask**> can be automatically assigned to the product in a local network that does not receive an IP from the DHCP server.
  To use this feature, check <**Enable**>. Once configured, the <**IP address**> and <**Subnet mask**> will be displayed.
  - Only the IP Controller and host connected to the same switch can connect with the configured address.
- **UPnP discovery**: Without any additional network settings, you can search for and connect to the product with <**Friendly name**> in a Windows computer network.
  To use this feature, check <**Enable**> and enter the product name to be displayed in <**Friendly name**>.
  - The Friendly name can contain up to 63 characters, and can include letters, numbers, special characters (~ ! @ $ _ - | { } [ ] , . / ?), and spaces. A space cannot be used as the first character.
- **Bonjour**: For an OS and client that support the Bonjour protocol, you can search for and connect to the product with <**Friendly name**>.
  To use this feature, check <**Enable**> and enter the product name to be displayed in <**Friendly name**>.
  - The Friendly name can contain up to 63 characters, and can include letters, numbers, special characters (~ ! @ $ _ - | { } [ ] , . / ?), and spaces. A space cannot be used as the first character.
  - On a Mac OS that supports Bonjour, you can check the connected IP Controller in Safari with the Bonjour bookmark. If the Bonjour bookmark is not displayed, activate the Bookmarks settings in the Preference menu.
  - In Safari on a Mac OS, previously searched IP Controller cookies may accumulate and be displayed when performing a Bonjour search.
  - If the Bonjour setting is disabled during the connection, it may take one to three minutes for the connection to be lost.

Certificate management

You can manage client certificates and CA certificates separately, and add or delete certificates.

Network > Certificate management



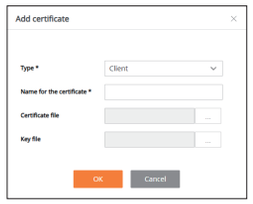
- **Add**: You can add certificates.
  - You can add up to eight client certificates and three CA certificates.
- **Delete**: Select the certificate to delete from the certificate list and click <**Delete**>. The certificate in use cannot be deleted.
- **Info**: You can click < ⓘ > to check the certificate information.

Setting Client Certificate

Client certificates can be created by users or selected from other certificates.

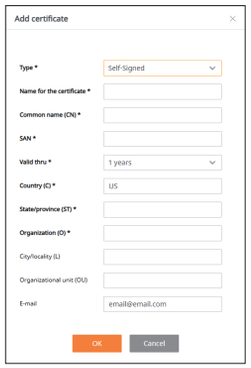
The certificate provided by Hanwha Vision is registered by default, and it cannot be deleted.

Network > Certificate management > Client certificate



- **Type***: If there is a certificate file, select <**Client**>.
- **Name for the certificate***: Enter the certificate name.
- **Certificate file**: Click < ... > to select a certificate file.
- **Key file**: Click < ... > to select a key file.

- * indicates a required field.



- **Type***: To create a certificate directly, select <**Self-Signed**>.
- **Name for the certificate***: Enter the certificate name.
- **Common name (CN)***: Enter the common name for the certificate.
- **SAN***: Enter the SAN (Subject Alternative Name) information for the certificate.
- **Valid thru***: Select the validity period of the certificate. The certificate period is based on the product's time.
- **Country (C)***: Enter the country. Only two alphabetical characters can be entered.
- **State/province (ST)***: Enter the region.
- **Organization (O)***: Enter the organization name.
- **City/locality (L)**: Enter the detailed region.
- **Organizational unit (OU)**: Enter the organizational unit.
- **Email**: Enter the email address.

■ * indicates a required field.

Setting CA Certificate

CA (certificate authority) certificates are issued by certification authorities.

The certificate provided by Hanwha Vision is registered by default, and it cannot be deleted.

Network > Certificate management > CA certificate

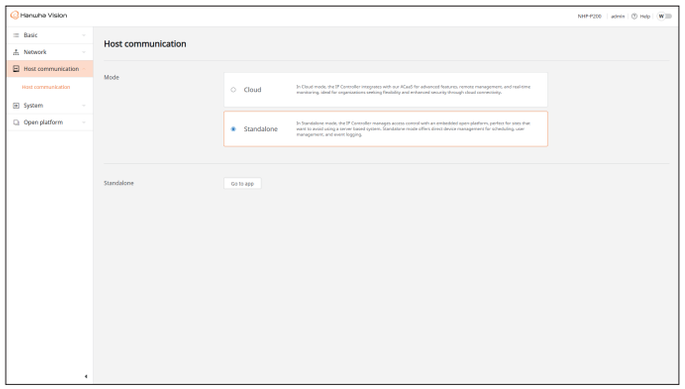
- **Name for the certificate**: Enter the certificate name.
- **Certificate file**: Click < ... > to select a certificate file.

HOST COMMUNICATION

You can configure the operation mode for the system and host.

Host communication

Host communication > Host communication



- **Cloud**: The IP Controller includes OnCAFE (On Cloud Access control For Everyone) and supports advanced features, remote management, and real-time monitoring. The cloud connection can be applied to areas that require flexibility and enhanced security.
- **Standalone**: The IP Controller uses an embedded open platform to support direct device management for scheduling, user management, and event logging, as well as an autonomous access control system. It can be applied to areas with an unstable network connection.
- **Go to app**: Go to the application screen corresponding to the selected mode.

■ If the mode is changed, all access control settings will be reset and the product will reboot.

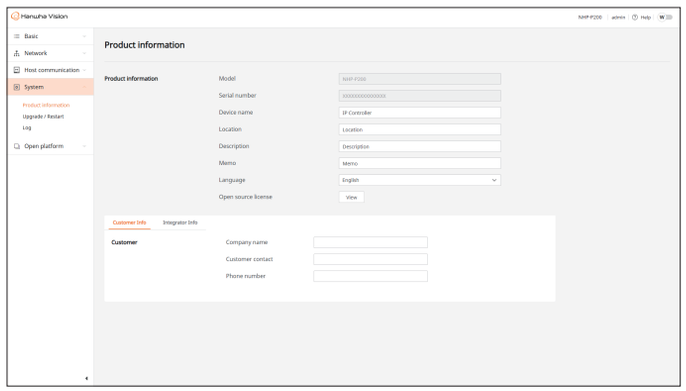
SYSTEM

You can check the detailed information and log information of the product and upgrade to the latest software version. You can also back up, restore, and reset settings information.

Product information

You can check the product model name, serial number, open source license information, and more. You can also check and modify user or service provider information.

System > Product information



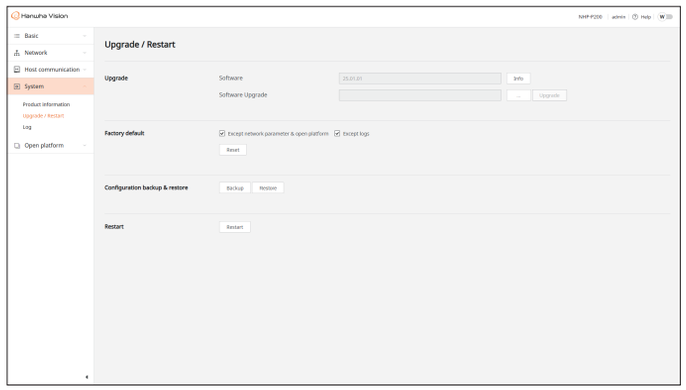
- **Model**: Display the product model name.
- **Serial number**: Display the product serial number.
- **Device name**: You can enter the device name.
  - Use different names to distinguish multiple identical devices.
- **Location**: You can enter the location where the product is installed.
- **Description**: You can enter the detailed product information.
- **Memo**: You can enter a few details for easy identification of the product.
- **Language**: You can select the language to be displayed on the screen.
- **Open source license**: You can click <**View**> to check the product's open source license information.
- **Customer Info**: You can enter information of the entity (customer) using the product, such as name or contact information.
- **Integrator Info**: You can enter information of the entity servicing the system, such as name or contact information.

- The device name can contain up to eight characters, and cannot include some special characters (# ' " " & + : < > = \ % *).
- The location, description, and memo can contain up to 32 characters each, and can include letters, numbers, spaces, and special characters (~ ` ! @ $ ^ ( ) _ - | { } [ ] ; , . / ?). A space cannot be used as the first character.
- The customer contact and service contact can contain up to 32 characters each, and can include letters, numbers, spaces, and special characters (~ ` ! @ $ ^ ( ) _ - | { } [ ] ; , . / ?). A space cannot be used as the first character.
- The phone number can contain up to 16 characters, and can include numbers, special characters (+ -), and spaces.

Upgrade / Restart

You can check the current software version of the product and upgrade to the latest version. You can also reset the product to the factory settings or save the settings information as a file.

System > Upgrade / Restart

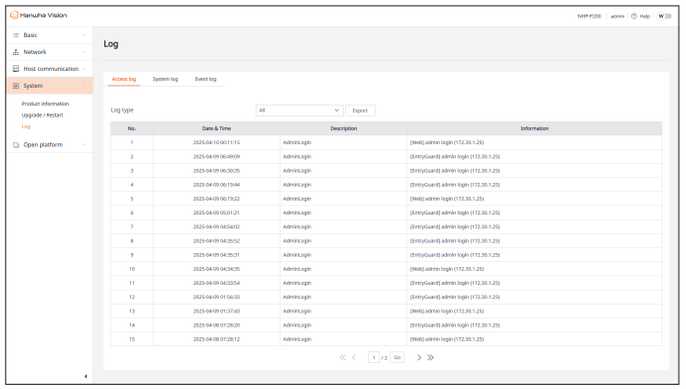


- **Software**: You can click Info to check the current version of the software module.
- **Software upgrade**: You can upgrade to the latest software.
  Click < ... > to select the latest software file. <**Upgrade**> will be activated.
  Click <**Upgrade**> to start the upgrade. The product will reboot upon completion.
  - Ensure that the power remains on during the upgrade.
  - If the software upgrade fails, it will automatically revert to the previous version and the product will reboot.
- **Factory default**: You can reset all product settings to the factory defaults.
  - **Except network parameter & open platform**: Check this option before performing a factory reset to retain network and open platform settings, including access control data and configurations.
    - When performing a factory reset including network settings, only HTTPS will be enabled by default.
  - **Except logs**: Check this option before performing a factory reset to retain log information.
  - **Reset**: Click <**Reset**> to display the <**Confirm**> window. To proceed with the factory reset, click <**OK**>.
    - The product's current time is retained after the factory reset, but <**Time zone**> is changed to <**(GMT) Greenwich Mean Time**>.
- **Configuration backup & restore**: You can save product settings or restore them by applying saved settings. You can create multiple settings files and restore desired settings according to the product usage or environment.
  - **Backup**: The current product settings are saved as a .bin file in the download path.
    - If authentication information is included when backing up the settings information, it will be encrypted and stored.
  - **Restore**: Select the saved settings file to restore to the time of the backup. The product will restart after the restoration is complete.
- **Restart**: Click <**Restart**> to display the <**Confirm**> window. To restart the product, click <**OK**>.

Log

You can check log information related to system access, configuration changes, and events and save it as files.

System > Log



- **Access log**: Display the date, time, and IP address of user login attempts and failures.
- **System log**: Display the date, time, and details of system starts, restarts, configuration changes, software upgrades, factory resets, and configuration backups/restorations.
- **Event log**: Display the date, time, and details of events related to input/output and application from the IP Controller.
  - You can view event logs via HTTPS.
- **Log type**: You can select items to search within the log category.
- **Export**: You can save searched log information as a file (.txt).

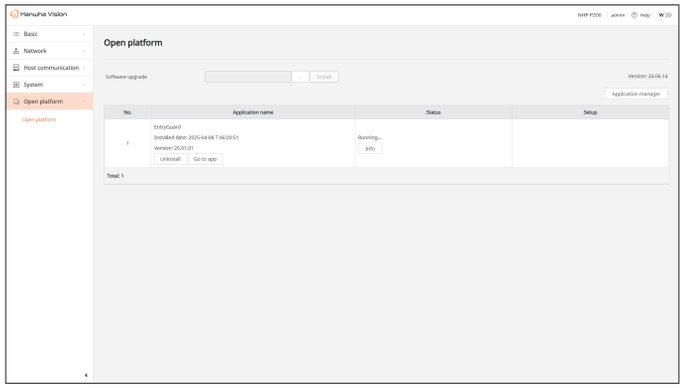
OPEN PLATFORM

To allow for the use of various features, the IP Controller supports the installation of third-party applications alongside the built-in EntryGuard.

- EntryGuard cannot be deleted, even with a factory reset.

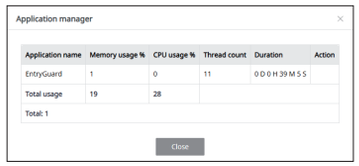
Open platform

Open platform > Open platform



- **Software upgrade**: You can upgrade to the latest application or install other applications.
  Click < ... > to select the application file, then click <**Install**>.
  - You can install up to 10 applications.
- **Application name**: You can check the name, installation date, and version of the application.
  - **Uninstall**: You can delete the selected application.
  - **Go to app**: Go to the web screen of the selected application.
- **Status**: Display the operation status of the application.
  - **Info**: Display the name, memory usage, CPU usage, thread count, and runtime of the application.
- **Setup**: For third-party applications other than EntryGuard, click < ↓ > to change the application settings.
  - **Priority**: You can change the priority for forced termination of the IP Controller when CPU usage is high. Select <**High**>, <**Medium**>, or <**Low**>.
  - **Auto start**: Check <**Enable**> to launch the application when the IP Controller's main task starts.

- **Application manager**: Display the name, memory usage, CPU usage, thread count, and runtime of the applications in use.



  - If the IP Controller's memory usage or CPU usage exceeds 80%, applications with lower priority and higher memory usage may be terminated to protect the system.

starting applications

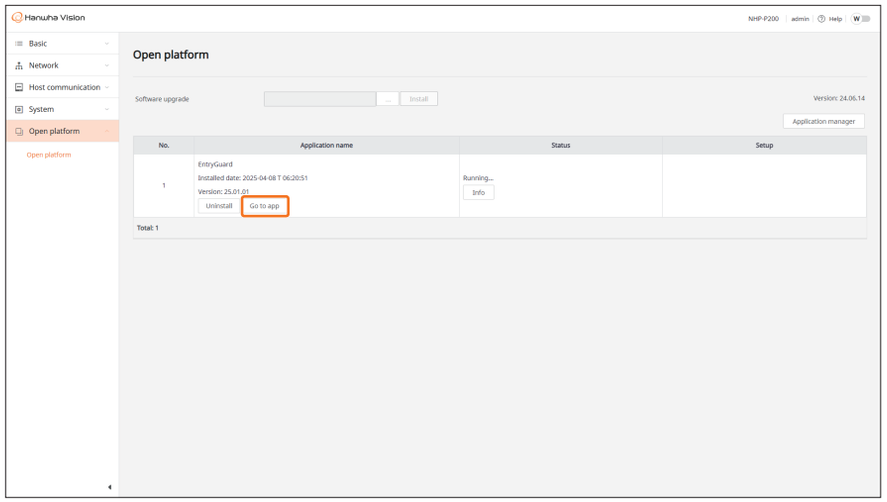
You can configure remote monitoring and efficient access management using the open platform application **EntryGuard**.

From the following menu, click <**Go to app**> to start the application. Click <**Go to app**> to display the EntryGuard application screen.

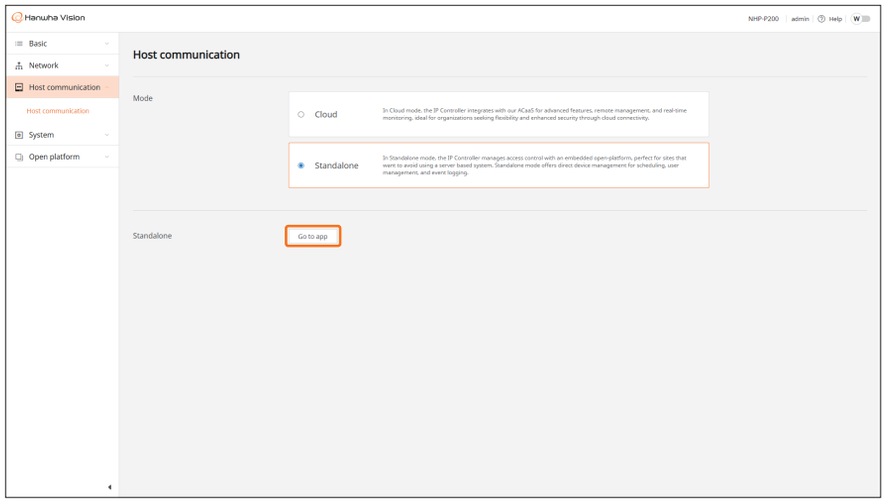
When you access EntryGuard for the first time, the initial setup screen will appear. Proceed with the step-by-step setup for the <**Access**> menu, or click <**Skip**> if you do not wish to configure it now.

For details on the step-by-step setup, refer to the item-specific guide in the <**Access**> menu.

Open platform > Open platform > Go to app



Host communication > Host communication > Go to app



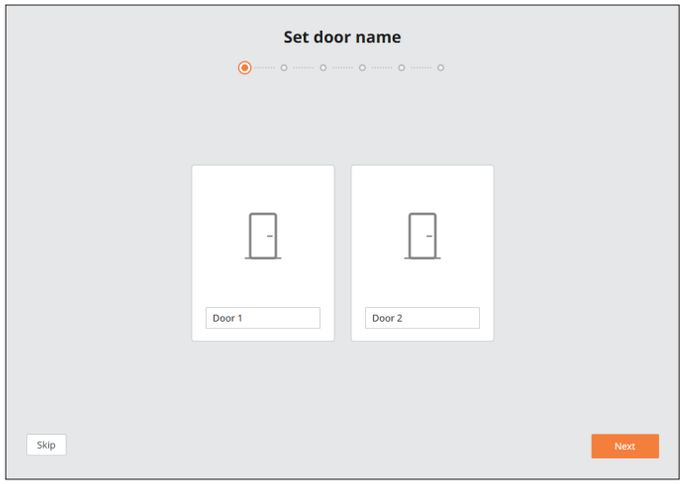
INITIAL SETUP

When you access EntryGuard for the first time, proceed with the step-by-step initial setup.

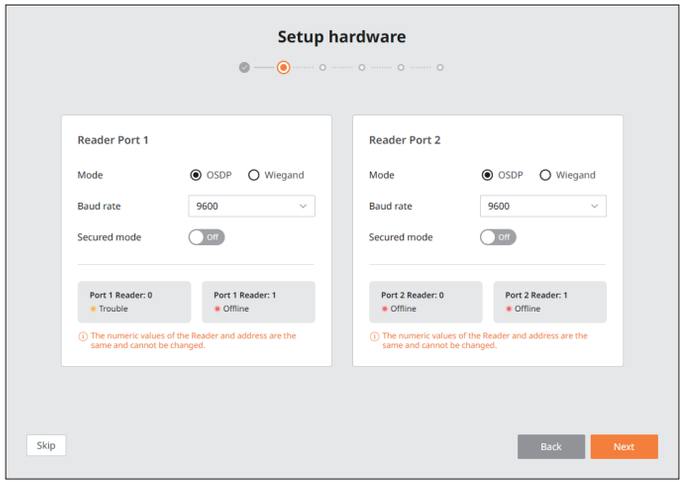
You can configure the door peripherals, operational settings, event alarms, and schedules.

If you do not wish to configure it, click <**Skip**>. You may continue by clicking <**Initial setup**> in the <**Access**> menu.

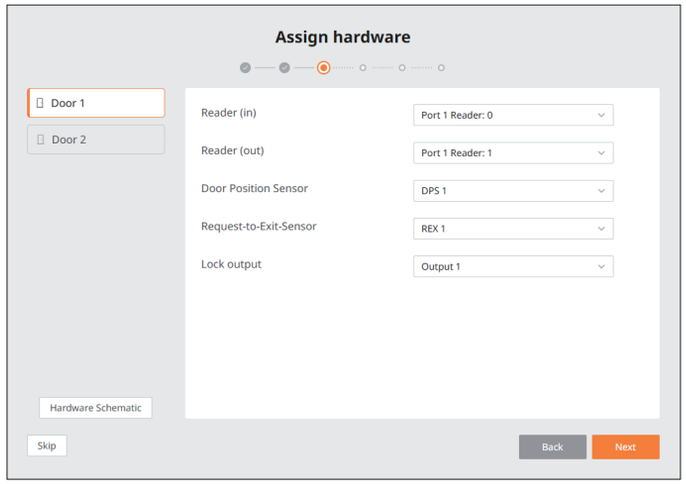
1. Set a name for each door and click <**Next**>.



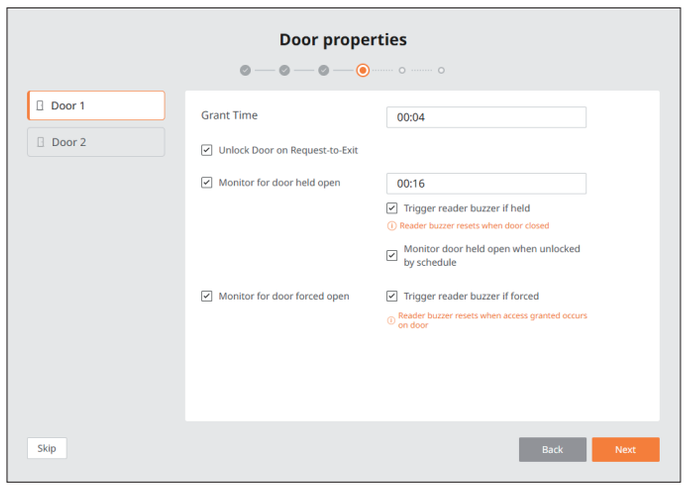
2. Configure the protocol mode of the reader connected to the door, then click <**Next**>.



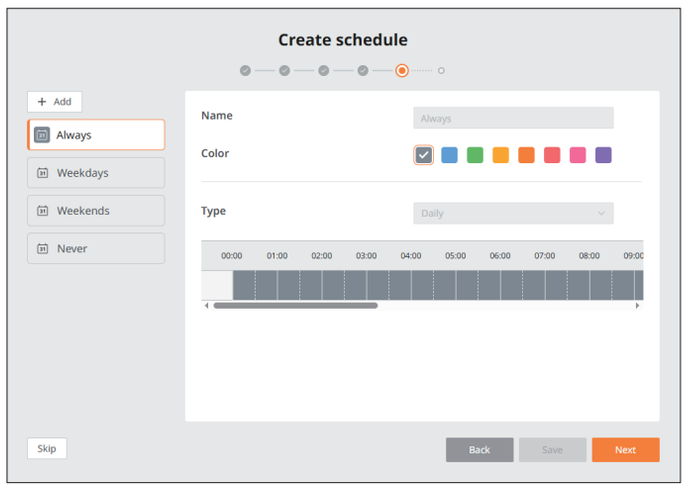
3. Configure the ports for the reader connected to the door, input, and output, then click <**Next**>.



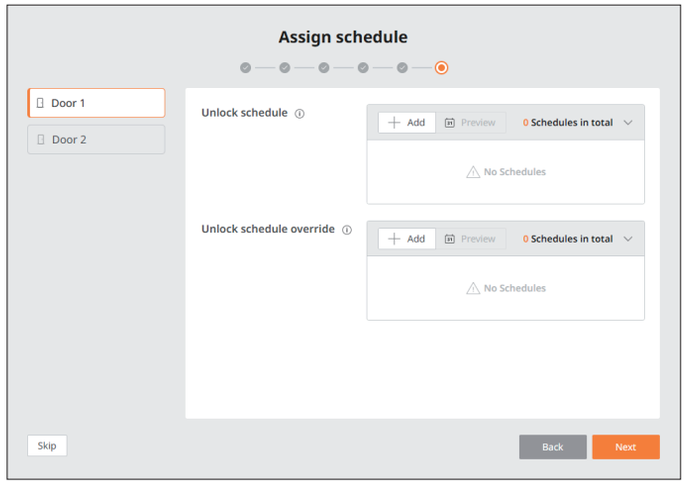
4. Configure the door locks and event alarms, then click <**Next**>.



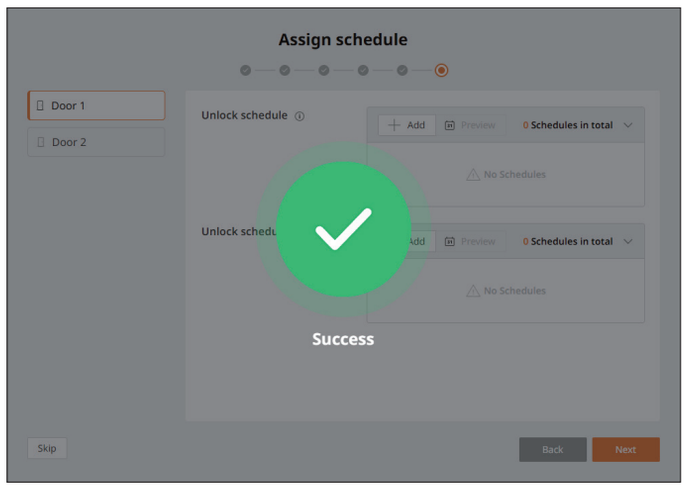
5. Modify or create new schedules for the door.
Click <**Save**> to save, then click <**Next**>.



6. Configure the unlock or temporary lock schedules for the door, then click <**Next**>.



7. When the setup is complete, a <**Success**> message will appear and you will be returned to the <**Access**> menu.



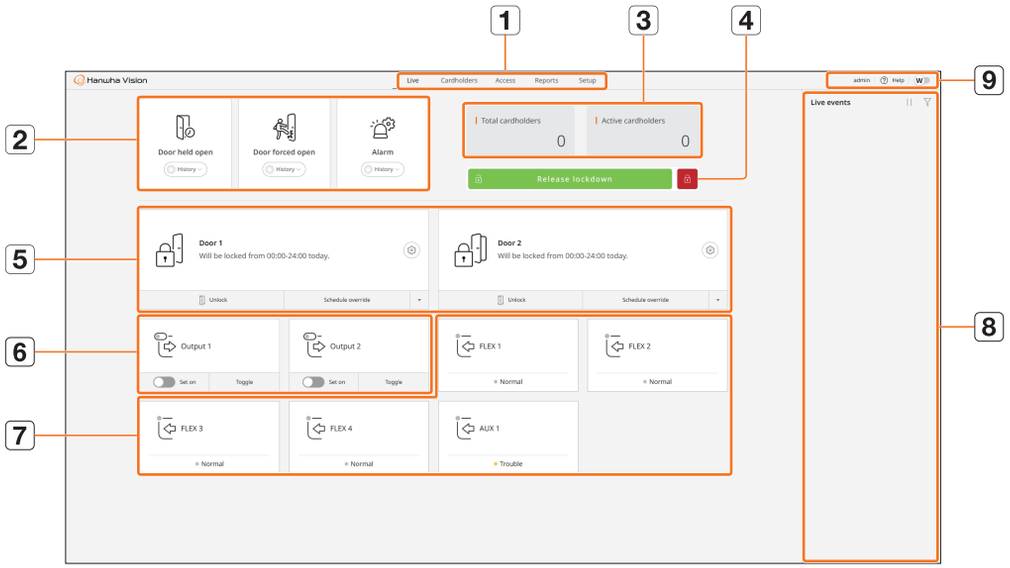
live

You can check the list of real-time events and the status of devices or cardholders connected to the IP Controller.

CONFIGURING LIVE SCREEN

The layout of the live screen is as follows.

Live



Description		Description
1	**Menu**	Click the menu to go to the selected menu screen.
2	**Alarm widget**	Display the event status for <**Door held open**>, <**Door forced open**> and <**Alarm**>. The event widget will blink when an event occurs. You can click <**History**> to clear it. To check the event occurrence history, click "**History** > **Go to report**". ● You can release notifications and view event history via HTTPS.
3	**Cardholder status**	Display the status of cardholders. ● You can view cardholder status via HTTPS.
4	**Lockdown** **Release lockdown**	You can lock or release all doors. ● If you click < >, all doors are locked and access authority is suspended. ● To release the lockdown, click < >.

Description		Description
5	**Door widget**	Display the lockdown status of entrance doors and the schedule for the day. ● : Click < > to go to the "**Access** > **Door configuration**" menu. You can check and modify entrance door settings. ● **Unlock**: You can temporarily unlock an entrance door. ● **Schedule override**: You can temporarily modify the lock or unlock schedule set for entrance doors. Click <▼>, then select <**Lock**> or <**Unlock**>. Set the time and click <**OK**> to add a temporary schedule. To delete a temporary schedule, select the desired schedule and click <**Delete**>.
6	**Output widget**	Display the operational status of output devices that are connected to the IP Controller but do not have functions assigned to entrance doors. ● **Set on**: You can turn the power to the output terminals on and off. ● **Toggle**: You can invert the status of the output terminals for one second. ● Output devices assigned to entrance doors are not displayed.
7	**Input widget**	Display the operational status of input devices connected to the IP Controller. ● Input devices assigned to entrance doors are not displayed.
8	**Live events list**	Display a list of real-time events. You can check the event name, the occurrence time, and information on the event-related entrance door. ● **II/▷**: You can pause or resume the reception of real-time events. ● : You can filter and display specific events. Click < > and check the event item you want to receive in real-time. ● Events that are not activated in the "**Access** > **Event monitor**" menu will not appear in the list.
9	**admin**	Display the user's ID.
	Help	Display the help pop-up window.
	W	You can change the color theme of the web viewer.

setting cardholder

Access can be authenticated using a card or PIN through the reader connected to the IP Controller. You can also create a cardholder group and add cardholders to the group.

- You can set up cardholders via HTTPS.

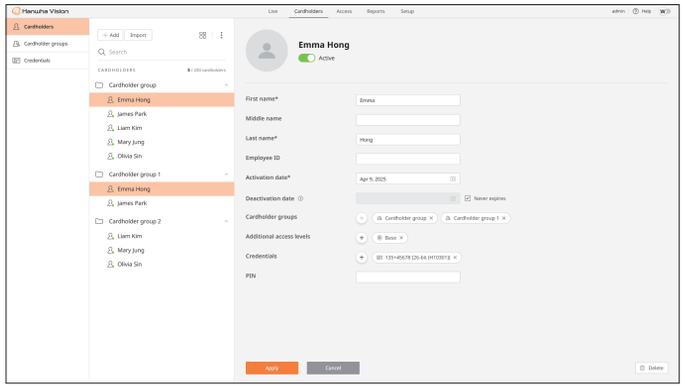
CARDHOLDERS

You can modify registered cardholder information or add or delete cardholders. When adding cardholders, you can use a separate list file. You can also sort a cardholder list by preferred format or criteria and search for specific groups.

Checking the Cardholders List

You can check the list of registered cardholders and modify their information or delete them.

Cardholders > Cardholders

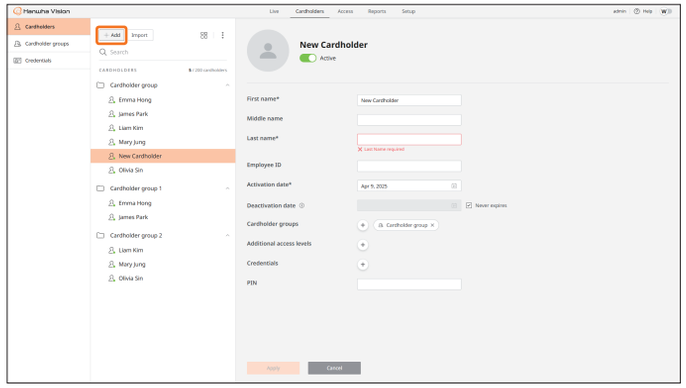


- **Add**: You can add new cardholders.
- **Import**: You can import a separate cardholder list file (CSV).
- : You can check registered cardholders in thumbnail or list format.
- : You can sort registered cardholders by group, activation status, access level, or name.
- **Search**: You can search by entering the name or part of the name.
- **Delete**: You can delete the selected cardholder(s). Select the cardholder(s) to delete from the list and click <**Delete**>.

Adding Cardholders

You can add new cardholders. When adding a cardholder, you can create the cardholder group, access level, and credential.

Cardholders > Cardholders > Add



To add a new cardholder, click <**Add**>.

- : You can add a representative image for the cardholder. Click < > to select an image file for the cardholder or drag and drop the file on < >. JPEG files up to 500 KB are supported.
- **Active**: You can set the activation status of the cardholder.
- **First name*** / **Middle name** / **Last name***: Enter the cardholder's name.
- **Employee ID**: Enter the cardholder's employee ID.
- **Activation date*** / **Deactivation date**: Click < 31 > and select the dates or the cardholder's credential (card type) to be activated and deactivated.
  - If <**Never expires**> is checked, the deactivation date is not selectable and the cardholder's credential will remain active after the activation date.
- **Cardholder groups**: Click <✚> to select the group to which the cardholder belongs.
  - **Search**: You can search by entering the cardholder group name or part of the name.
  - **Create**: You can add a new cardholder group.
    - For information on creating a cardholder group, refer to **Adding Cardholder Groups**.
- **Additional access levels**: Click <✚> to select the access level of the cardholder.
  - **Search**: You can search by entering the access level name or part of the name.
  - **Create**: You can add a new access level.
    - For information on creating an access level, refer to **Adding Access Levels**.
- **Credentials**: Click <✚> to select the credential of the card type that will be used by the cardholder.
  - **Search**: You can search by entering the credential name or part of the name.
  - **Create**: You can add new credentials.
    - For information on creating a credential, refer to **Adding Credentials**.
- **PIN**: Enter the PIN for the cardholder.

- * indicates a required field.
- You can register up to 200 cardholders.
- Each cardholder can register two card type credentials and one PIN.

setting cardholder

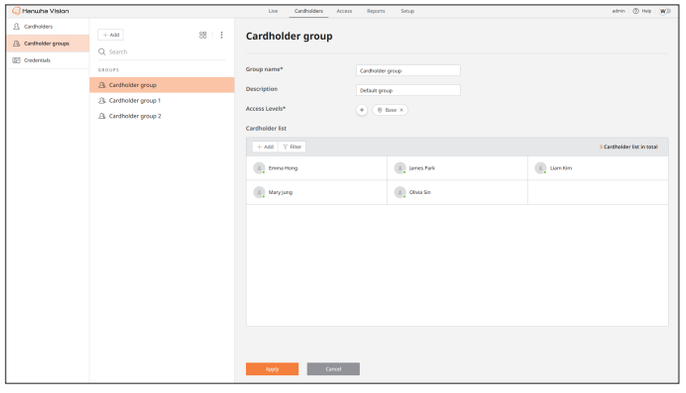
CARDHOLDER GROUPS

You can modify the information of registered cardholder groups or add or delete groups. You can also sort the group list by preferred format or criteria and search for specific groups.

Checking the Cardholder Groups List

You can check the list of registered cardholder groups and modify information or delete groups.

Cardholders > Cardholder groups

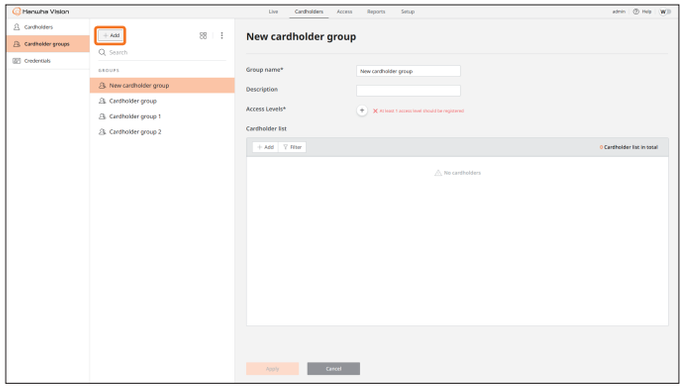


- **Add**: You can add a new cardholder group.
- : You can check registered cardholder groups in thumbnail or list format.
- : You can sort registered cardholder groups by access level or name.
- **Search**: You can search by entering the cardholder group name or part of the name.
- **Delete**: You can delete selected cardholder groups. Select the cardholder group to delete from the list and click <**Delete**>.

Adding Cardholder Groups

You can add a new cardholder group. When adding a cardholder group, you can create and add an access level.

Cardholders > Cardholder groups > Add



To add a new cardholder group, click <**Add**>.

- **Group name***: Enter the cardholder group's name.
- **Description**: You can enter an additional description about the cardholder group.
- **Access levels***: Click <**+**> to select the access level for the cardholder group.
  - For information on creating an access level, refer to **Adding Access Levels**.
- **Cardholder list**: Click <**Add**> to select cardholders to include in the group.
  - **Search**: You can search by entering the name or part of the name.
  - **Filter**: You can sort by group status (active or inactive) or by cardholder name.

* indicates a required field.

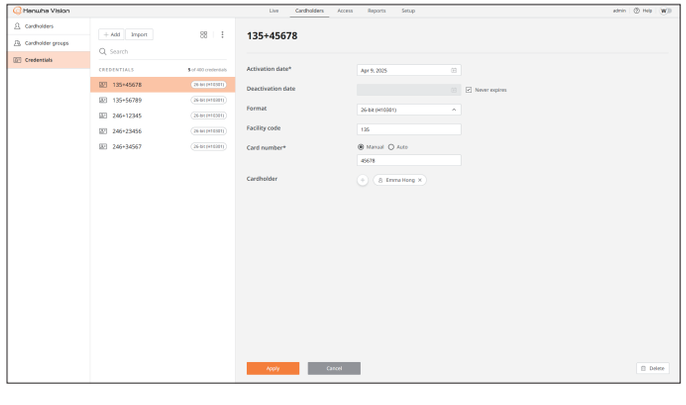
CREDENTIALS

You can modify the credential information of registered cardholders, or add or delete credentials. When adding credentials for a cardholder, you can use a separate list file. You can also sort a credentials list by preferred format or criteria and search for specific credentials.

Checking the Credentials List

You can check the list of registered credentials and modify information or delete credentials.

Cardholders > Credentials

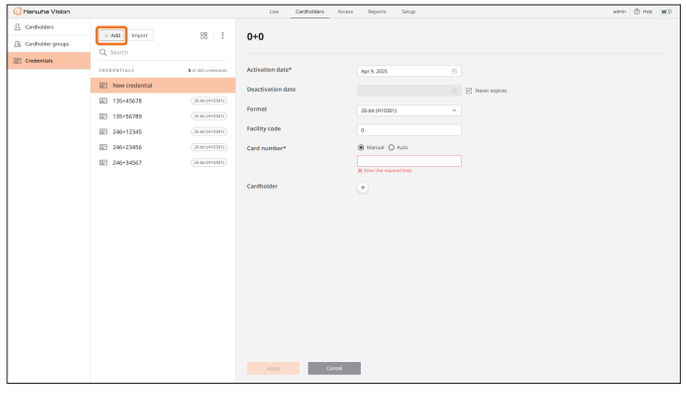


- **Add**: You can add new credentials.
- **Import**: You can import a separate credentials list file (CSV).
- : You can check registered credentials in thumbnail or list format.
- : You can sort registered credentials by name. Click <**Show format info**> to toggle the display of the credential's format information.
- **Search**: You can search by entering the credential name or part of the name.
- **Delete**: You can delete selected credentials. Select the credential to delete from the list and click <**Delete**>.

Adding Credentials

You can add new credentials for cardholders to use.

Cardholders > Credentials > Add



To add a new credential, click <**Add**>.

- **Activation date*** / **Deactivation date:** Click < 31 > and select the dates for the cardholder's credential (card type) to be activated and deactivated.
  - If <**Never expires**> is checked, the deactivation date is not selectable and the cardholder's credential will remain active after the activation date.
- **Format**: Select the format for the credential information.
- **Facility code**: Enter the facility code.
  - The facility code can be selected based on the credential type.
- **Card number***: Register the card number.
  - To scan and register a card, select <**Auto**>.
    After tagging the card on the card reader, select <**Load**> to display the card number.
    Click <**Apply**> to register the card number.
  - To manually enter and register the card number, select <**Manual**>.
    Enter the card number and the card will be registered.
- **Cardholder**: Click <**+**> to select cardholders to use the registered credential.
  - **Search**: You can search by entering the name or part of the name.

- * indicates a required field.

setting access

You can configure the door peripherals, operational settings, event alarms, and schedules.

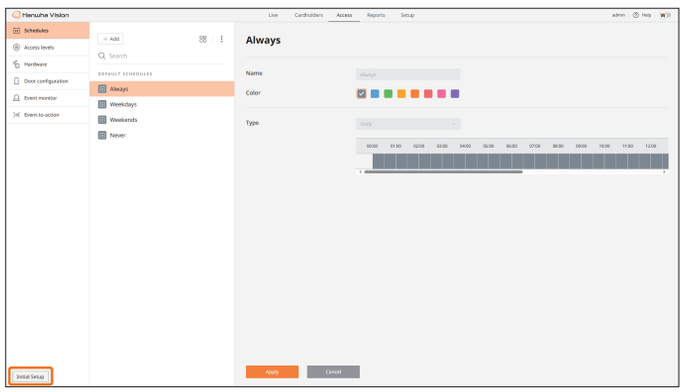
INITIAL SETUP

Proceed with the step-by-step setup for the <**Access**> menu.

For details on the step-by-step setup, refer to the item-specific guide in the <**Access**> menu.

If you do not wish to configure it, click <**Skip**>.

Access > Initial setup



SCHEDULES

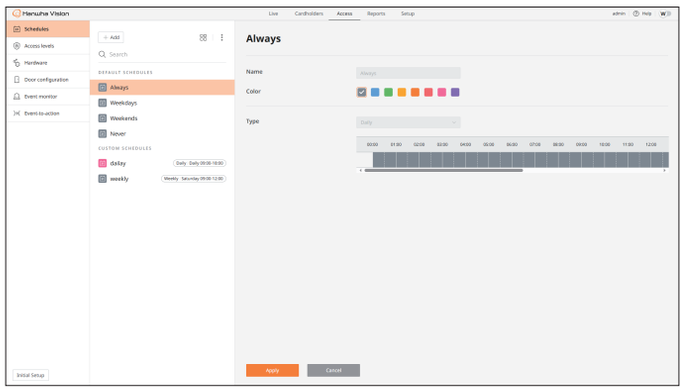
You can modify registered schedule information or add or delete a schedule. Schedules can be applied to entrance doors and access levels.

You can also sort and search schedules by preferred format or criteria.

Checking the Schedules List

You can check the list of registered schedules and modify information or delete schedules.

Access > Schedules

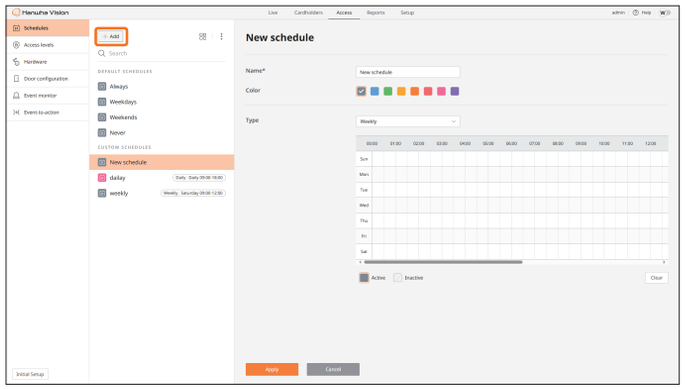


- **Add**: You can add new schedules.
- : You can check registered schedules in thumbnail or list format.
- : You can sort registered schedules by name. Click <**Show detail**> to toggle the display of the schedule's configuration details.
- **Search**: You can search by entering the schedule name or part of the name.
- **Delete**: You can delete the selected schedule(s). Select the schedule(s) to delete from the list and click <**Delete**>.
- **DEFAULT SCHEDULES**: You can check the schedules set as default.
  Default schedules cannot be deleted, and settings other than color cannot be modified.
  - **Always**: A schedule that includes all times, every day.
  - **Weekdays**: A schedule that includes Monday to Friday, from 09:00 to 18:00.
  - **Weekends**: A schedule that includes Saturday and Sunday, from 09:00 to 18:00.
  - **Never**: A schedule with no time, date, or days of the week included.
- **Name**: The name of the schedule, which cannot be changed.
- **Color**: The color of the schedule. You may change it if desired.
- **Type**: The type of the schedule, which cannot be changed.

Adding Schedules

You can add new schedules. Schedules can be applied to entrance doors and access levels.

Access > Schedules > Add



To add a new schedule, click <**Add**>.

- **Name***: Enter the schedule name.
- **Color**: Enter the color of the schedule.
- **Type**: Select the schedule type.
  - **Weekly**: Create a schedule that repeats weekly.
  - **Daily**: Create a schedule that repeats daily.
  - **Ordinal**: Create a schedule that repeats annually.
  - **Specific**: Create a non-repeating schedule for a specific time period.
- **Active**: You can select dates or time fields from the schedule table.
- **Inactive**: You can delete selected dates or time fields from the schedule table.
- **Clear**: You can delete all selected fields from the schedule table.

- * indicates a required field.
- You can create up to 16 schedules.

ACCESS LEVELS

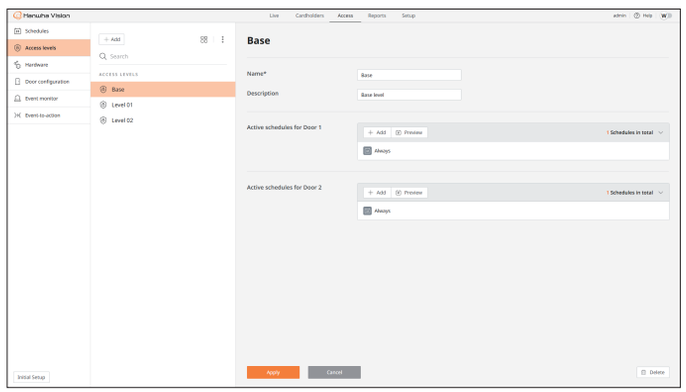
You can modify the information of the registered access levels or add or delete access levels. Access levels can be applied to each entrance door by setting schedules.

You can also sort access levels by preferred format or criteria and search for specific access levels.

Checking the Access Levels List

You can check the list of registered access levels and modify information or delete levels.

Access > Access levels

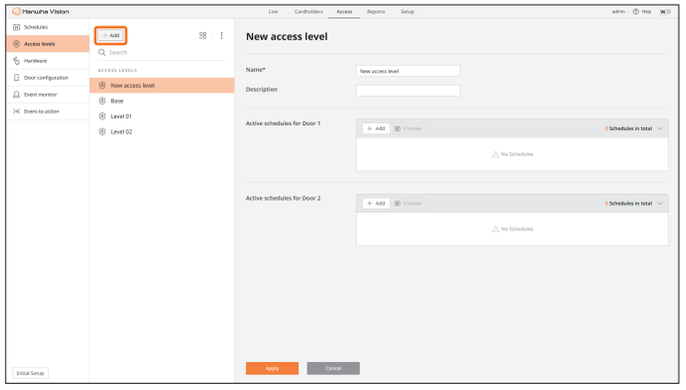


- **Add**: You can add a new access level.
- : You can check registered access levels in thumbnail or list format.
- : You can sort registered access levels by name.
- **Search**: You can search by entering the access level name or part of the name.
- **Delete**: You can delete the selected access level(s). Select the access level(s) to delete from the list and click <**Delete**>.

Adding Access Levels

You can add a new access level. Access levels can be applied to each entrance door by setting schedules.

Access > Access levels > Add



To add a new access level, click <**Add**>.

- **Name***: Enter the name of the access level.
- **Description**: You cna enter an additional description about the access level.
- **Active schedules for Door**: You can add action schedules for each entrance door.
  - **Add**: Select the schedule(s) to apply to the entrance door. You can select up to four schedules for each door.
  - **Search**: You can search by entering the schedule name or part of the name.
  - **Create**: You can add new schedules.
    - For information on creating a schedule, refer to **Adding Schedules**.
  - **Preview**: When one or more schedules are added, <**Preview**> is enabled.
    Click <**Preview**> to display the monthly calendar with the added schedules.
    If more than four schedules are assigned to a single day, click <**more**> to check.
  - If you hover over the schedule you want to delete, < > will appear. Click it to delete the selected schedule from the list.
- **Delete**: You can delete the selected access level(s). Select the access level(s) to delete from the list and click <**Delete**>.

- * indicates a required field.

HARDWARE

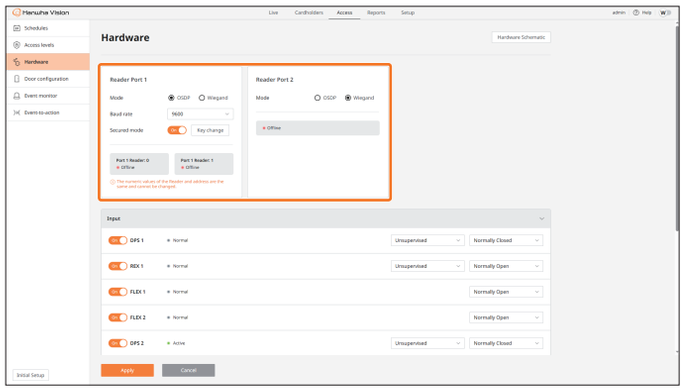
You can check and change the status and settings of readers or input devices connected to the IP Controller.

- The number of devices that can be connected to the IP Controller varies depending on the model.

Reader port

You can set the communication mode of the readers connected to the entrance door.

Access > Hardware > Reader port



OSDP Mode

- **Baud rate**: Select the RS-485 communication speed.
- **Secured mode**: Select <**On**> to enable a secure connection, and then click <**Apply**>.
- **Key change**: You can change the encryption key.
  - The <**Key change**> option is displayed when <**Secured mode**> is set to <**On**>.
- **Port 1 Reader: 0** / **Port 1 Reader: 1**: Display the status of readers with the address set to 0 or 1 connected to each port. Refer to the manufacturer's specifications for reader address settings.
  - **Active**: A reader is connected and operational.
  - **Trouble**: A reader is connected but communication is not established.
  - **Offline**: A reader is not connected.

Wiegand Mode

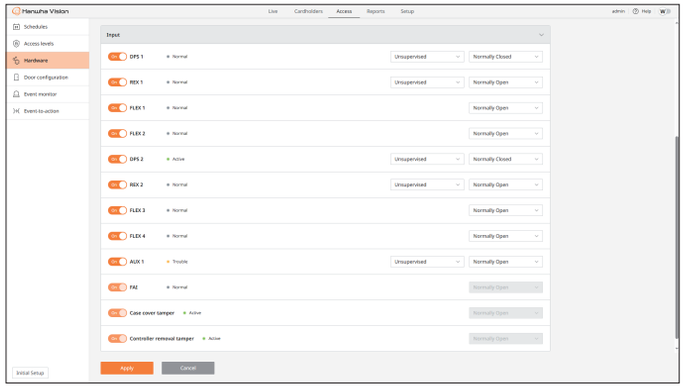
In Wiegand mode, you can connect up to one reader per port and only the operational status can be monitored.

- Refer to the reader manufacturer's manual for instructions on setting the reader mode.

Input

You can check the status of the input devices connected to the entrance door, and configure connectable inputs and connection methods.

Access > Hardware > Input



- **On** / **Off**: You can enable or disable the device.
- You can check the status of input devices connected to the entrance door.
  - **Disabled**: The device is not operating and is not being monitored.
  - **Normal**: The devices is being monitored and is operating normally.
  - **Active**: The device is being monitored and is active.
  - **Trouble**: The device is being monitored but is experiencing an issue such as disconnection.
  - **Unavailable**: The input cannot be used. To use this input, set the reader port to <**OSDP**> mode.
- **Unsupervised**: Select while no resistor is connected to the input device.
- **Supervised**: Select while a resistor is connected to the input device. You can monitor the <**Trouble**> status of the input device.
  Only input devices connected to DPS, REX, and AUX inputs can be set to <**Supervised**>.
- **Normally Open**: The contact of the input device is open in the <**Normal**> state. The device becomes <**Active**> when the contact is closed.
- **Normally Closed**: The contact of the input device is closed in the <**Normal**> state. The device becomes <**Active**> when the contact is opened.

- <**FLEX**> is enabled exclusively in OSDP mode and functions as an input.
- The <**FAI**>, <**Case cover tamper**>, and <**Controller removal tamper**> settings cannot be changed.

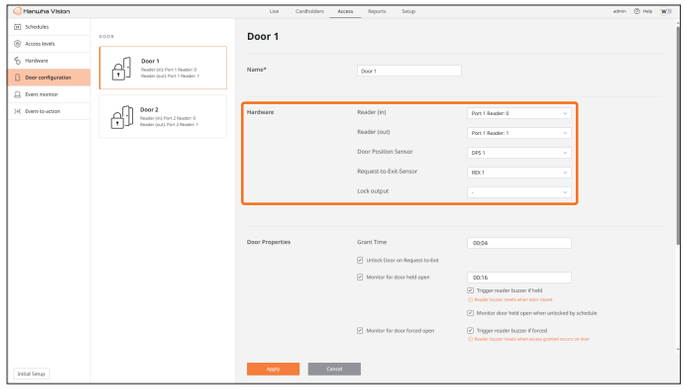
DOOR CONFIGURATION

You can set configuration and operational settings or assign lock schedules for peripheral devices of entrance doors.

Hardware

You can configure the direction (IN/OUT) and the input and output ports of readers connected to the door.

Access > Door configuration > Hardware



- **Reader (in)**: Select the reader installed at the door entrance.
- **Reader (out)**: Select the reader installed at the door exit.
- **Door Position Sensor**: Select the number of the input port connected to the door position sensor.
- **Request-to-Exit-Sensor**: Select the number of the input port connected to the door request-to-exit sensor.
- **Lock output**: Select the number of the door lock output port.

- Ensure the numbers for all entrance doors and input ports are set differently.
- Check the input and output ports according to the IP Controller model.

NHP-P200

Input/Output	OSDP Mode	Wiegand Mode
DSP / REX	Input ports DPS1, 2 / REX1, 2 / FLEX1–4 / AUX1	Input ports DPS1, 2 / REX1, 2/ AUX1
Lock output	Output ports 1, 2	

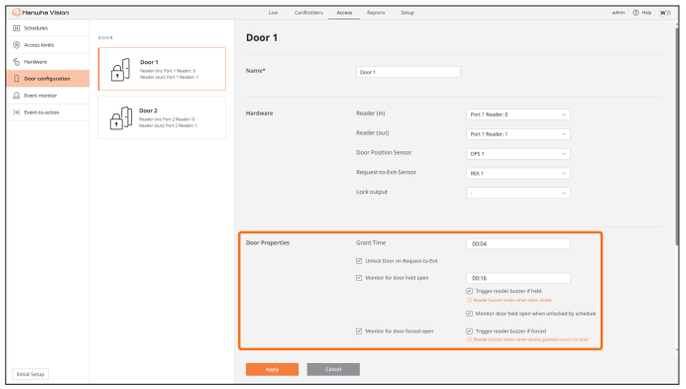
NHP-P100

Input/Output	OSDP Mode	Wiegand Mode
DSP / REX	Input ports DPS1 / REX1 / FLEX1–2 / AUX1	Input ports DPS1 / REX1 / AUX1
Lock output	Output port 1	

Door properties

You can set the entrance door lock devices and event alarms.

Access > Door configuration > Door properties

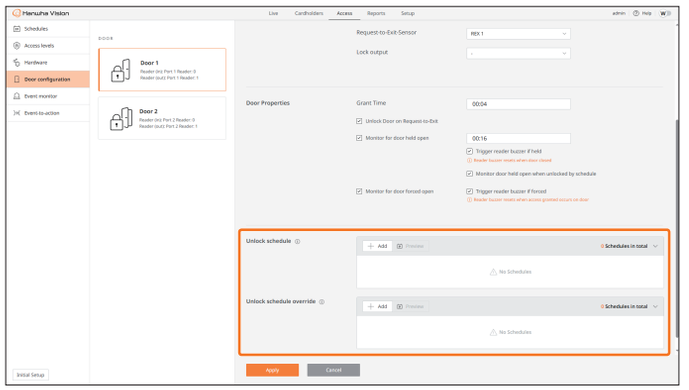


- **Grant time**: You can set how long the door remains unlocked.
  It cannot exceed the <**Monitor for door held open**> time.
- **Unlock door on Request-to-Exit**: Check this option to unlock the door using the request-to-exit sensor.
- **Monitor for door held open**: To monitor door held events in real-time on the <**Live**> screen, check this option and set the event trigger time (less than 60 seconds).
  A door held event occurs if the door does not lock within the set time after being unlocked.
  - **Trigger reader buzzer if held**: Check this option to trigger an alarm through the reader buzzer if a door held event occurs.
  - **Monitor door held when unlocked by schedule**: Check this option to monitor door held events in real-time when the door remains unlocked according to the set schedule.
- **Monitor for door forced open**: Check this option to monitor door forced events in real-time on the <**Live**> screen. A door forced event occurs when the door is open while the door lock remains locked.
  - **Trigger reader buzzer if forced**: Check this option to trigger an alarm through the reader buzzer if a door forced event occurs.

Unlock schedule / Unlock schedule override

You can set a schedule for unlocking the entrance door. You can also set a schedule to temporarily cancel an unlock schedule and keep the door locked.

Access > Door configuration > Unlock schedule / Unlock schedule override

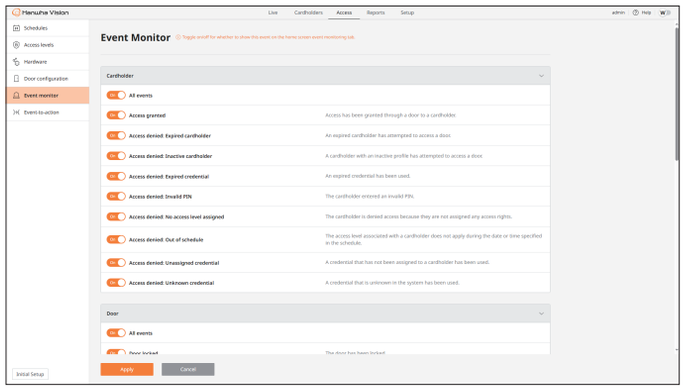


- **Unlock schedule**: You can set a schedule for unlocking the entrance door.
  - **Add**: Select the schedule(s) to apply to the entrance door. You can select up to eight schedules for each door. You can enter the name or a part of the name of the schedule in <**Search**> to search.
  - **Preview**: When one or more schedules are added, <**Preview**> is enabled.
    Click <**Preview**> to display the monthly calendar with the added schedules.
    If more than four schedules are assigned to a single day, click <**more**> to check.
  - : If you hover over the schedule you want to delete, < > will appear. Click it to delete the selected schedule from the list.
- **Unlock schedule override**: You can set a schedule to temporarily cancel the door unlock schedule and keep the door locked.
  - **Add**: Select the schedule(s) to apply to the entrance door. You can select up to eight schedules for each door. You can enter the name or a part of the name of the schedule in <**Search**> to search.
  - **Preview**: When one or more schedules are added, <**Preview**> is enabled.
    Click <**Preview**> to display the monthly calendar with the added schedules.
    If more than four schedules are assigned to a single day, click <**more**> to check.
  - : If you hover over the schedule you want to delete, < > will appear. Click it to delete the selected schedule from the list.

EVENT MONITOR

You can set real-time monitoring for event items triggered by cardholders, entrance doors, and devices.

Access > Event monitor

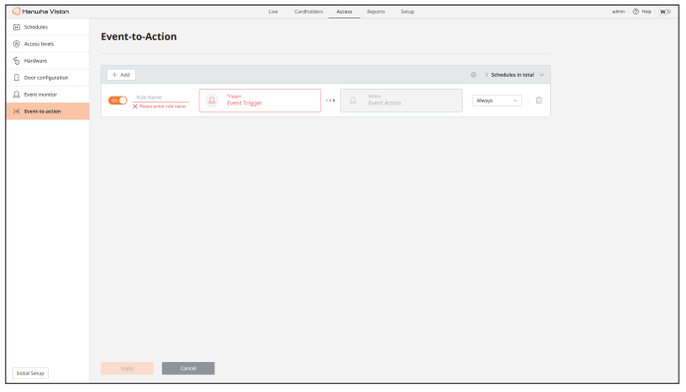


- **On** / **Off**: You can select whether to monitor the event in real time.
- **All events**: If you select <**On**> or <**Off**>, it will apply to all items within the <**Cardholder**>, <**Door**>, and <**Device**> categories.
- **Cardholder**: You can select event items to deny or grant access to based on the access levels and credentials status of the cardholder.
  - **Access granted**: Access has been granted to the cardholder.
  - **Access denied: Expired cardholder**: Access has been denied due to an expired cardholder access level.
  - **Access denied: Inactive cardholder**: Access has been denied due to an inactive cardholder access level.
  - **Access denied: Expired credential**: Access has been denied due to an expired cardholder credential.
  - **Access denied: Invalid PIN**: Access has been denied due to an incorrect PIN.
  - **Access denied: No access level assigned**: Access has been denied due to no access level being assigned.
  - **Access denied: Out of schedule**: Access has been denied due to an incorrect schedule for the cardholder access levels.
  - **Access denied: Unassigned credential**: Access has been denied due to the use of a credential not assigned to the cardholder.
  - **Access denied: Unknown credential**: Access as been denied due to the use of an unknown credential in the system.
- **Door**: You can select event items related to the locking/schedule status of entrance doors.
  - **Door locked**: The entrance door has been locked.
  - **Door unlocked**: The entrance door has been unlocked.
  - **Door closed**: The entrance door has been closed. Install a door sensor to use this event.
  - **Door opened**: The entrance door has been opened. Install a door sensor to use this event.
  - **Door forced open**: The entrance door has been forced open. The entrance door is open but the door lock remains locked.
  - **Door open too long**: The entrance door has remained open beyond the set time. The entrance door did not lock within the set time after being unlocked.
  - **Door lock down**: All entrance doors have been locked. Access is restricted.
  - **Lock down release**: Access restrictions on the entrance door have been lifted.
- **Device**: You can select event items related to opening the device's case, fire detection, and the status of input/output devices.
  - **Input active**: The input is active.
  - **Input normal**: The input is operating normally.
  - **Input trouble**: The input has encountered a problem.
  - **Reader tamper**: The reader (OSDP) settings have been changed.
  - **Reader active**: The reader (OSDP) is active.
  - **Reader trouble**: The reader (OSDP) encountered a problem.
  - **Reader offline**: The reader (OSDP) is offline.
  - **Output activated**: The output is active.
  - **Output normal**: The output is operating normally.
  - **Case cover tamper**: The IP Controller cover has been removed.
  - **Controller removal tamper:** The IP Controller has been removed from the wall.
  - **Fire alarm**: The fire alarm has been triggered.
  - <**Case cover tamper**>, <**Controller removal tamper**>, and <**Fire alarm**> events cannot be set to <**Off**>.

EVENT-TO-ACTION

You can set event triggers and action rules to output alarms when events occur.

Access > Event-to-action



- **Add**: Add a new event rule.
- **On** / **Off**: You can select whether use the event rule.
- **Rule name**: Enter the name of the event rule.
- **Event trigger**: Select an event trigger.
- **Event action**: Select an event action.
- **Always**: Select a schedule to run the event action. Schedules created under "**Access** > **Schedules**" and the default schedule list will be displayed.
- : You can delete selected event rules.

setting report

You can search logs of cardholders, doors, devices connected to doors, and system events by applying dates or filters. You can also export search results as a file (.csv).

■ You can configure reports via HTTPS.

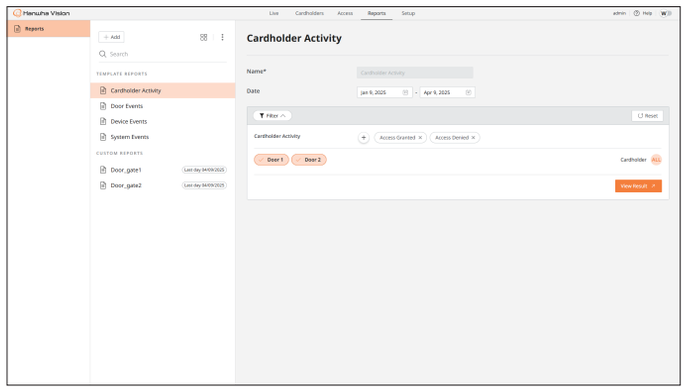
REPORTS

You can modify the information of registered reports or add or delete reports. You can also sort the reports list by preferred format or criteria and search for specific reports.

Checking the Reports List

You can check the list of registered reports and modify information or delete reports.

Reports > Reports

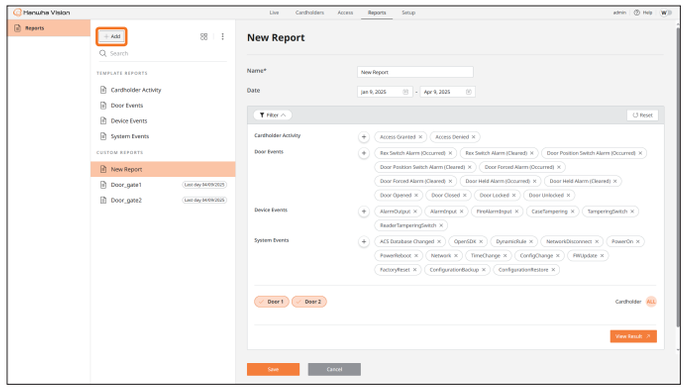


- **Add**: You can add new reports.
- : You can check reports in thumbnail or list format.
- : You can sort the list of registered reports by name. You can click <**Show last history**> to sort reports in the order of the most recently saved information.
- **Search**: You can search by entering the report name or part of the name.
- **Delete**: You can delete the selected report(s). Select the report(s) to delete from the list and click <**Delete**>.
- **TEMPLATE REPORTS**: You can search logs from default report templates by filtering the desired event items.
  - **Cardholder Activity**: Reports on movements and access attempts by cardholders.
  - **Door Events**: Reports on openings, closings, and access attempts of entrance doors.
  - **Device Events**: Reports on inputs and outputs of devices connected to entrance doors.
  - **System Events**: Reports on system events, including start/stop, configuration change, etc., of devices.

Adding Reports

You can add new reports.

Reports > Reports > Add



To add a new report, click <**Add**>.

- **Name***: Enter the report name.
- **Date**: Select dates to search logs. Click < 31 > to select the start and end dates, then click <**OK**>.
- **Filter**: You can filter the items to include in the report. Select log items related to cardholders, doors, devices, and systems.
  - **+**: Select events to search. You can enter the name or part of the name of the event in <**Search**> to search. Select the desired event, then click <**OK**>.
  - **X**: You can delete the selected report(s).
  - **Door**: Select doors to search.
  - **Cardholder**: Click <**+**> to select a cardholder to search. You can enter the name or part of the name of the cardholder in <**Search**> to search. Select the desired cardholder, then click <**OK**>.
  - **View Result**: You can check the search results. Click <**Export**> to save the search results as a file. The file (CSV) will be stored in the designated download path.
- **Reset**: You can initialize and reset log items.
- **Save**: You can save newly added reports or reports with modified settings.

■ * indicates a required field.

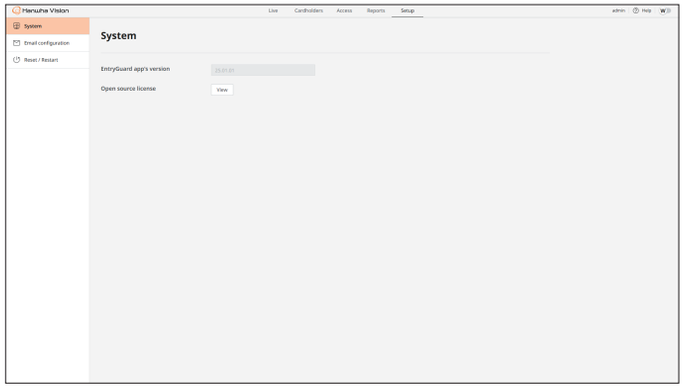
setting application

You can check application versions. You can register licenses and settings related to the SMTP server and email. You can also reset the application settings or backup the settings information or restore it by applying backup settings.

SYSTEM

You can check application versions.

Setup > System

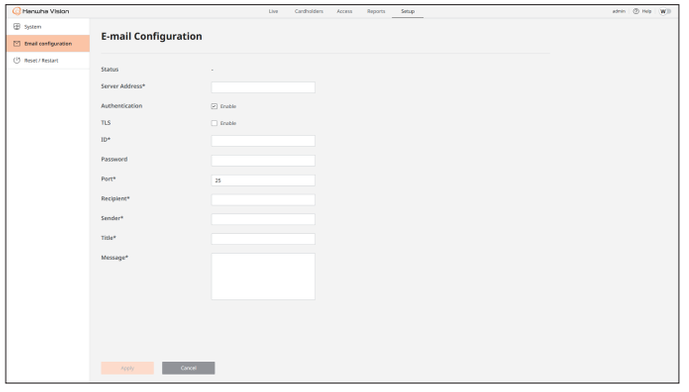


- **EntryGuard app's version**: You can check application versions.
- **Open source license**: You can click <**View**> to check the product's open source license information.

EMAIL CONFIGURATION

When sending emails as part of event actions, you can set the SMTP server, the recipient/sender email addresses, and the message to be sent.

Setup > Email configuration



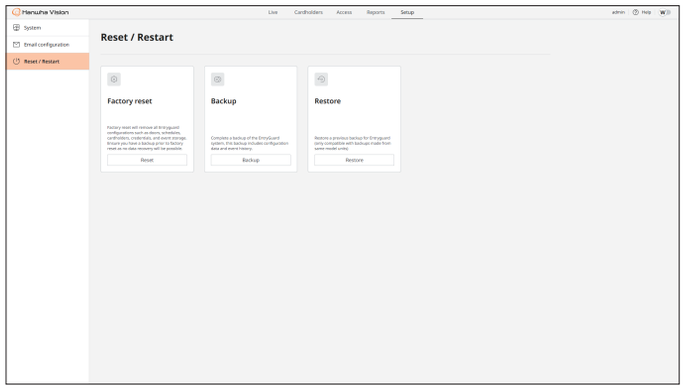
- **Status**: Before email configuration, <**Trying**> is displayed.
  After entering the details below, click the <**Apply**> button. If the settings are correct, the status will be <**Pass**>. If <**Fail**> is displayed, check and correct the settings.
- **Server address***: To send images from the event trigger time via email, enter the email SMTP server address. Limited to 64 characters.
- **Authentication**: To perform ID and password authentication for sending emails, check <**Enable**>.
- **TLS**: To use TLS for email servers requiring security, check <**Enable**>.
- **ID***: Enter the ID for the email SMTP server account. Limited to 32 characters, and special characters such as #, %, &, =, +, \, :, ', ", <, > are not allowed.
- **Password**: Enter the password for the email SMTP server account. Limited to 32 characters, and special characters such as #, %, &, =, +, \, :, ', ", <, > are not allowed.
- **Port***: Enter the email SMTP server port. The default is 25, and 465 is used for TLS.
- **Recipient***: Enter the recipient's email address. Limited to 64 characters.
- **Sender***: Enter the sender's email address. Limited to 64 characters, and the email may not be sent if the sender address is incorrect.
- **Title***: Enter the title of the email to be sent when an event occurs. Limited to 60 characters, and \ is not allowed.
- **Message***: Enter the message of the email to be sent when an event occurs. Limited to 255 characters, and \ is not allowed.

▪ * indicates a required field.

RESET / RESTART

You can reset the application settings. You can also save the current settings and restore them later by the applying previously saved settings.

Setup > Reset / Restart



- **Factory reset**: You can reset the application settings.
  When you perform a reset, all EntryGuard settings, including entrance doors, schedules, cardholders, credentials, and event storages, will be removed. Since data cannot be recovered after a reset, ensure that any settings that need to be backed up are saved before proceeding with the reset.
  – Click <**Reset**> to display the <**Confirm**> window. To proceed with the reset, click <**Confirm**>.
    ■ Log information is not deleted in a reset.
- **Backup**: You can save the application settings information.
  – Click <**Backup**> to display the <**Confirm**> window. To proceed with the backup, click <**Confirm**>.
  The current application settings are saved as a .bin file in the download path.
    ■ If authentication information is included when backing up the settings information, it will be encrypted and stored.
- **Restore**: You can restore by applying the saved settings information. You can create multiple settings files and restore desired settings according to the product usage or environment.
  – Click <**Restore**> to display the <**Confirm**> window. To proceed with the restore, click <**Confirm**>.
  Select the saved settings file to restore to the time of the backup. The product will restart after the restoration is complete.

WIRE RECOMMENDATION

Ethernet	CAT-5, 328 ft (100 m) maximum
OSDP	24 AWG 4 conductor twisted pair with shield, 2,000 ft (610 m) maximum
Wiegand	18 AWG 4 conductor with shield, 500 ft (150 m) maximum
Alarm Input	18–22 AWG, 1,000 ft (304 m) maximum
Power/Relay out	18–22 AWG, 500 ft (150 m) maximum
PIR	18–22 AWG, 1,000 ft (304 m) maximum

- Reader Ports are evaluated by UL in condition that length of cable is limited to 98.5ft (30m).

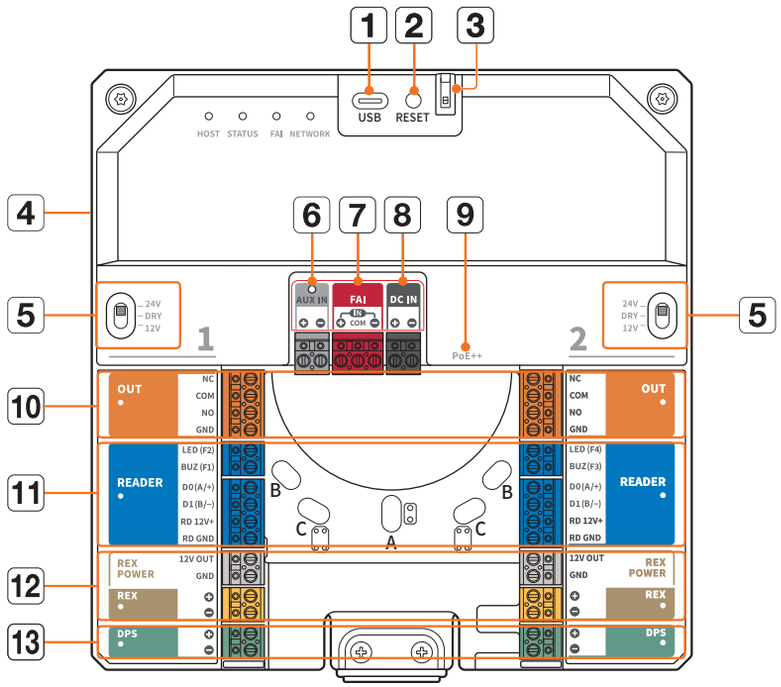
LED INDICATORS

You can check the device status with the LED indicators on this product.

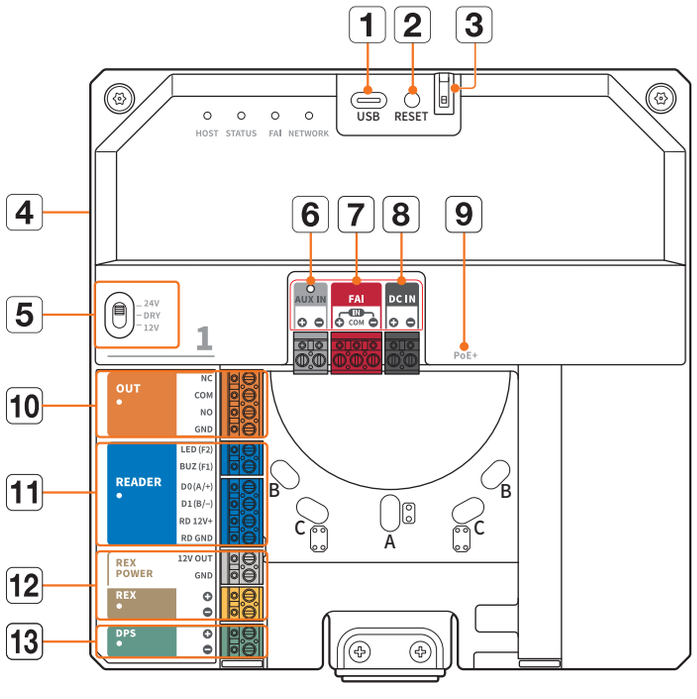
Item	LED	Status
HOST	Green	Stable connection to the host
	Red	Unstable connection or disconnected
	Off	Not connected to the host
STATUS	Green	Operating normally
	Off	Issue with operation
FAI	Red	Fire alarm signal triggered
ETHERNET	Green	Network connection or data transmission in progress
OUT	Green	Wet contact mode, output signal present
	Red	Dry contact mode, output signal present
	Off	Connected to entrance door
READER	Green	Properly connected to reader or in Wiegand mode
	Red	Communication with reader not smooth
	Off	Not connected to reader
REX	Red	• Flashing: Input signal present • Blinking: Monitoring in progress and malfunction in circuit
DPS	Red	• Flashing: Input signal present • Blinking: Monitoring in progress and malfunction in circuit

INTERNAL PART NAMES AND FUNCTIONS

NHP-P200



NHP-P100



	Name	Functions
1	USB	Terminal for connecting USB devices. (USB 2.0 supported)
2	RESET	Resets the device to its factory default settings.
3	Case cover tamper	Detects whether the IP Controller's cover has been removed.
4	Controller removal tamper	Detects whether the IP Controller has been removed from the mount plate. (Located on the rear of the device)
5	24V DRY 12V	Switch for selecting between dry and wet contacts. • **24V / 12V**: Select the appropriate voltage when using wet contacts. • **DRY**: Select when using dry contacts.
6	AUX IN	Terminal for connecting alarm inputs.
7	FAI	Terminal for connecting to the fire alarm panel.
8	DC IN	Terminal for connecting power.
9	PoE++ PoE+	Terminal for connecting network; supports PoE. • NHP-P200: Supports PoE++ • NHP-P100: Supports PoE+
10	OUT	Terminal for alarm output.
11	READER	Terminal for connecting the reader. • **LED (F2) / LED (F4)**: Connects to the LED terminal of the reader. • **BUZ (F1) / BUZ (F3)**: Connects to the buzzer terminal of the reader. • **D0 (A/+)**: Connects to the D0 (A/+) terminal of the reader. • **D1 (B/-)**: Connects to the D1 (B/-) terminal of the reader. • **RD 12V+ / RD GND**: Terminal for providing power to the reader. Connects to the power input terminal of the reader.
12	REX POWER REX	Terminal for connecting Request-to-exit (REX) buttons and passive infrared (PIR) sensors. • **12V OUT**: Terminal for providing power to the PIR sensor. • **GND**: Terminal for connecting the ground wire. • **+/-**: Terminal for connecting Request-to-exit buttons.
13	DPS	Terminal for connecting the door opening sensor.

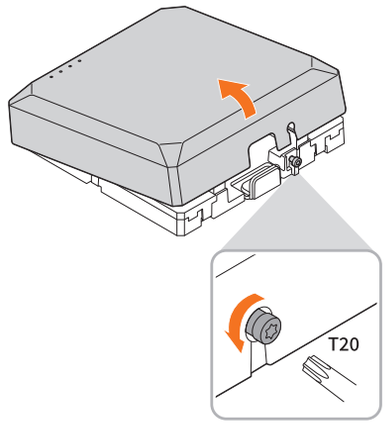
INSTALLATION AND CONNECTION

Check the following matters before installing the product.

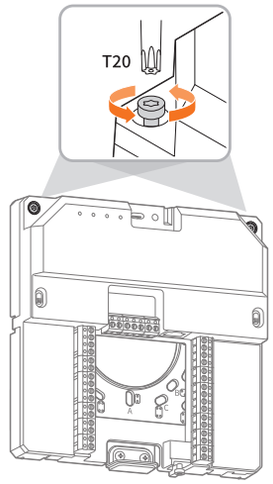
- Use this product in compliance with local laws and regulations.
- If you want to use the product outdoors or in an outdoor-like environment, contact the service center.
- Do not attempt to repair the product yourself; contact the service center first.
- Do not apply shock, strong pressure, vibration to the product.
- Do not install the product on a surface with vibration and unstability or walls.
- To prevent injury, this product must be securely attached to the Wall/ceiling in accordance with the installation instructions.

■ The following figures are based on Model NHP-P200.

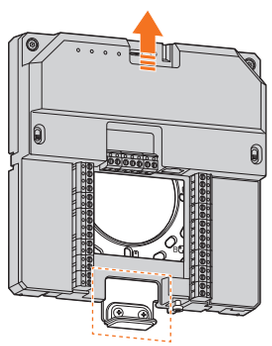
1 Disconnecting top case



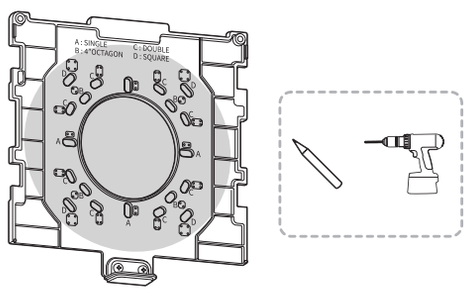
2 Disconnecting IP Controller and mount plate (1)



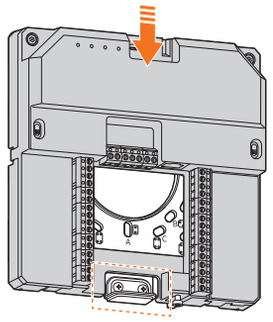
3 Disconnecting IP Controller and mount plate (2)



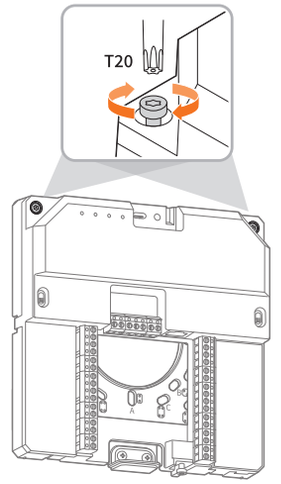
4 Fixing the mount plate onto the installation surface



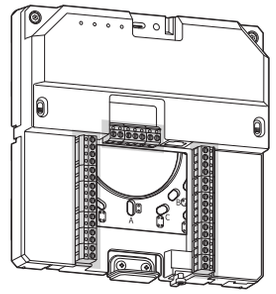
5 Fastening IP Controller and mount plate (1)



6 Fastening IP Controller and mount plate (2)

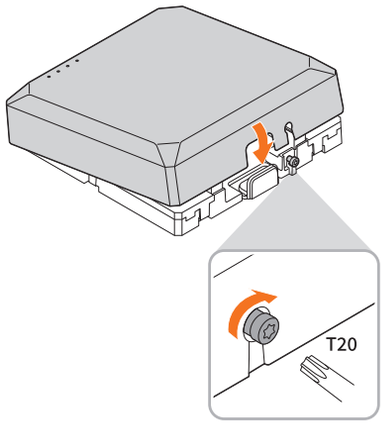


7 Connecting cable



■ For more information about connection, see the Wiring Guide.

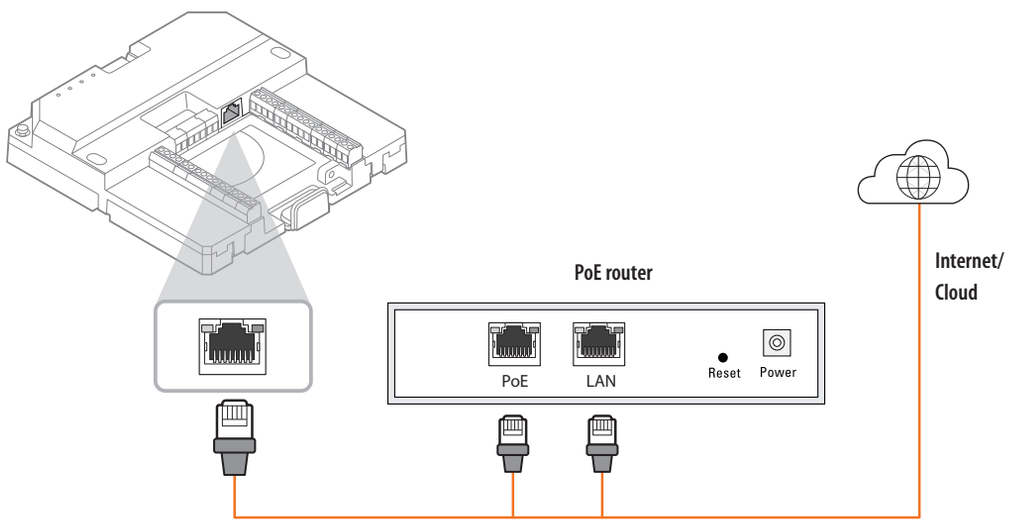
8 Fastening top case



Powering and Networking

Connect the PoE device to the PoE port on the IP Controller.

- The following figure is based on Model NHP-P200.



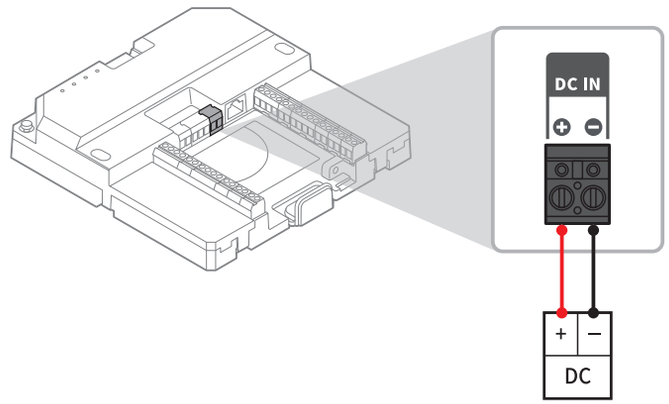
- Use a PoE enabled router.
- If a PoE enabled router is used, you don't need to connect a separate power source.

Network Cable Specifications

Item	Description	Remarks
Connector	RJ45(10/100/1000BASE-T)	
Ethernet	10/100/1000BASE-T	To operate it with 1000BASE-T, it is necessary to use a Category 6 or higher cable on the Giga hub.
Cable	Category 6	
Max distance	100 m	DC resistance ≤ 0.125 Ω/m
PoE support	IEEE 802.3at	

Connecting to Power

Connect the +/- wires on the power adapter to the power input terminals on the IP Controller using a screwdriver.



- Simultaneous input of PoE and DC (12V or 24V) power makes the IP Controller's power run both on PoE and DC power at the same time.
  - If a PoE enabled router is used, you don't need to connect a separate power source.
  - For PoE+, use a device that supports the IEEE 802.3at standard, and for PoE++, use a device that supports the IEEE 802.3bt standard.
- Connect DC power carefully because it has polarity.
- To connect an external device, be sure to power off the IP Controller before connecting it.
- Connect the IP Controller and adapter power cord first, then connect it to the 220V power source.
- Do not extend the power adapter output cable.
  If extended installation is needed, contact the service center.

Power Cord Specifications by Model

Model Name	Power	Wire gauge (AWG)	Wire length (Max.)
NHP-P200	DC 12V	#14	15 m
		#16	9 m
	DC 24V	#18	24 m
		#20	15 m
NHP-P100	DC 12V	#14	25 m
		#16	16 m
	DC 24V	#18	40 m
		#20	25 m

SPECIFICATIONS

	NHP-P100	NHP-P200
Hardware		
Readers	1 OSDP/Wiegand Reader Port (capable of supporting 2 OSDP Readers or 1 Wiegand Reader)	2 OSDP/Wiegand Reader Port (capable of supporting 4 OSDP Readers or 2 Wiegand Readers)
Reader Port Specs	OSDP Protocol (v2.2), Legacy Wiegand Support 1 Reader Power: 12VDC @ Max 500mA (per port)	OSDP Protocol (v2.2), Legacy Wiegand Support 2 Reader Power: 12VDC @ Max 500mA (per port)
General Purpose Inputs	5ea : 3 input (1ea Door Position, 1ea REX, 1ea Aux In) + 2 additional input (when OSDP is used) *3 supervised input port (Door Position Switch, REX, Aux In)	9ea : 5 input (2ea Door Position, 2ea REX, 1ea Aux In) + 4 additional input (when OSDP is used) *5 supervised input port (2 Door Position Switch, 2 REX, Aux In)
Door	1 (Door Output)	2 (Door Output)
Door Output Specs	Dry/12vDC/24vDC Field selectable power (per door) 30VDC @ Max 2A DRY, 12VDC @ Max 500mA WET, 24VDC @ Max 250mA WET	Dry/12vDC/24vDC Field selectable power (per door) 30VDC @ Max 2A DRY, 12VDC @ Max 500mA WET, 24VDC @ Max 250mA WET
Dedicated Inputs	Housing tamper (built-in; removal of housing cover, removal from wall) 1 FAI for Power Drop	
REX Power Output	1 port, 12VDC @ Max 100mA (per port)	2 port, 12VDC @ Max 100mA (per port)
Memory	1GB DDR4, 8GB eMMC	
Access		
Doors	1 Door	2 Door
Credentials	Server/Cloud Based : 50,000 EntryGuard : 400	
Cardholders	Server/Cloud Based : 50,000 EntryGuard : 200	
Event History	250,000 (offline cache event)	
Network		
Ethernet	RJ-45 (10/100BASE-T)	
Protocol	IPv4, IPv6, TCP/IP, UDP/IP, NTP, HTTP, HTTPS, SSL/TLS, SMTP, ICMP, IGMP, SNMP V3(MIB-2), ARP, DDNS, DNS, UPnP, Bonjour, LLDP	
Data Security	Secure Boot, Firmware verification, TPM with FIPS 140-3 Level 3	
System Integration		
Application Programming Interface	ONVIF Profile A/C, SUNAPI (HTTP API), Wisenet OpenPlatform	

	NHP-P100	NHP-P200
Environmental & Electrical		
Operating Temperature / Humidity	-20~+60°C / 20~85% RH (non-condensing)	
Storage Temperature / Humidity	-50~+60°C / Less than 95% RH	
Input Voltage	PoE+, 12VDC / 24VDC	PoE++, 12VDC / 24VDC
Power Consumption	PoE+ : 53V @ Max 0.48A, 12VDC @ Max 2.08A / 24VDC IN @ Max 1.04A	PoE++ : 55V @ Max 0.78A, 12VDC @ Max 3.5A / 24VDC IN @ Max 1.75A
Mechanical		
Color / Material	White / Aluminum	
Product Dimensions / Weight	184 x 184 x 43(mm), 1.1kg	184 x 184 x 43(mm), 1.3kg
General		
Webpage Language	IP Controller : English, French, Korean EntryGuard : English, Korean	
Included Accessories	Quick Guide, Wiring Guide	
Warranty	5 years	
Certifications	UL 294, UL 2043, UL 62368-1, FCC,CE,KC, UKCA, California Prop 65, SIA, IK10* * IK10: Excluding conduit cover	

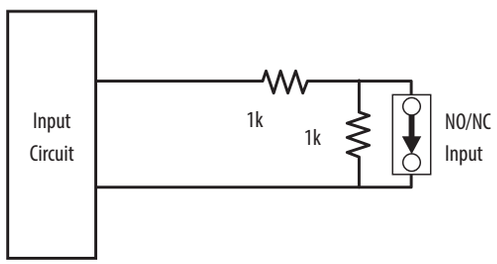
Supervised Inputs

REX, DPS, AUX input support a supervised input mode. If using supervised mode, EOL termination resistors will be required.

End-of-Line (EOL) Termination Resistors

Using two end-of-line (EOL) termination resistors, the supervised input can detect trouble conditions resulting from a short or open loop.

EOL termination resistor configuration



NO input
Normal = 2 kΩ
Active = 1 kΩ
Trouble = Short, Open

NC input
Normal = 1 kΩ
Active = 2 kΩ
Trouble = Short, Open

REQUIREMENT FOR UL294 COMPLIANCE

When installing and using the device, comply with UL standards. Please review the following information and guidelines to ensure compliance with UL standards.

Performance Levels for Access Control

Check the level information by required feature to ensure compliance with the UL294 standards.

Feature	Level
Destructive Attack	I
Line Security	I
Endurance	IV
Standby Power	I

Support Reader

Check the level information by required feature to ensure compliance with the UL294 standards.

Reader Maker	Model Name
Wavelynx	ET10-7WS/6WS/3WS/2WS ET20-7WS/6WS/3WS/2WS ET25-7WS/6WS/3WS/2WS
HID	SIgno 20/20K/40/40K

Safety Instructions

- Hanwha Vision products must be installed and serviced by a qualified professional.
- Hanwha Vision products must be installed within a protected area (secure zone).
- Hanwha Vision products must be installed indoors. UL approval for outdoor use has not been obtained.
- All interconnected devices must be registered to UL.
- When the Hanwha Vision product reaches the end of its service life, dispose of it in compliance with local laws and regulations.
- Use with UL294 Listed class2, power limited source.
- Remote Access function is not evaluated by UL.
- The installation should follow the requirements in National Electrical Code, ANSI/NFPA 70 Electrical.

Battery

The 3.0 V rechargeable lithium battery used in Hanwha Vision products is UL certified.

Item	Description
Type	Lithium Rechargeable Battery
Maker / Part number	Seiko Instruments Inc. / ML414H IV01E
Charging Voltage	From 2.7 V to 3.1 V
Nominal Capacity	1.0 mA (After charging)
Standard Discharge Current	0.005mA
Nominal Dimensions	Diameter 4.8 mm, Height 1.4 mm
Standard Mass	0.07 g (Without taps)

Operating Environment

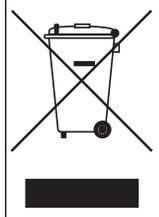
Normal operating conditions (Not evaluated by UL)	Temperature: -20°C – 60°C (-4°F – 140°F) Humidity: 20 – 85% RH (non-condensing)
UL294	Temperature: -20 °C ~ 60 °C (-4 °F ~ 140 °F) Humidity: 85% RH

Any changes or modifications in construction of this device which are not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.
This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Hanwha Vision cares for the environment at all product manufacturing stages, and is taking measures to provide customers with more environmentally friendly products.
The Eco mark represents Hanwha Vision's devotion to creating environmentally friendly products, and indicates that the product satisfies the EU RoHS Directive.



Correct Disposal of This Product (Waste Electrical & Electronic Equipment)

(Applicable in the European Union and other European countries with separate collection systems)

This marking on the product, accessories or literature indicates that the product and its electronic accessories (e.g. charger, headset, USB cable) should not be disposed of with other household waste at the end of their working life. To prevent possible harm to the environment or human health from uncontrolled waste disposal, please separate these items from other types of waste and recycle them responsibly to promote the sustainable reuse of material resources.

Household users should contact either the retailer where they purchased this product, or their local government office, for details of where and how they can take these items for environmentally safe recycling.

Business users should contact their supplier and check the terms and conditions of the purchase contract. This product and its electronic accessories should not be mixed with other commercial wastes for disposal.

Correct disposal of batteries in this product

(Applicable in the European Union and other European countries with separate battery return systems.)

This marking on the battery, manual or packaging indicates that the batteries in this product should not be disposed of with other household waste at the end of their working life. Where marked, the chemical symbols Hg, Cd or Pb indicate that the battery contains mercury, cadmium or lead above the reference levels in EC Directive 2006/66. If batteries are not properly disposed of, these substances can cause harm to human health or the environment.

To protect natural resources and to promote material reuse, please separate batteries from other types of waste and recycle them through your local, free battery return system.


Hanwha
Vision