NUCLIAS CONNECT HUB PLUS

DNH-200 User Manual

V 1.10

nuclias connect

Table of Contents

Introduction

The DNH-200 Nuclias Connect Hub Plus is a hardware controller with pre-loaded Nuclias Connect software. Nuclias Connect is D-Link’s centralized management solution for Small-to-Medium-Sized Business (SMB) networks. Managing a group of access points and network cameras is made easy and economical through Nuclias Connect. Nuclias Connect gives you the scalability and technical flexibility to expand from a small network to a larger one, while retaining a robust and future-proof management system. And with its intuitive Graphical User Interface (GUI) supporting 11 languages and compliant apps for mobile accessibility, Nuclias Connect minimizes the hassle of deployment, configuration, and administration tasks. The DNH-200 is a successor to the DNH-100 Nuclias Connect Hub, equipping with a hardware controller with pre-loaded Nuclias Connect software plus camera surveillance capability. In addition to the centralized management of wireless networks, the new camera surveillance facilitates surveillance applications with greater efficiency and manageability. Coupled with the Nuclias Protect app, the live feeds of the cameras can be accessed anytime, anywhere. It is designed to support on-premises security by providing useful surveillance functions such as video monitoring, recording and playback, and event notifications. The Nuclias Connect Hub Plus can currently manage up to 50 APs and 20 cameras of supported models per unit with the potential to extend to other Nuclias Connect products in future firmware updates.

Hardware Installation

Before configuring the DNH-200 for more advanced operation requirements, you need to install the device. Use the instructions in the following sections to guide you through the installation process and initial setup of the system for Ethernet or console communication. Make sure your DNH-200 package includes the following items:

- DNH-200 Nuclias Connect Hub Plus
- Power adapter
- Rack Mount Kit
- Ethernet cable
- Documentation

If any of the above items are damaged or missing, please contact your local D-Link reseller.

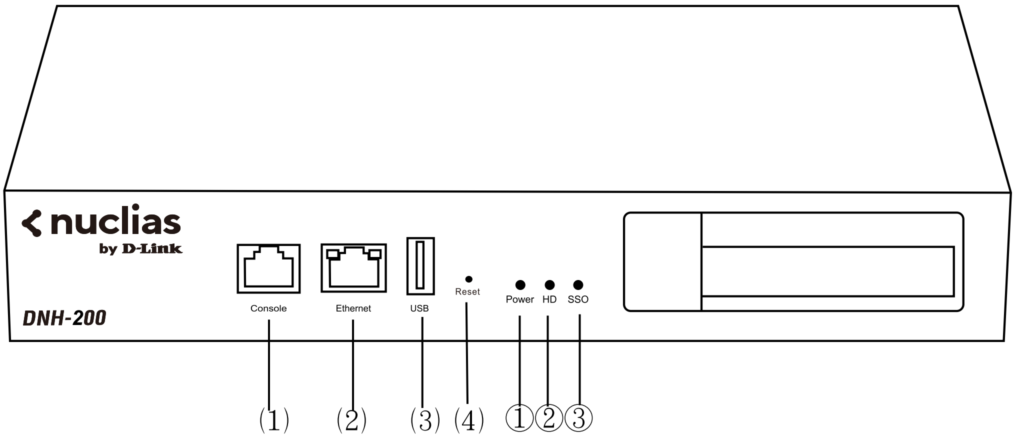
System Requirements

- Computers with Windows®, Macintosh®, or Linux-based operating systems
- Browser support for H.264 video stream: Microsoft® Edge, Google® Chrome, Mozilla® Firefox, Mac® Safari
- Browser support for H.265 video stream: Microsoft® Edge, Mac® Safari

Notes:

1. DNH-200 can manage IP cameras compatible with H.265 and H.264 but does not provide any coding or decoding services for video streaming, live view, or playback. Video coding and decoding need to be processed via the operating system or the web browser.
2. Browser compatibility requirements are subject to change. Before making any purchase, obtain the latest information from your D-link reseller or product website.
3. Google® Chrome and Mozilla® Firefox browsers don’t support High Efficiency Video Coding (HEVC) for H.265 decode. Microsoft® Edge requires the installation of HEVC video extensions to view H.265 videos (fees may apply).

Hardware Overview



LED Indicators

#	LED	Status	Color and Behavior
1	Power LED	Power On	Green: solid
		System Startup	Green: blinking while the system boots up (Normal Speed)*
		System Ready	Red: solid when the startup fails
		Firmware Update	Green: solid
		Recovery Mode	Red and Green: blinking alternately (Normal Speed)*
		Uplink and IP provision	Red: blinking (Normal Speed)*
		Power Off	Orange: blinking (Normal Speed)*
2	HD LED	HDD is Present	Green: solid
		HDD Read/Write	Green: blinking (Normal Speed)*
		HDD Power Off	Light off
		HDD Failure	Red: solid
3	SSO LED	Connect to Nuclias Server	1. Light Off: DNH-200 does not connect to the Nuclias server in the cloud with a Single Sign-on (SSO) account. 2. Blue: solid, DNH-200 connects to the Nuclias server in the cloud with a Single Sign-On

			(SSO) account.
* Normal speed = 1 second On, 1 second Off			

Interface Connectors

#	Connector	Description
1	Console Port	RJ-45 port to connect the RJ-45 connector of a serial-to-RJ-45 console cable for CLI management.
2	Ethernet Port	Gigabit RJ-45 port for LAN connection.
3	USB Port	USB 2.0 supports flash drive for video export and configuration backup.
4	Reset	Device Reboot Press the Reset button once to reboot the DNH-200. Reset to Factory Default Hold the Reset button for 5 seconds; all LEDs will turn on at the same time. After 1 second, all the LEDs will turn off and the DNH-200 will reboot and reset back to factory defaults. Recovery Press and hold the Reset button and then turn on the power. It will enter the Recovery Mode for the firmware recovery process.

Configuration

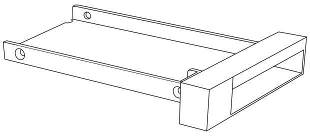
Note: D-Link recommends manual configuration of the DNH-200 before mounting it onto the rack. The management computer, DHCP server, and DNH-200 must be in the same network.

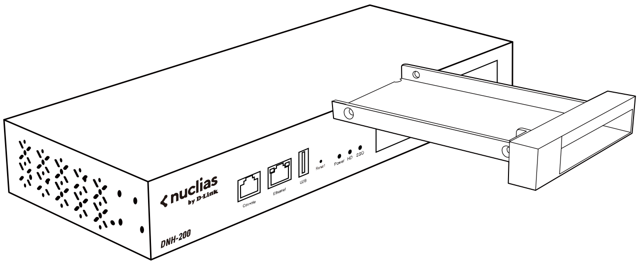
Ethernet Connection

You need the following equipment to access the web interface of the DNH-200:

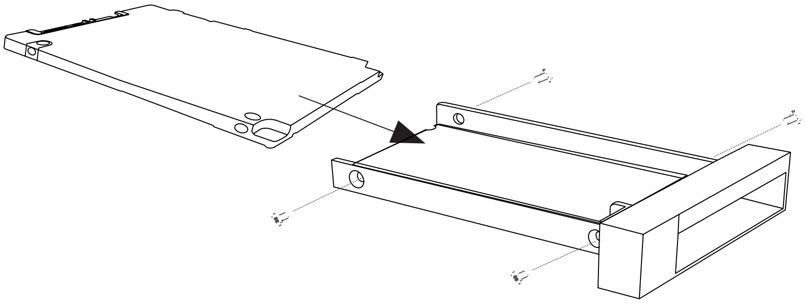
- A PC with a RJ-45 Ethernet connection
- An Ethernet cable
- A power adapter

1. Pull out the hard disk tray of the DNH-200 device.

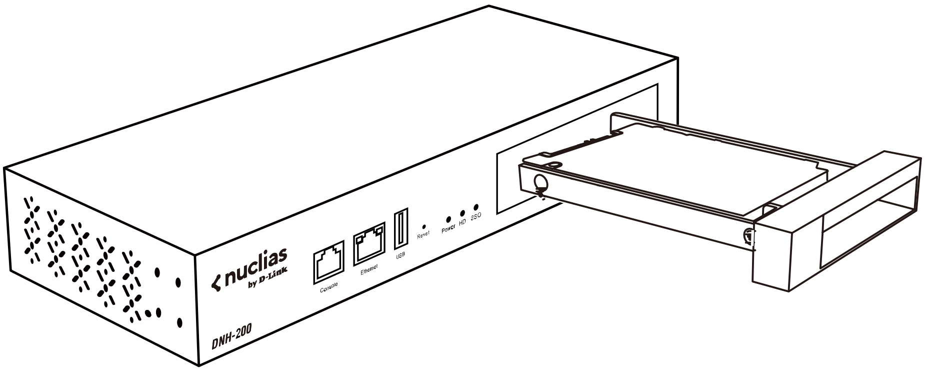




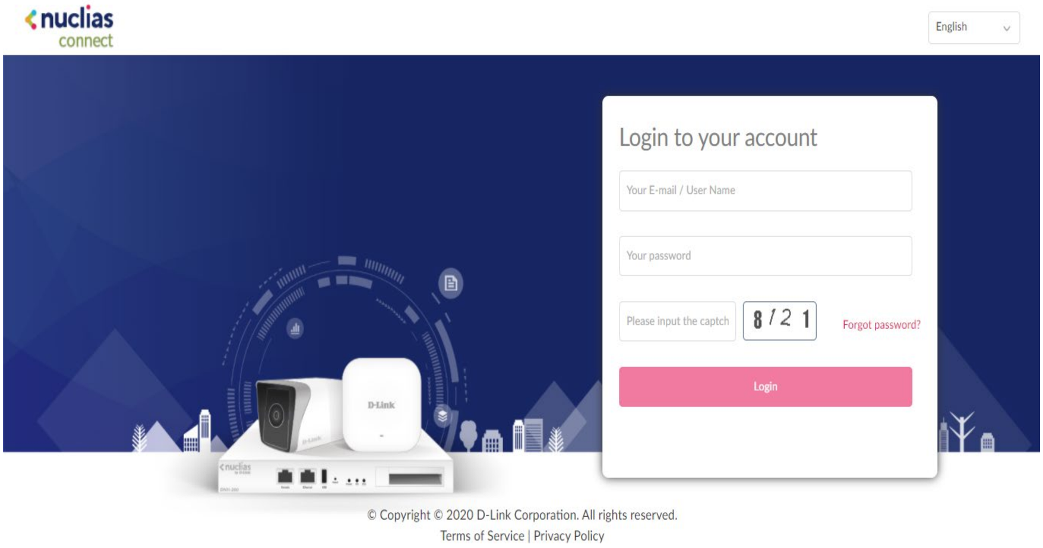
2. Insert a 2.5-inch hard disk into the tray and secure the HDD with the supplied screws.



3. Reinsert tray back into the device.



4. Connect the adapter to the power input on the DNH-200, then plug the adapter into a nearby power outlet.
5. Use an Ethernet cable to connect the DNH-200 with a switch or router that the management computer is connected to.
6. Configure the DNH-200 from a computer. Enter https://DNH-200-XXXX.local* in the address field of your browser (*where XXXX are the last four digits of your device's MAC address). You can find the MAC address printed on the label on the bottom of the DNH-200).
7. Log into the device's web interface. The default username is "*admin*" and password is "*admin*".



© Copyright © 2020 D-Link Corporation. All rights reserved.
Terms of Service | Privacy Policy

8. Configure the DNH-200 via its web interface after login.

Console Connection

Use a console cable to connect to the DNH-200’s console port. The console cable should be a RS-232 serial-to-RJ-45 cable designed to use with the device. A terminal emulation program is required for serial communication.

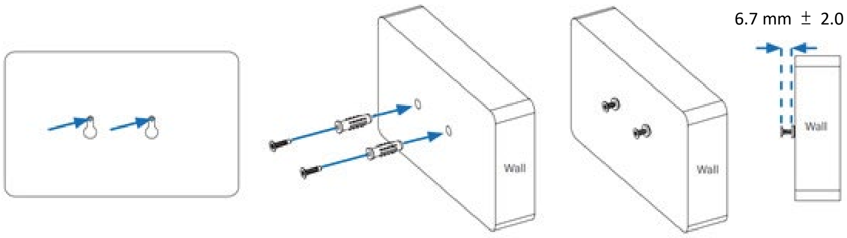
1. Connect the RS-232 interface to the serial port of the management PC.
2. Connect the RJ-45 interface to the console port of the device.
3. Open a terminal emulation program on the management PC and configure the properties for connection as follows:
   - The speed (baud): 115200 bps
   - The data bits: 8
   - The parity: None
   - The stop bits: 1
   - The flow control should be None.

Start the communication and the Limited Command Line Interface (CLI) should be available.

Installation

Mounting to a Solid Wall or Ceiling

The DNH-200 can be mounted on a solid wall or in an EIA standard 19-inch rack, which can be placed in a wiring closet with other equipment.
You can either hang the unit on the wall by using the wall mount keyholes on the rear of the unit or by using the supplied mounting bracket.



The following procedure explains how to use the keyholes.

1. Use the wall mount template to mark the screw positions on the wall.
2. Drill the 2 supplied wall anchors into the wall at the marked positions and screw the 2 supplied screws into them. Make sure they stand out ~6.7mm.
3. Hang the device on the wall by aligning the key holes with the mounted screws.

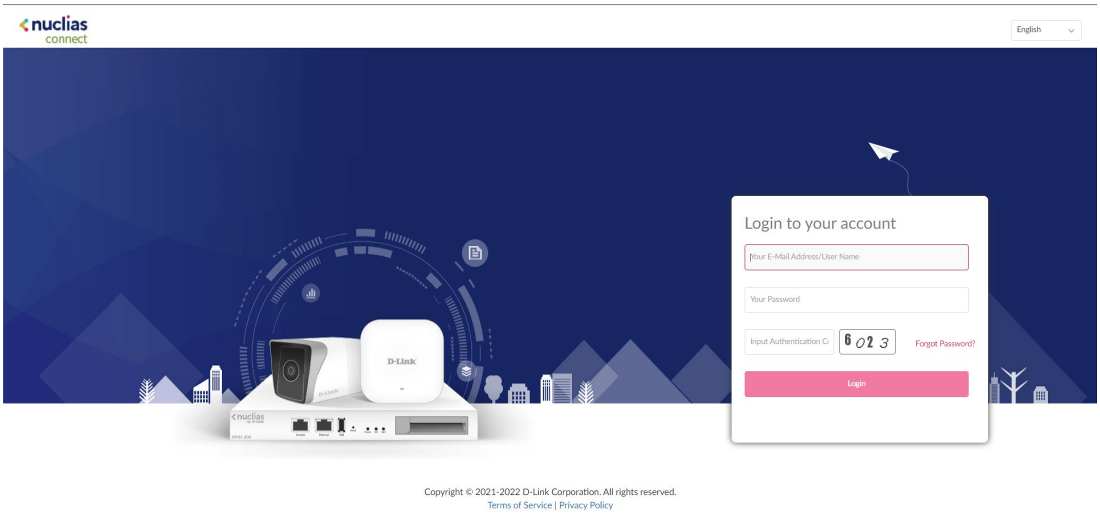
Basic Configuration

Launch Nuclias Connect

The DNH-200 comes preloaded with Nuclias Connect. Open a web browser from the management computer and enter the **IPaddress** or **Domain Name** of the DNH-200. The default domain name is https://DNH-200-XXXX.local. At the login page, enter *admin* for both username and password.
Enter the CAPTCHA code as shown on the screen, then click **Login** to proceed.

Notes:

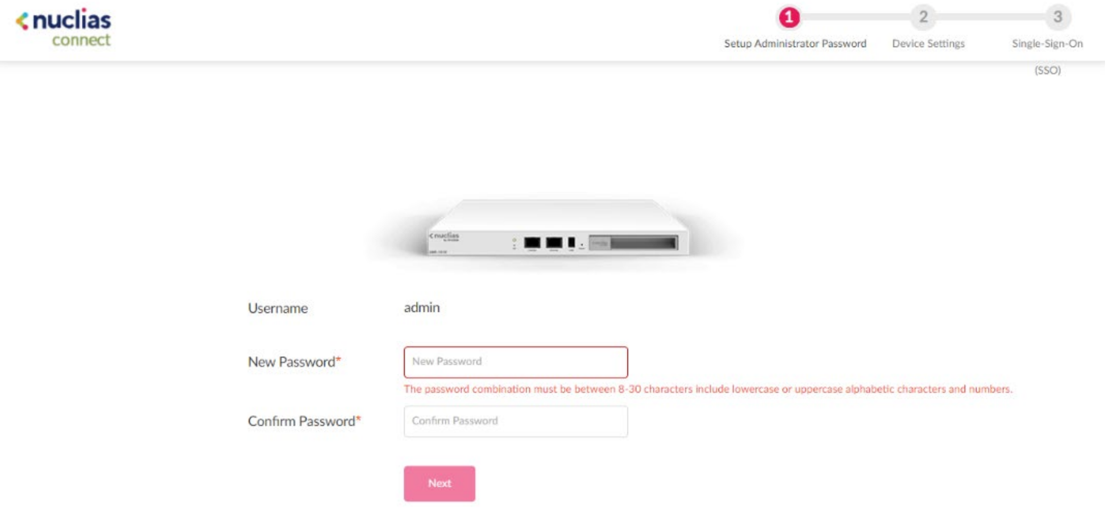
1. In the default domain name https://DNH-200-XXXX.local, XXXX is the last four digits of your DNH-200's MAC address. The MAC address and web management URL are printed on the label on the bottom of the DNH-200.
2. The IP address can be obtained from the client list of the uplink router connected to your DNH-200.
3. For initial configuration, the management computer and DNH-200 must be in the same subnet.


nuclias connect
English
Login to your account
Your E-Mail Address/User Name
Your Password
Input Authentication C
6023
Forgot Password?
Login
Copyright © 2021-2022 D-Link Corporation. All rights reserved.
Terms of Service | Privacy Policy

Notes:

- The **Forgot Password?** function provides an option to reset your password in the event that you’ve forgotten your current password. To use this function, the SMTP server and email address must be configured first. Refer to **System Settings > Mail Server Settings**.
- The Interface supports multilanguage options. By clicking the language menu, a different language can be selected.

After the web browser opens and connects successfully to the server, a change-password dialog appears. You are required to change your password. It must be 8-30 characters and contains both and uppercase and lowercase letters and numbers. Also avoid using common words or names.



Username admin

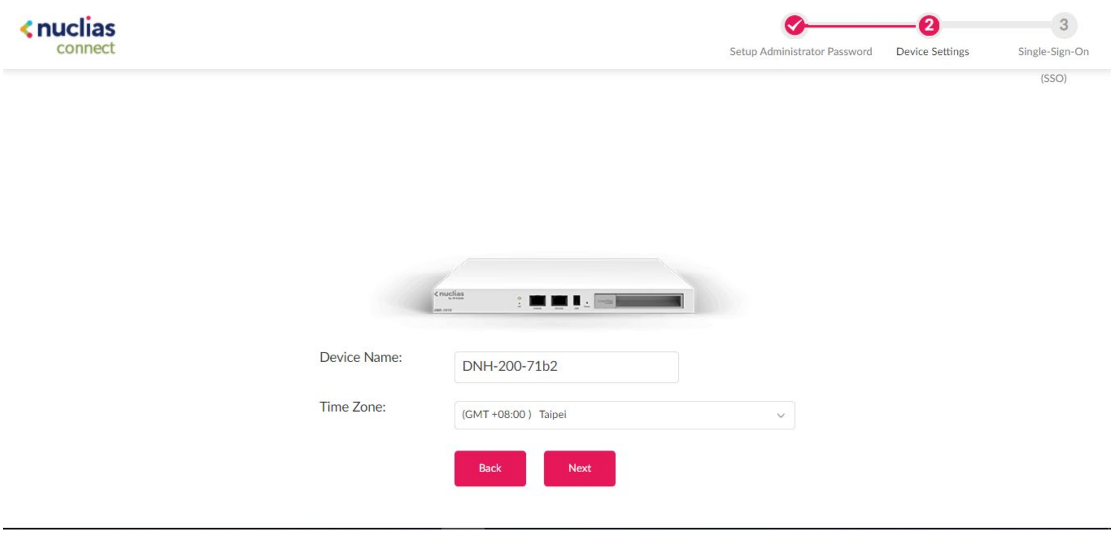
New Password* New Password

The password combination must be between 8-30 characters include lowercase or uppercase alphabetic characters and numbers.

Confirm Password* Confirm Password

In the **New Password** field enter a new password. Enter the same password in the **Confirm Password** field to verify the entry. Then click **Next** to proceed.

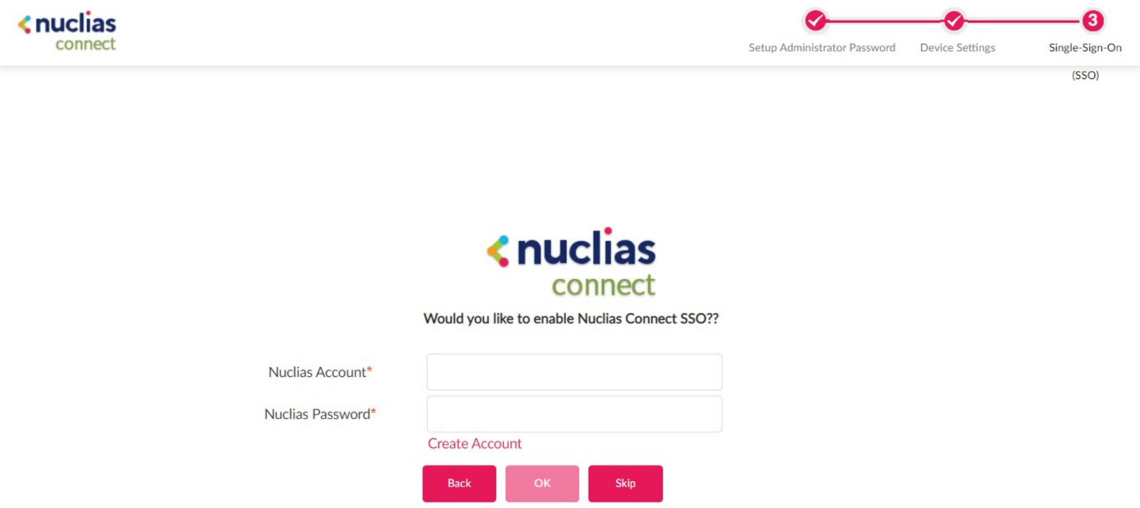
You can modify the device name with a more descriptive name for easy identification of the device. Also select the time zone for the device.



Device Name: DNH-200-71b2

Time Zone: (GMT +08:00) Taipei

If you have a Nuclias account for **Single Sign-On**, enter it now. If you do not already have a Nuclias account, you can click **Create Account** and a browser window will open to a link where you can create one. The Single Sign-On allows you to use a Nuclias account to access Nuclias Cloud and the Nuclias Connect portal.



Would you like to enable Nuclias Connect SSO??

Nuclias Account*

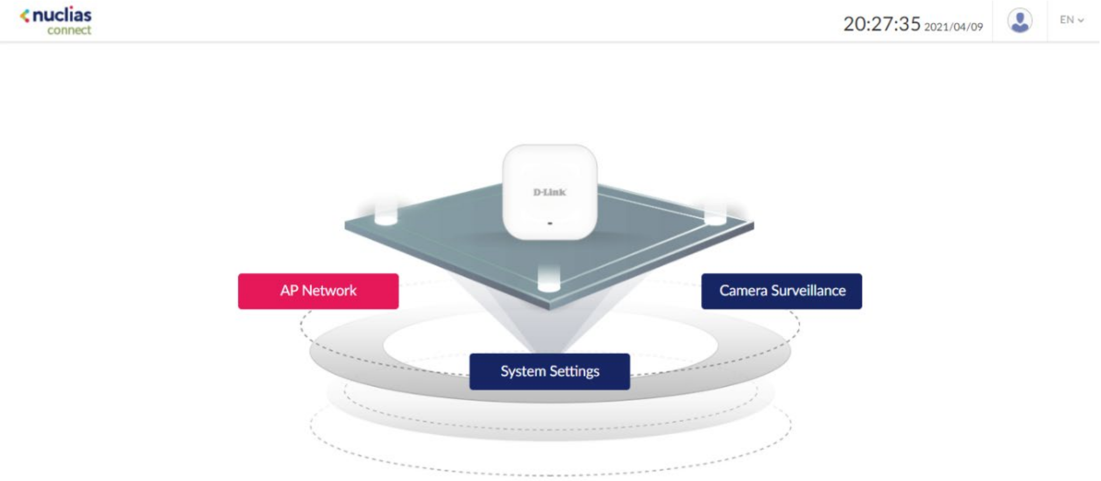
Nuclias Password*

After entering your Nuclias account information, click **OK** to confirm it.

Home

After successfully logging in to the server, the Home page displays the 3 modules of the Nuclias Connect Hub Plus (may be referred to as the Hub hereafter):

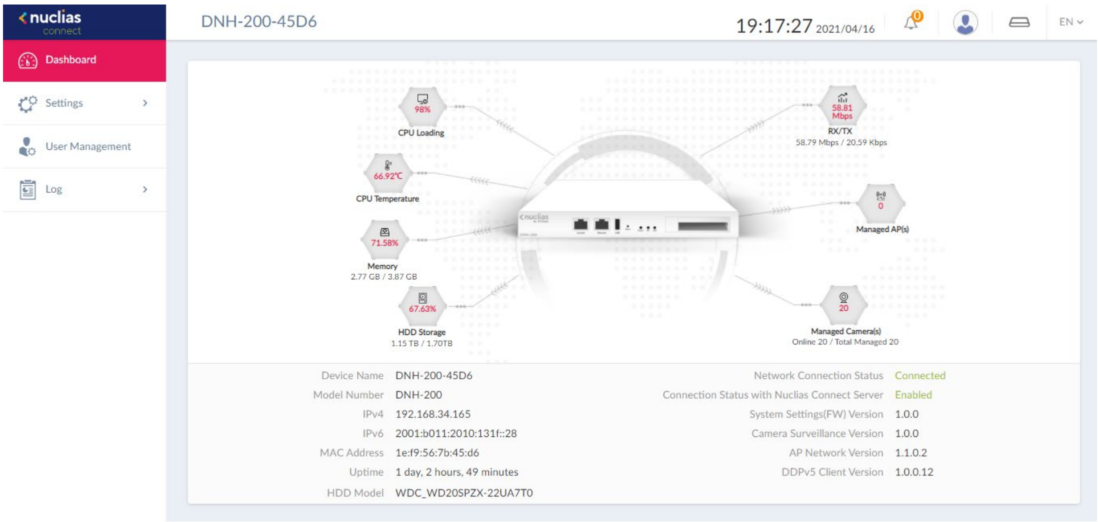
- **AP Network:** Manage your current sites and networks through Nuclias Connect.
- **System Settings:** Manage system-wide configurations and operations.
- **Camera Surveillance:** Monitor and manage network cameras centrally and maintain recordings on the Hub.



System Settings

Dashboard

The **Dashboard** page presents a summary of information about relevant system resource utilization.



Device Name DNH-200-45D6
Model Number DNH-200
IPv4 192.168.34.165
IPv6 2001:b011:2010:131f::28
MAC Address 1e:f9:56:7b:45:d6
Uptime 1 day, 2 hours, 49 minutes
HDD Model WDC_WD20SPZX-22UA7T0

Network Connection Status Connected
Connection Status with Nuclias Connect Server Enabled
System Settings(FW) Version 1.0.0
Camera Surveillance Version 1.0.0
AP Network Version 1.1.0.2
DDPv5 Client Version 1.0.0.12

CPU Loading	The CPU’s workload in percentage.
CPU Temperature	The current CPU temperature under load.
Memory	The RAM usage: used/total.
HDD Storage	The HDD storage usage: used/total.
RX/TX	The data transmission statistics of the Ethernet port.
Managed AP(s)	The number of managed APs through the AP Network module of the Hub: Online/Total Managed.
Managed Camera(s)	The number of managed network camera(s) through the Camera Surveillance module of the Hub: Online/Total Managed.

You can also obtain basic device information of the Hub.

Device Name	The descriptive name of the Hub.
Model Number	The model number of the Hub.
IPv4	The IP address of the Hub in IPv4 addressing scheme.
IPv6	The IP address of the Hub in IPv6 addressing scheme.
MAC Address	The MAC address of the Hub.
Uptime	Total number of hours and minutes that the device has been

	running.
HDD Model	The model name of the hard disk installed in the Hub.
Network Connection Status	Shows whether the Hub is connected to or disconnected from the network.
Connection Status with Nuclias Connect Server	Shows whether the Hub is connected to the Nuclias server in the cloud.
System Settings (FW) Version	The firmware version of the System Settings module.
Camera Surveillance Version	The firmware version of the Camera Surveillance module.
AP Network Version	The firmware version of the AP Network module.
DDPv5 Client Version	The DDPv5 (D-Link Discovery Protocol) client version.

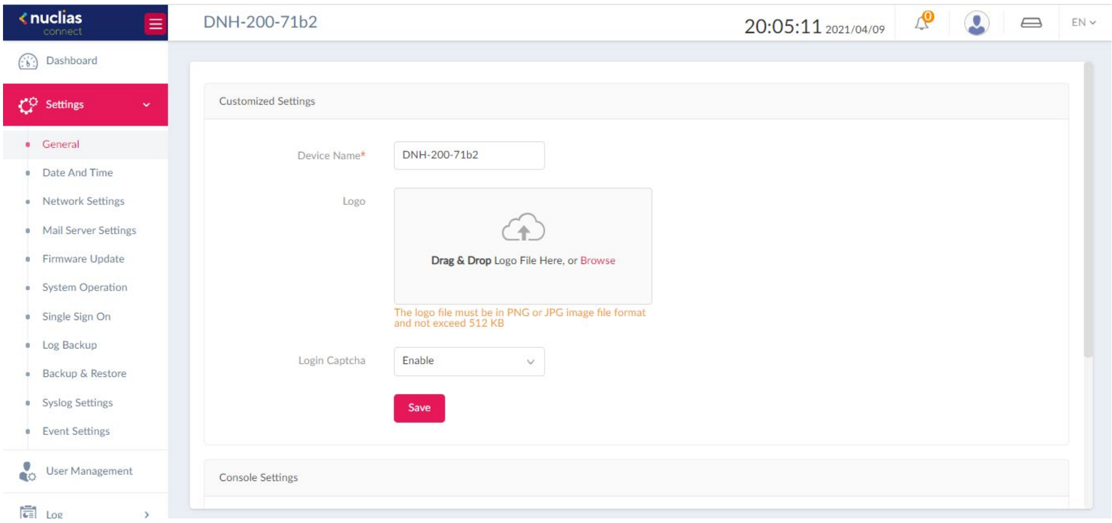
Settings

The **Settings** page provides configurable settings of the system. It contains these menus: **General, Date and Time, Network Settings, Mail Server Settings, Firmware Update, System Operation, Single Sign On, Log Backup, Backup & Restore, Syslog Settings,** and **Event Settings.**

Note: Only the **System Admin** has the editing privilege in **Settings**.

General

The General page allows you to add the logo of the DNH-200 and configure the connection settings for serial communication. Navigate to **Settings > General** to configure settings for these functions.



Customized Settings

Device Name* DNH-200-71b2

Logo

Drag & Drop Logo File Here, or Browse

The logo file must be in PNG or JPG image file format and not exceed 512 KB

Login Captcha Enable

Save

Console Settings

In the Customized Settings, configure the device name and logo:

Device Name	Click the text field to modify the name of the Hub.
Logo	Drag and Drop Logo File in the box or browse to locate the logo file. Note that the logo file must be within 512 KB in size and in PNG or JPG image format. The logo will be displayed on the top left-hand side next to the device name.
Display Authentication Code	Enable or disable the display of authentication code

	(the CAPTCHA code) in the login screen.

Click **Save** to save the values and update the screen.

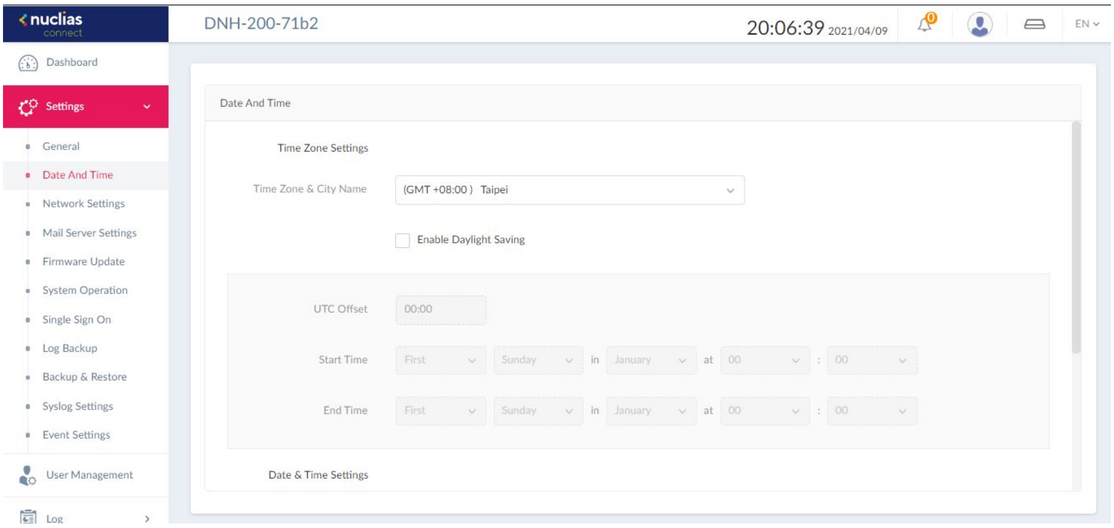
In the **Console Settings** section, parameters for data communication through the console port of the DNH-200 can be configured:

Console	Check to enable management through the console port.
Console Protocol	Choose whether to use Telnet or SSH as the terminal emulator.
Timeout	Click the drop-down menu to select timeout in minutes: 5 minutes or Never.

Click **Save** to save the values and update the screen.

Date and Time

Setting the time is essential for proper maintenance and troubleshooting of a network device by checking system logs and alerts. Navigate to **Settings** > **Date and Time** to configure these settings.



Date And Time

Time Zone Settings

Time Zone & City Name: (GMT +08:00) Taipei

□ Enable Daylight Saving

UTC Offset: 00:00

Start Time: First Sunday in January at 00 : 00

End Time: First Sunday in January at 00 : 00

Date & Time Settings

You can configure the time zone, adjust for daylight saving time, and configure the Network Time Protocol (NTP) server to synchronize the date and time with a time server.
Configure the date and time and NTP server settings with the following parameters:

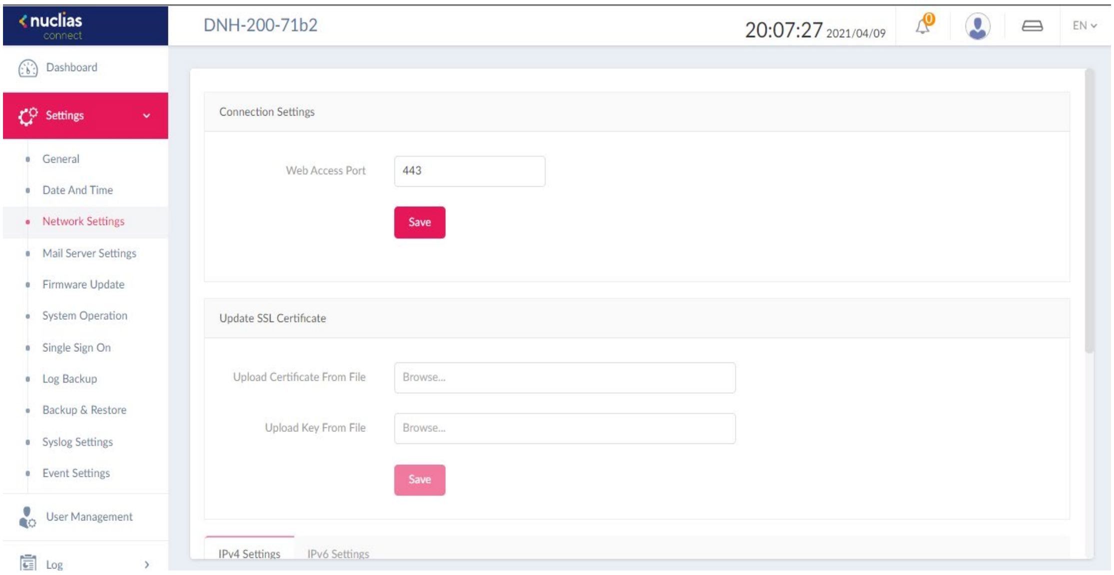
Time Zone & City Name	Select the time zone.
Enable Daylight Saving	Enable the daylight saving function.
DST Offset	Select Daylight Saving Time (DST) Offset time.
DST Start (24HR)	Designate the start date and time for DST.

DST End (24HR)	Designate the end date and time for DST.
Date & Time Settings	Enter the date and time manually or choose **Copy Your Computer's Time** to import the date and time from your computer's time settings.
Enable NTP	Enable or disable NTP.
NTP Server 1*	Enter a qualified NTP server name.
NTP Server 2*	Enter a qualified NTP server name as a backup.

Click **Save** to save the values and update the screen.

Network Settings

The **Network Settings** page displays device connection parameters and enables you to configure or modify network related parameters. These parameters are essential for the management computer to connect to the Hub. Navigate to **Settings > Network Settings**.



Connection Settings

Web Access Port: 443

Update SSL Certificate

Upload Certificate From File: Browse...

Upload Key From File: Browse...

In the **Connection Settings** section, the following parameters can be configured:

Web Access Port	Enter the port number for communicating with the Hub's web interface. The default is 443 for secure HTTP.

In the **Update SSL Certificate** section, the following can be configured:

Upload Certificate From File	An SSL certificate ensures security in data communication. Browse to upload and import the certificate from your computer.
Upload Key From File	Upload the key used with the certificate.

IPv4 Settings

Provision	Select either **Dynamic IP (DHCP)** or **Static IP Address**: DHCP automates the assignment of IP addresses, subnet masks, default gateways and other settings. On the other hand, Static IP addressing scheme requires you to enter IP addresses, subnet masks, default gateways and other settings manually.
Obtain DNS Servers Automatically or Configure DNS Servers Manually	If DHCP is selected, choose to either obtain DNS server settings automatically or enter them manually.
IPv4/Subnet Mask	If Static IP Address is selected, assign an IPv4 address and the subnet mask, which are used for networked devices to communicate and determine the subnet of the IP address respectively.
Gateway	If Static IP Address is selected, enter the gateway IP address. This is the address of a router interface connected to the Hub that forwards packets out to another subnet or network.
Primary DNS	Enter the IP address of a DNS server.
Secondary DNS	Enter the IP address of a DNS server as a backup if the primary DNS server fails.

IPv6 Settings

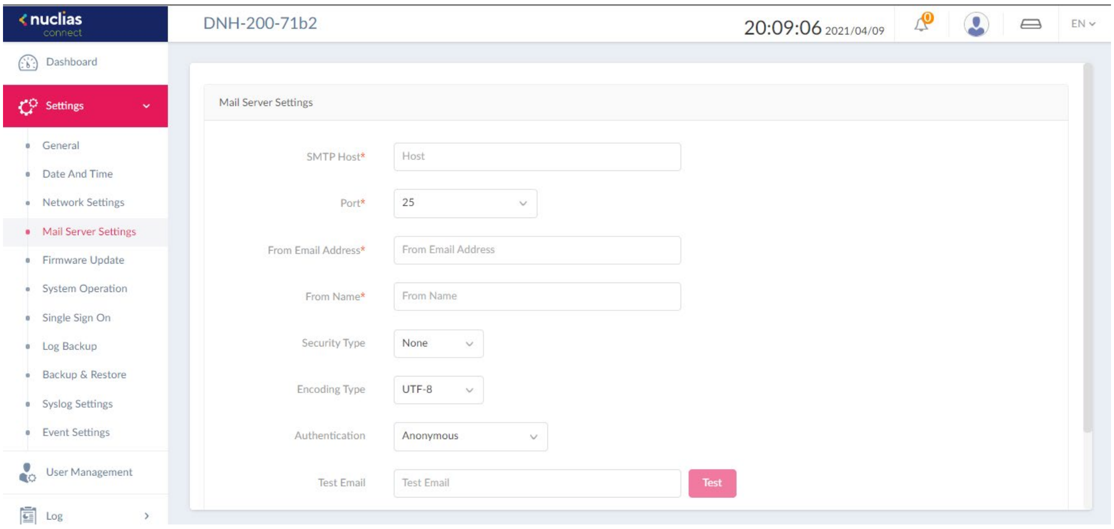
Provision	Select **Static IPv6 Address**, **IPv6 Auto Configuration** or **Local Connectivity Only**. DHCP automates the assignment of IP addresses, subnet masks, default gateways, and other settings. On the other hand, Static IP address scheme requires you to enter IP addresses, subnet masks, default gateways and other settings manually. Select **Local Connectivity Only** to use the link-local address of the device for the local network.
Obtain DNS Servers Automatically or Configure DNS Servers Manually	If Auto Configuration is selected, choose to either obtain DNS server settings automatically or enter them manually.
IPv6 Address/Prefix Length	Enter the IPv6 address and prefix length. The prefix is used to identify the IPv6 network. The valid range is 1-128.

Gateway	If Static IP Address is selected, enter the gateway IP address. This is the address of a router interface connected to the Hub that forwards packets out to another subnet or network.
Primary DNS	Enter the IP address of a DNS server.
Secondary DNS	Enter the IP address of a DNS server as a backup if the primary DNS server fails.

Click **Save** to save the values and update the screen.

Mail Server Settings

The **Mail Server** Settings page lets you configure outgoing email service using the simple mail transfer protocol (SMTP). It is a standard for sending emails on behalf of the system such as validation emails for password reset. Setting an SMTP server is also necessary for email notification of events to work. Navigate to **Settings > Mail Server Settings**.



Mail Server Settings

SMTP Host* Host

Port* 25

From Email Address* From Email Address

From Name* From Name

Security Type None

Encoding Type UTF-8

Authentication Anonymous

Test Email Test Email

Set an SMTP server and a sender's email account for password reset:

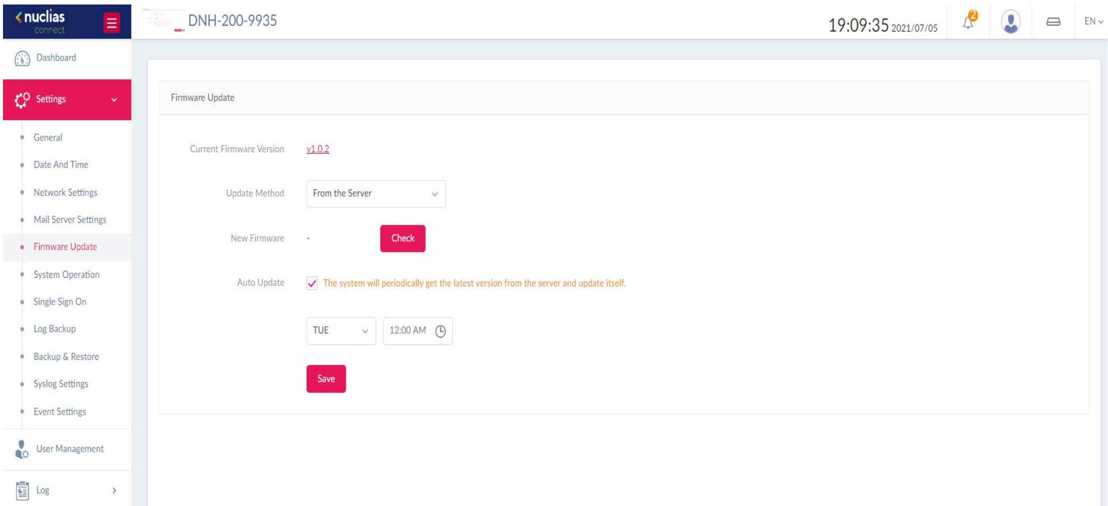
SMTP Host	Enter the SMTP server's IP address or domain name.
Port	Enter the SMTP server's port number. Default port is 25 for unencrypted connections. Encrypted connections commonly use port 465 or 587.
From Email Address	Enter the email address that you want to appear as the sender of an email.

From Name	Enter the sender's name of an email.
Security Type	Select the security type to be used in the email system. The options include None or SSL.
Encoding Type	Select character encoding type to match that of the supported e-mail client. The options include UTF-8 or ASC-II.
Authentication	Select the authentication mechanism for logging supported by the email server. The options include Anonymous or SMTP Authentication.
Username/Password	If authentication is enabled, you must specify a username and password for the users to log in to the mail server.
Test Email	Enter the recipient's email address to initiate a test email through the SMTP configuration. Click **Test** to send a test mail to the specified account. Please check your inbox to verify if the test mail has been sent successfully.

Once the outgoing email has been configured properly, email messages can then be distributed to pre-configured recipients on a per-alert basis using **Event Notification**. Refer to **Settings > Event Settings** in **System Settings** and **System > Event Settings** in **Camera Surveillance** for more information.

Firmware Update

The **Firmware Update** page allows you to perform firmware upgrade.
Keeping your firmware up-to-date protects your system from future bugs and allows for new features to be added to your device. You have the options of automatic or manual update.
Navigate to **Settings** > **Firmware Update**.



Firmware Update

Current Firmware Version v1.0.2

Update Method: From the Server

New Firmware -

Auto Update ☑ The system will periodically get the latest version from the server and update itself.

TUE 12:00 AM

Choose **From the Server** as the **Update Method** and configure the following:

Current Firmware Version	Displays the current firmware version
New Firmware	Click **Check** to verify if the current firmware is up to date.
Auto Update	**The system will periodically get the latest version from the server and update itself.** If this option is enabled, choose the desired days of a week and the time for firmware updates.

Click **Save** to save the values and update the screen.

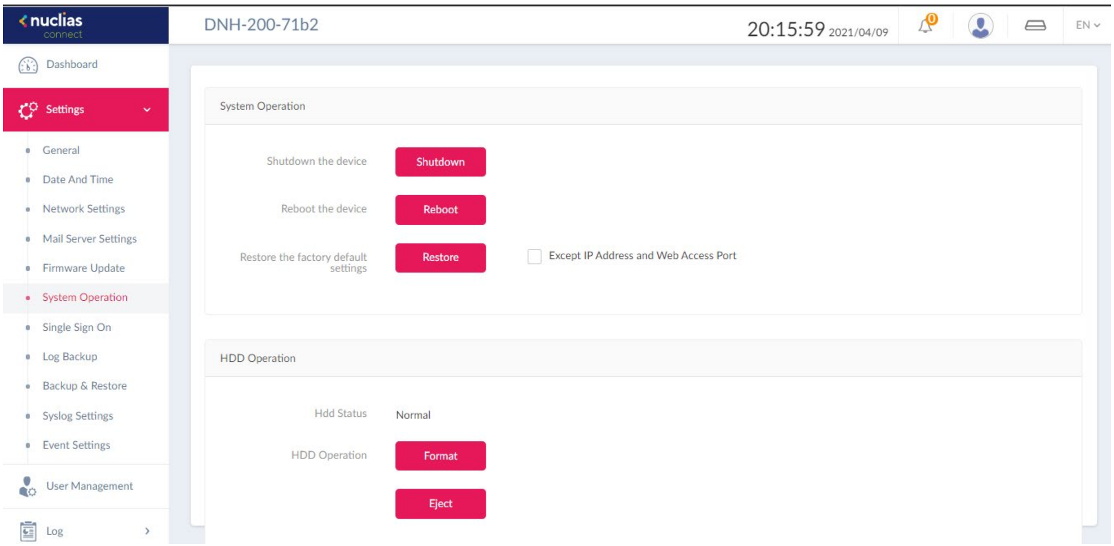
Or choose **From a Local storage** and perform the manual update:

Firmware File	Click **Browse….** to locate the firmware file. The firmware is a bin file type.
Update	Click this button to start the update process immediately.

Note: The firmware update will update the firmware for all 3 modules of the Hub. During a firmware update, do not power off or reset the device or interrupt the process in any way, until the operation is complete. Interrupting the update process may corrupt the Hub and require further RMA services.

System Operation

The **System Operation** page provides you with maintenance functions such as reboot, restore to factory defaults, and hard disk formatting.



Hdd Status: Normal

The system operation functions are explained below:

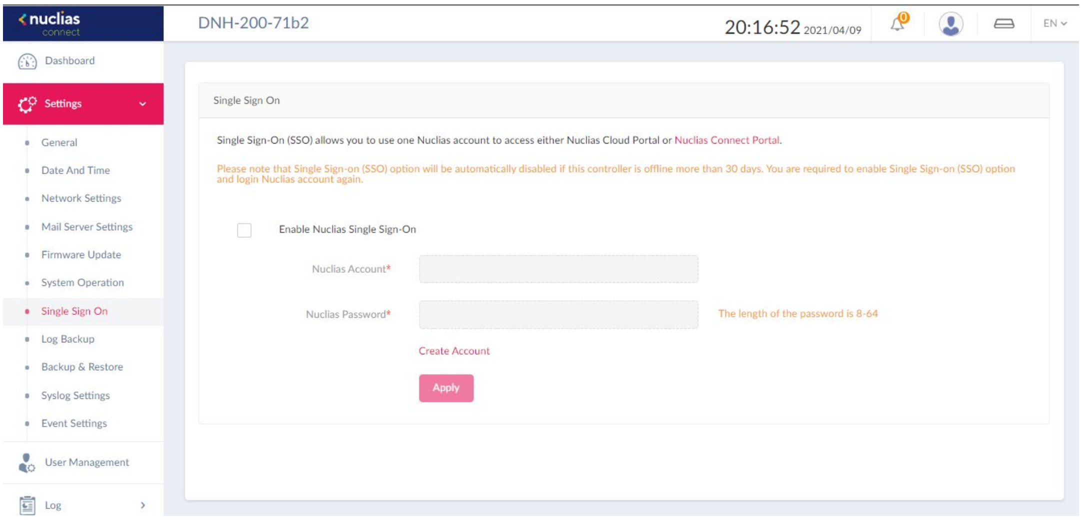
Shutdown the Device	Click this button to shut down the Hub.
Reboot the Device	Click this button to restart the Hub.
Restore the Factory Default Settings	Click this button to restore the Hub to factory default settings.
Except IP Address and Web Access Port	If this option is checked, then the Hub' IP address and the port number for accessing web interface will be preserved after factory reset.

In the **HDD Operation** section, the following can be performed:

HDD Status	Indicates HDD operation status such as normal or Empty.
Format	Please format the HDD to ext3 filesystem to be recognized by the system. Please be aware that you will lose all information on the HDD once you proceed with the operation.
Unmount/Mount	Before physically removing the HDD from the slot to replace it, unmount it first from the filesystem. Click **Mount** to let the system recognize the HDD as a storage device after installing it in the device.

Single Sign-On

The Single Sign-On page allows you to use one Nuclias account to access Nuclias Cloud and Nuclias Connect portal. If you do not already have a Nuclias account, you can click **Create Account** where a browser window will open to a link where you can create one.



Single Sign On

Single Sign-On (SSO) allows you to use one Nuclias account to access either Nuclias Cloud Portal or Nuclias Connect Portal.

Please note that Single Sign-on (SSO) option will be automatically disabled if this controller is offline more than 30 days. You are required to enable Single Sign-on (SSO) option and login Nuclias account again.

□ Enable Nuclias Single Sign-On

Nuclias Account*

Nuclias Password* The length of the password is 8-64

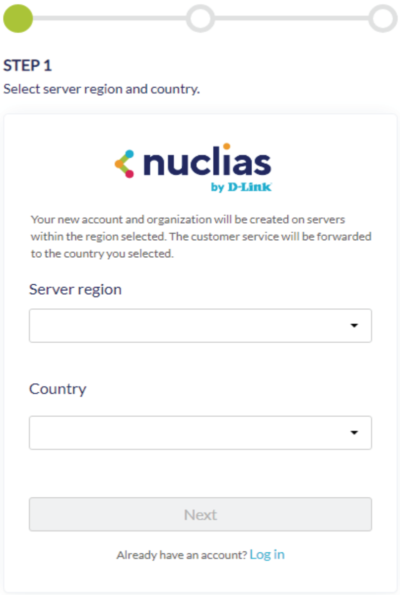
Create Account

Apply

To register a Nuclias account, follow these steps:

1. Selecting server region and country.

The account is created on the servers within the selected region and the selected country. Your account data will be stored in the regional server based on your selected region and country.


STEP 1

Select server region and country.

Your new account and organization will be created on servers within the region selected. The customer service will be forwarded to the country you selected.

Server region

Country

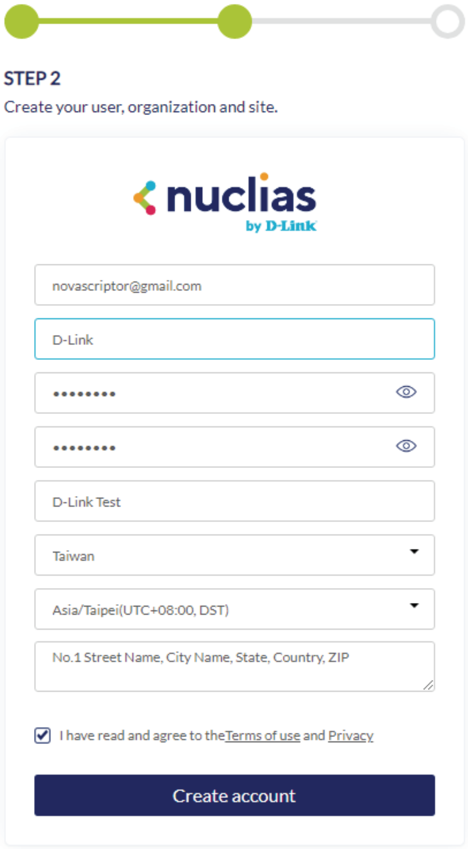
Next

Already have an account? Log in

2. Create organization and site.

Once the region and country have been entered, you will see the user, organization, and site page. Enter the required information and agree to the **Terms of Use and Privacy** agreement.

Click **Create account** to continue.



STEP 2

Create your user, organization and site.

novascriptor@gmail.com

D-Link

••••••••

••••••••

D-Link Test

Taiwan

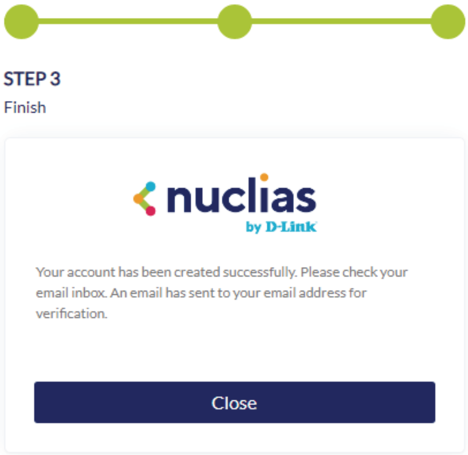
Asia/Taipei(UTC+08:00, DST)

No.1 Street Name, City Name, State, Country, ZIP

☑ I have read and agree to the Terms of use and Privacy

3. Finish the registration.

Click **Close** to complete the process. The registered account is now available for use. The verification information will be delivered to the registered email of the account.



STEP 3

Finish

Your account has been created successfully. Please check your email inbox. An email has sent to your email address for verification.

Your Nuclias account must be validated before use. You will receive an email from verify@nuclias.com with a verification link included. Please click the verification link to activate your Nuclias account.

Once finished, specify the following parameters on the **Single Sign-On** page, then click **Login**.

Enable Nuclias Single Sign-on	Check to enable Single Sign-On (SSO).
Nuclias Account	Enter your Nuclias account username.
Nuclias Password	Enter your Nuclias account password.

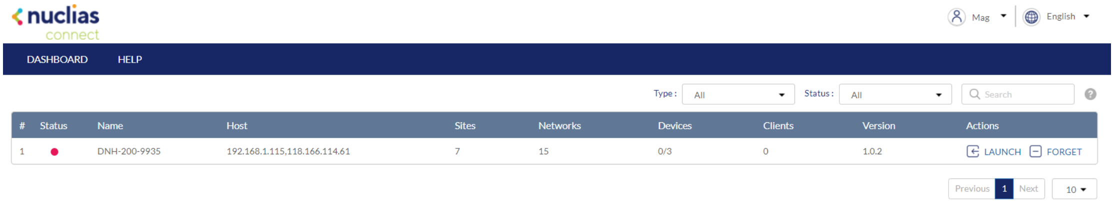
Note: The Single Sign-on (SSO) will be automatically disabled if the Hub is offline for more than 30 days. You will need to enable Single Sign-on (SSO) again and log in with your Nuclias account.

The Nuclias Connect portal provides you with an easy way to access and check the status of all your Hub(s).

Requirements for use include:

- A Nuclias account
- DNH-200 device(s) with Single Sign-On enabled

The portal can be found at: https://connect.nuclias.com/



#	Status	Name	Host	Sites	Networks	Devices	Clients	Version	Actions
1	●	DNH-200-9935	192.168.1.115,118.166.114.61	7	15	0/3	0	1.0.2	LAUNCH FORGET

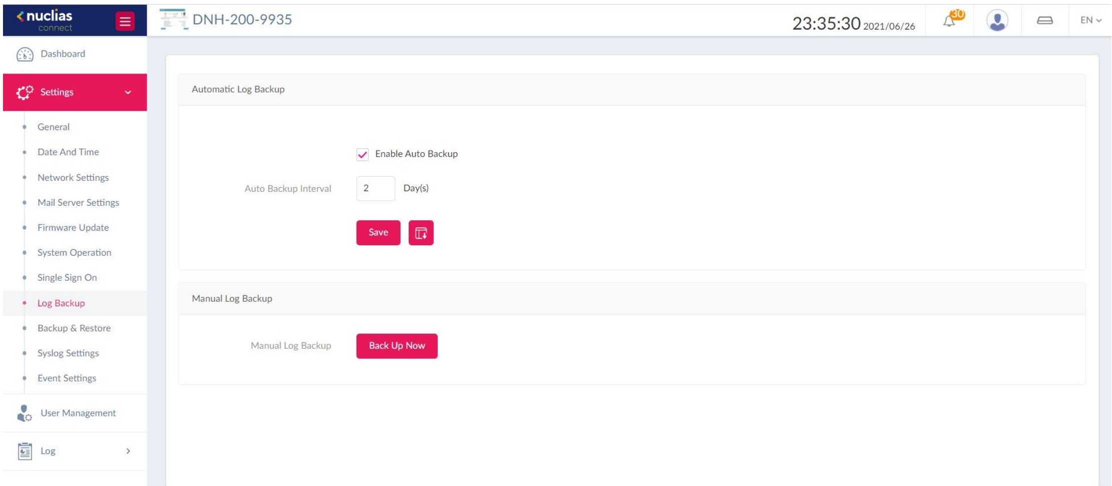
After logging in to the portal, you can view the following information:

Number	Order on the list.
Status	Displays whether the Nuclias Connect portal can link to the Hub.
Name	Name of the Hub.
Host	Displays both the Hub's LAN IP address and public IP address.
Sites	Number of sites managed by the Hub.
Networks	Number of networks managed by the Hub.
Devices	Number of devices (including both AP and camera devices) managed by the Hub: Online / Total.
Clients	Number of clients connected to AP devices managed by the Hub.
Version	Firmware version of the Hub.
Actions	Click **Launch** to open the Hub's web interface. Please note that IP address mapping between WAN and LAN is required for instances behind a firewall or router. Click **Forget** to disconnect

	the Hub from the Nuclias Connect portal. (**Forget** is only available when that device is offline.)

Log Backup

The **Log Backup** page allows you to back up logs generated from the system automatically or manually.



Automatic Log Backup

☑ Enable Auto Backup

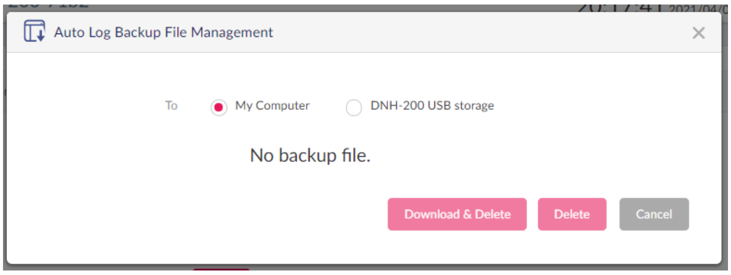
Auto Backup Interval 2 Day(s)

Manual Log Backup

Manual Log Backup

For **Automatic Log Backup**, configure the following:

Enable Auto Backup	Check this option to enable automatic backup.
Auto Backup Interval	Specify the frequency of automatic backup. The valid range is 1 to 365 days.
Auto Log Backup File Management	Select the directory to store backup files: **My Computer** or **DNH-200 USB storage**. Please ensure that a USB disk is installed on the device. You can also specify to **Download & Delete**, **Delete**, or **Cancel** for log files on the system after the automatic backup.



Auto Log Backup File Management

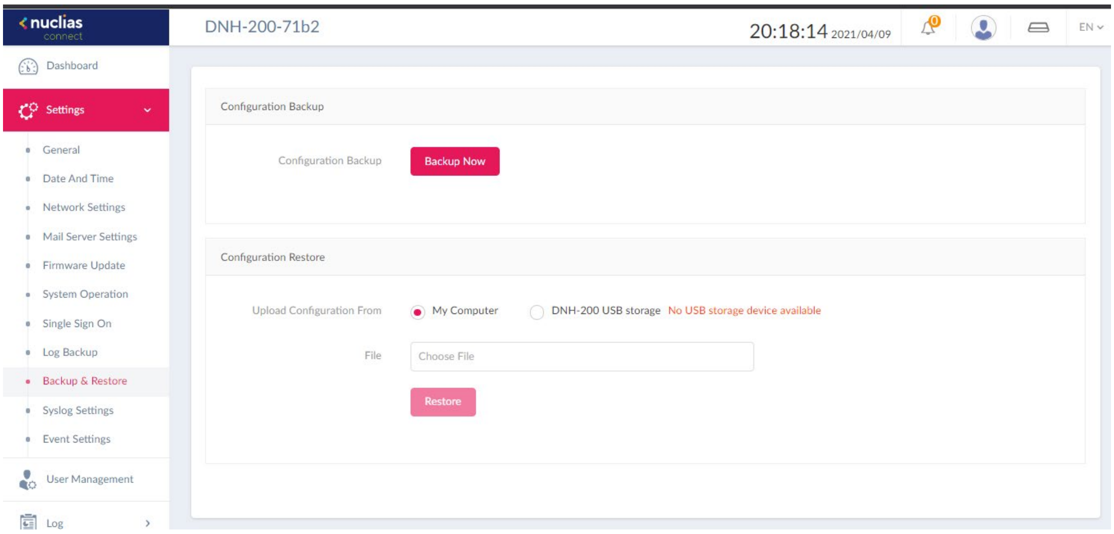
To ● My Computer ○ DNH-200 USB storage

No backup file.

For **Manual Log Backup**, click **Back Up Now**. The log files will be compressed as a single tar file and will be saved in your browser’s download directory. The tar file contains 3 log files from the 3 modules of the DNH-200, i.e., **AP Network, Camera Surveillance**, and **System Settings**. These files will be named as follows: Function_date_log.xlsx.

Backup & Restore

The **Backup & Restore** page allows you to back up system settings and restore the system to an earlier state with previously stored configuration.



Configuration Backup

Configuration Backup: Backup Now

Configuration Restore

Upload Configuration From: ● My Computer ○ DNH-200 USB storage No USB storage device available

File: Choose File

In the **Configuration Backup** section, click **Back Up Now** to back up the current system configuration. The file will be saved in your browser’s download directory and named as *date_configuration*.tar.

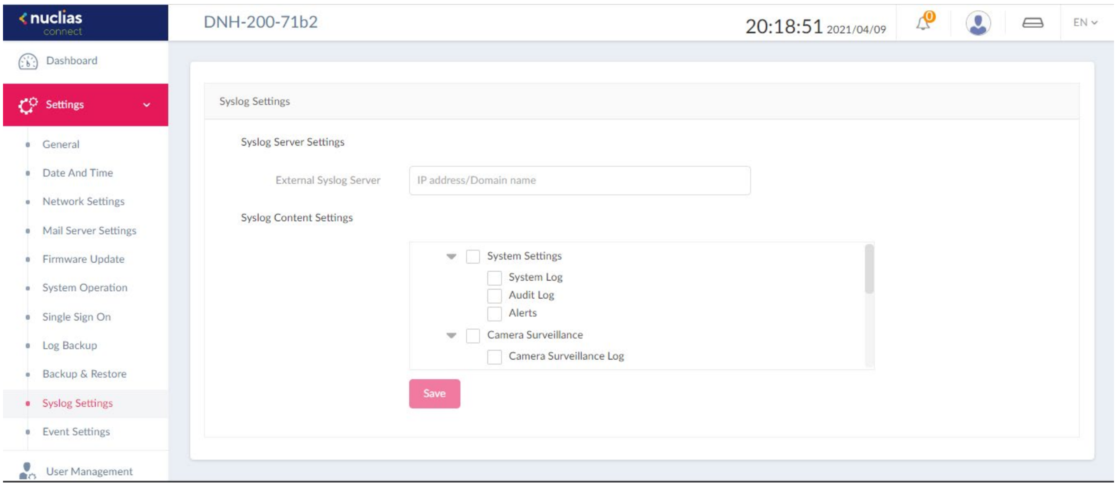
In the **Configuration Restore** section, device configuration can be restored from a local hard drive or USB storage.

Specify the following parameters, then click **Restore** to restore your system.

Restore Configuration From	Choose either **My Computer** or **DNH-200 storage** to upload your configuration file.
File	Click **Choose File** to browse your local directory and select your configuration file.

Syslog Settings

The **Syslog Settings** page allows you to back up system logs to a remote site. Navigate to **Settings > Syslog Settings** to configure the location of an external backup server and the type of logs for backup.



Syslog Settings

Syslog Server Settings

External Syslog Server: IP address/Domain name

Syslog Content Settings

- □ System Settings
  - □ System Log
  - □ Audit Log
  - □ Alerts
- □ Camera Surveillance
  - □ Camera Surveillance Log

Save

In the **Syslog Server Settings** section, enter the IP address or domain name of an external syslog server.

In the **Syslog Content Settings** section, select the log type to be backed up from the 3 major modules of the Hub.

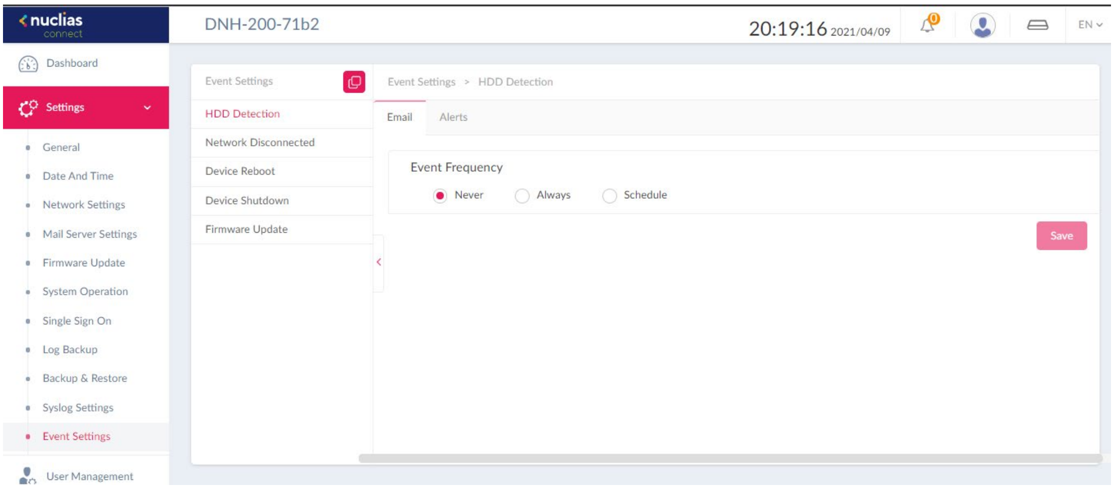
Function Group	**Log Type**
System Settings	System Log
	Audit Log
	Alerts
Camera Surveillance	Camera Surveillance Log
	Camera Log
	Audit Log
	Alerts
	Event Log
AP Network	Device Syslog
	System Event Log
	Device Log
	Audit Log
	Alerts

Click **Save** to save the settings and update the screen.

Event Settings

The **Event Settings** page allows you to configure automatic notifications based on event type. Navigate to **Settings > Event Settings**.

To configure an event notification:



Event Frequency ● Never ○ Always ○ Schedule

1. Select an event type in the left pane from the following: **HDD Status Detection, Network Disconnected, Device Reboot, Device Shutdown,** and **Firmware Update**.
2. For each event type, you can configure both email notifications and system alerts. Configure the following for Email Notification:

Event Frequency	Choose one of the following: Never, Always, or Schedule **Never:** no email notifications will be sent for this type of event. **Always:** designated users will receive email notifications whenever the event happens. **Schedule:** send notifications according to the defined schedule.
Contacts	For **Always** and **Schedule**, select users to receive email notifications whenever the event happens by keeping them in the **Authorized Users** list. Select users and move them to the **Unauthorized Users** list to exclude them from the recipient list.
Schedule	Click the start time and drag to the end time of the selected days of the week to specify time periods for scheduled notifications. You can replicate the scheduled time periods

	among different days of the week by clicking ⧉.

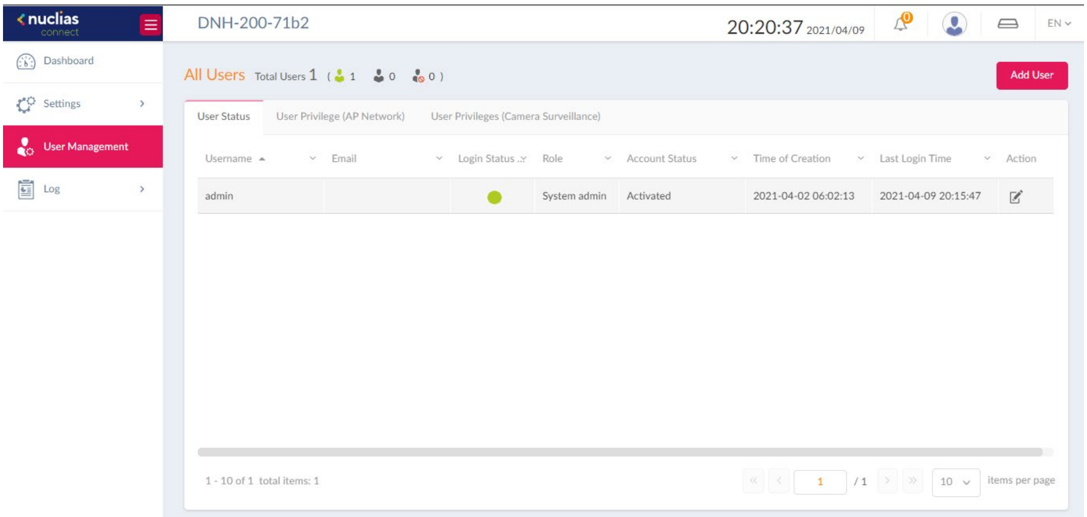
Click **Save** to save the values and update the screen.

Note: The Authorized/Unauthorized Users List is obtained from the users list in **User Management** of **System Settings**. For email notifications, the emails are obtained from the entered email addresses of the User’s List. Please refer to User Management for more information.

To configure alert notifications, click the **Alerts** tab and follow the same steps for setting email notifications above.
To view system alerts, go to **Log > Alerts**.

User Management

The **User Management** page allows administrators to view the current status of all registered user profiles as well as edit and delete the profile. Navigate to **User Management** to view the relevant information.


nuclias connect
Dashboard
Settings
User Management
Log
DNH-200-71b2
20:20:37 2021/04/09
EN
All Users Total Users 1 (1 0 0)
Add User
User Status
User Privilege (AP Network)
User Privileges (Camera Surveillance)
1 - 10 of 1 total items: 1
1 / 1
10
items per page

Username	Email	Login Status	Role	Account Status	Time of Creation	Last Login Time	Action
admin		●	System admin	Activated	2021-04-02 06:02:13	2021-04-09 20:15:47	✎

User Status

The User Status displays the login state of the user, indicating a logged-in or logged-off state.

To edit a user’s profile, select a user and click ✎. The username, password, email, role, account status, location, and contact phone number as well as the user description can be modified from the modifications page. Note that the system administrator account cannot be deleted or have its username or privilege settings changed.

Once you have finished editing user settings, click **Save** to confirm or **Cancel** to return to the previous menu.

Notes:

1. The System Admin account cannot be deleted or have its username and privilege settings modified.
2. The time limit for idle web sessions is 15 minutes. You will be logged out when the limit has been reached.

The following are the available user roles and descriptions of their privileges:

System Admin: This is the operator account and cannot be deleted. Only the System Admin can modify the system related configurations in **Settings** and edit all users in **User Management.** In addition, this role can view the **Audit Log** in **Log**.

Root Admin: Can manage all sites/networks on this server. This role can edit users with the below roles. In addition, this role can view the **Audit Log** in **Log**.

Root User: Can view all sites/networks on this server.

Local Admin: Can manage his own network.

Local User: Can view his own network.

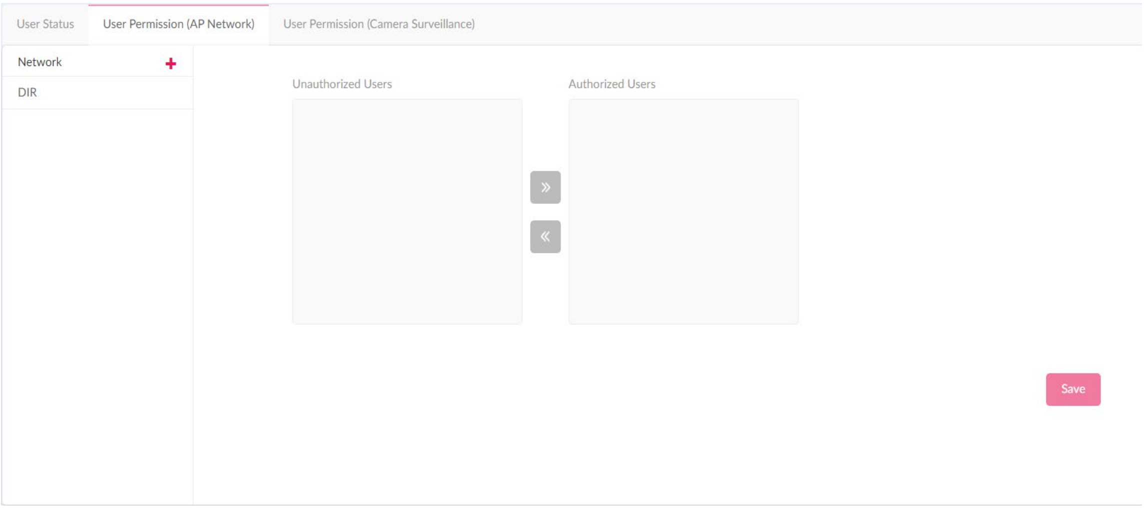
Front Desk Staff: Can generate and manage passcodes.

To add a user, click **Add User** in the upper-right corner. In the Create User page enter the new user information. Fields marked with an asterisk (*) are required to complete the new entry. Once the information is filled completely, click **Create** to savethe new user profile. Alternatively, click **Cancel** to return to the previous screen without saving.

A user can be authorized to a selected AP Network or granted the permission to access selected channels in Camera Surveillance.

User Permission (AP Network)

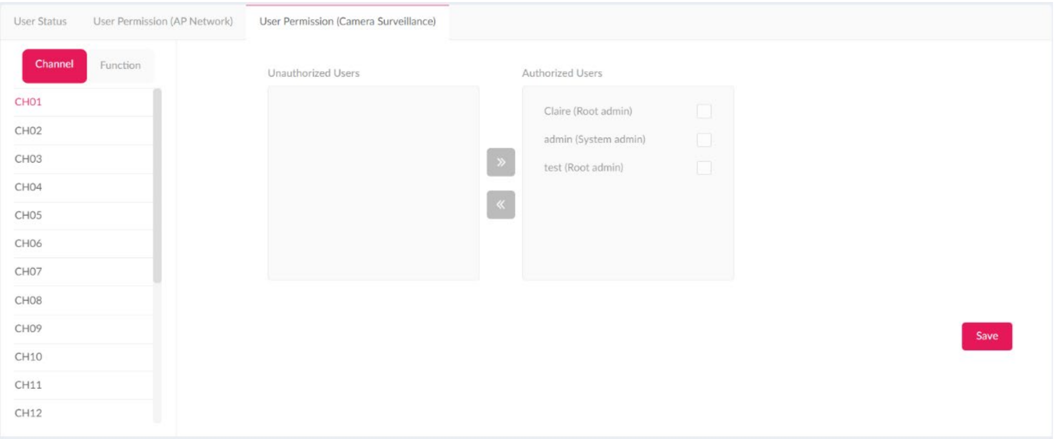
To grant an existing user the right to a network, click an available site and the target network, and select users and move them to the **Unauthorized Users** list or keep them in the original **Authorized Users** list. Then click **Save** to apply your settings.


User Status
User Permission (AP Network)
User Permission (Camera Surveillance)
Network
+
DIR
Unauthorized Users
Authorized Users
»
«
Save

User Permission (Camera Surveillance)

For **Camera Surveillance**, first select a channel in the left pane, and select users and move them to the **Unauthorized Users** list or keep them in the original **Authorized Users** list. Then click **Save** to apply your settings.

You can also configure the permission for exporting video recordings on the **Function** tab. Refer to the **Export** function in **Camera Surveillance > Timeline**.

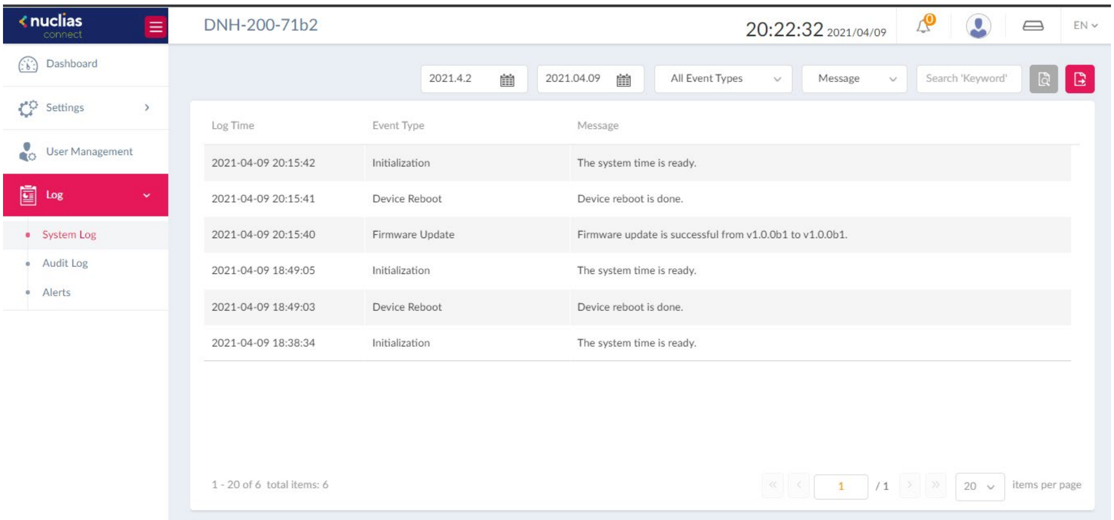

User Status
User Permission (AP Network)
User Permission (Camera Surveillance)
Channel
Function
CH01
CH02
CH03
CH04
CH05
CH06
CH07
CH08
CH09
CH10
CH11
CH12
Unauthorized Users
Authorized Users
Claire (Root admin) □
admin (System admin) □
test (Root admin) □
»
«
Save

Log

The Log page stores the activities of the system and the log entries are grouped into the following categories: **System Log, Audit Log,** and **Alerts**. To navigate among log types, select the respective tab. In each log window, you can apply type-specific filters, for example, event types to see log entries of your interest.

System Log

The System Log page allows administrators to view alert messages for events concerning system operation. Log messages for the system can be viewed here. Navigate to **Log > System Log** to view the relevant information.



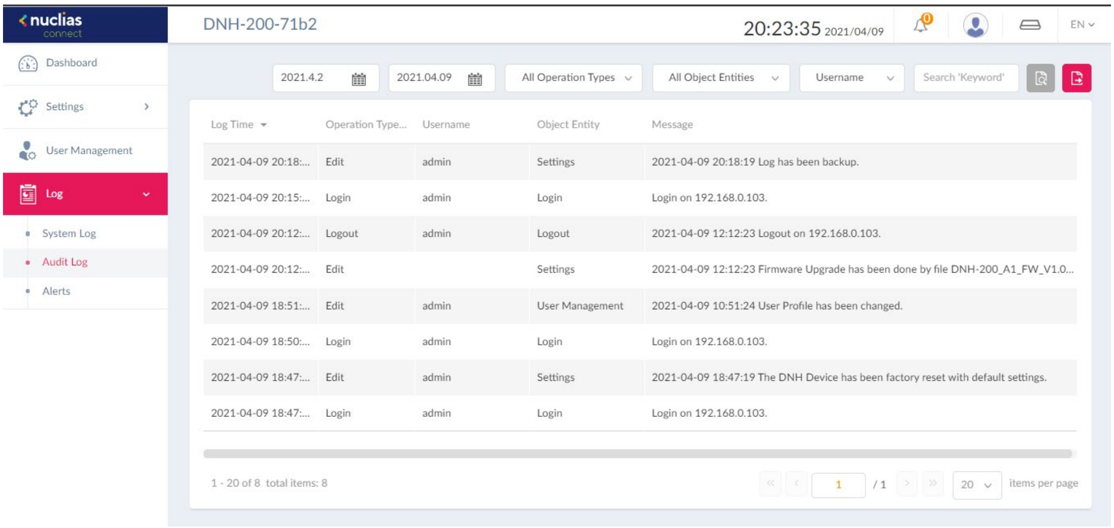
Log Time	Event Type	Message
2021-04-09 20:15:42	Initialization	The system time is ready.
2021-04-09 20:15:41	Device Reboot	Device reboot is done.
2021-04-09 20:15:40	Firmware Update	Firmware update is successful from v1.0.0b1 to v1.0.0b1.
2021-04-09 18:49:05	Initialization	The system time is ready.
2021-04-09 18:49:03	Device Reboot	Device reboot is done.
2021-04-09 18:38:34	Initialization	The system time is ready.

To generate a System Log report, select the time period, select the system event type, enter a keyword to filter the log messages, then click to display the search results.

Once a report has been generated, click to export it as a CSV file. The file will be saved in your browser's download directory and will be named as follows: System_Settings_*Log Type_YYYY_MMDD_HHMMSS*.

Audit Log

This type of log records user activities such as configuration editing or deletion, and login and logout of the system.



Log Time	Operation Type...	Username	Object Entity	Message
2021-04-09 20:18:...	Edit	admin	Settings	2021-04-09 20:18:19 Log has been backup.
2021-04-09 20:15:...	Login	admin	Login	Login on 192.168.0.103.
2021-04-09 20:12:...	Logout	admin	Logout	2021-04-09 12:12:23 Logout on 192.168.0.103.
2021-04-09 20:12:...	Edit		Settings	2021-04-09 12:12:23 Firmware Upgrade has been done by file DNH-200_A1_FW_V1.0...
2021-04-09 18:51:...	Edit	admin	User Management	2021-04-09 10:51:24 User Profile has been changed.
2021-04-09 18:50:...	Login	admin	Login	Login on 192.168.0.103.
2021-04-09 18:47:...	Edit	admin	Settings	2021-04-09 18:47:19 The DNH Device has been factory reset with default settings.
2021-04-09 18:47:...	Login	admin	Login	Login on 192.168.0.103.

1 - 20 of 8 total items: 8

1 / 1 20 items per page

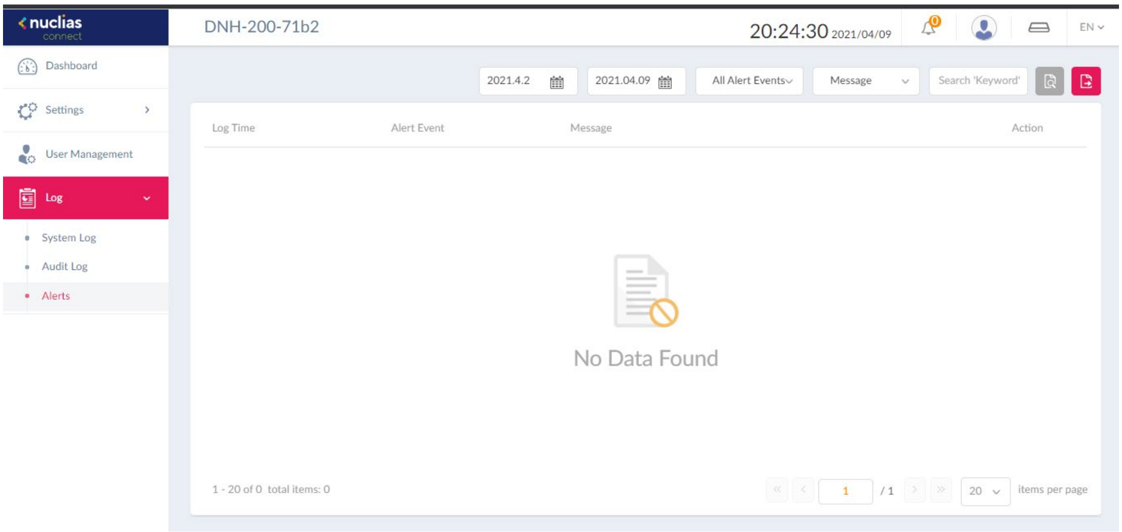
To generate an Audit Log report, select the time period, select the entries by operation type (operations that performed on the object entities) and object entity (i.e., the objects associated with the functional tabs in the left pane), and select username. Then click to display the search results.

Once a report has been generated, click to export it as a CSV file. The file will be saved in your browser's download directory and will be named as follows: System_Settings_*Log Type_YYYY_MMDD_HHMMSS.*

Note: The **Audit Log** is only available to users with the **System Admin** or **Root Admin** role.

Alerts

This type of log records event activities for alert, i.e., **HDD Status Detection, Network Disconnected, Device Reboot, Device Shutdown,** and **Firmware Update**. The alerts are generated according to the rules based on event frequency and authorized users. Refer to **Settings > Event Settings** for more information.



2021.4.2 – 2021.04.09

No Data Found

1 - 20 of 0 total items: 0

To generate an Alert report, select the time period, select the event type, and enter a keyword to filter the log messages. Then click to display the search results.

Once a report has been generated, click to export it as a CSV file. The file will be saved in your browser's download directory and will be named as follows: System_Settings_*Log Type_YYYY_MMDD_HHMMSS*.

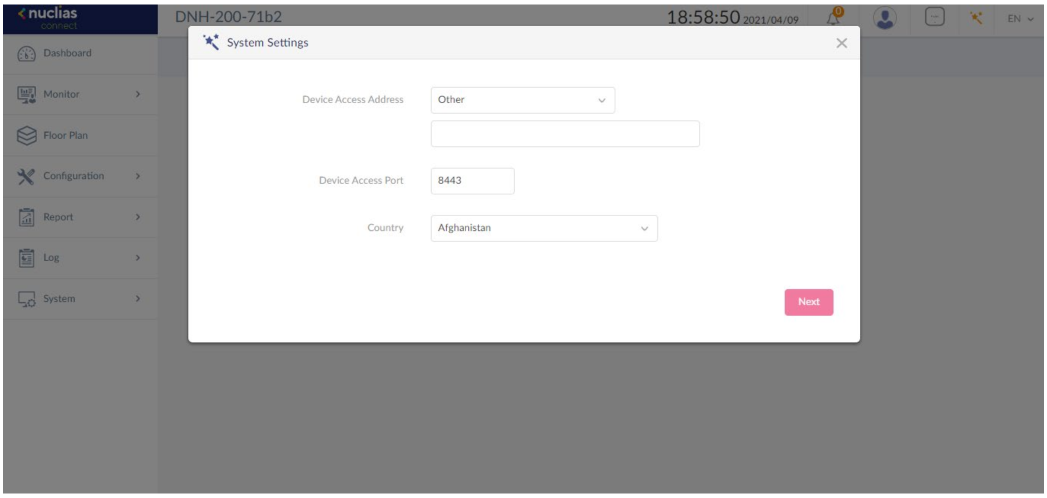
AP Network

Wizard

A wizard is available to guide you through first-time setup of the device. Follow the instructions to complete the process of device configuration. The wizard can be accessed and run repeatedly by clicking the icon in the upper-right corner.

Follow these steps of the setup wizard:

1. On the **System Settings** page, the Hub connection parameters can be configured. These settings allow the management computer to connect to the device.



System Settings

Device Access Address: Other

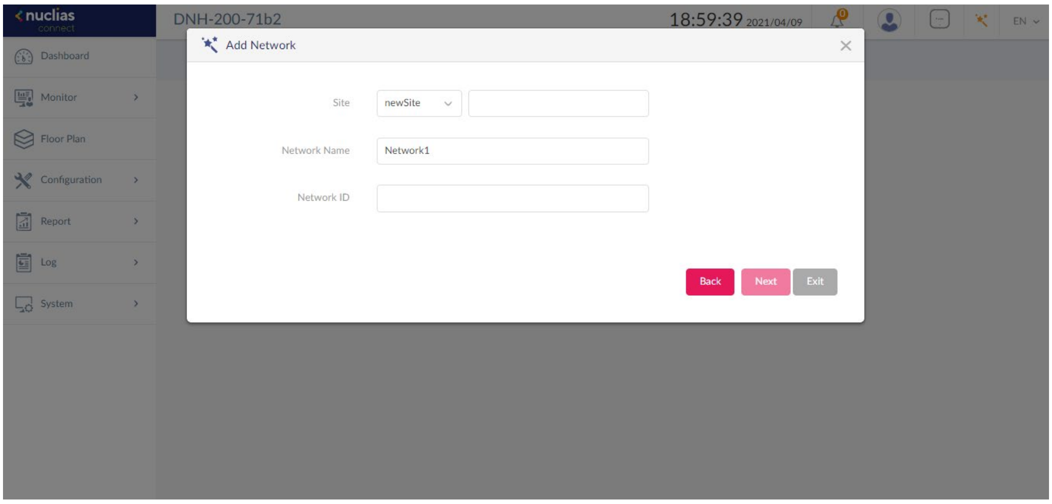
Device Access Port: 8443

Country: Afghanistan

Device Access Address	Enter the Nuclias Connect Server application's IP address. To manage remote APs, the IP address must be a public IP address; You may need to set port forwarding or IP address mapping between WAN and LAN for instances behind a firewall or router.
Device Access Port	Enter the Nuclias Connect server application's listening port number. The default value is 8443. For remote AP management behind a firewall or router, use this port information for setting port forwarding.
Country	Select your country.

Click **Next** to continue.

2. On the **Add Network** page, from the **Site** menu, select an existing site or select newSite and enter a name that describes the site in the text field.
3. In the **Network Name** field, enter a name to identify the new network. In the **Network ID** field, enter a unique key for REST API data communication credential (optional). Click **Next** to continue or **Exit** to return to the previous screen.



Add Network

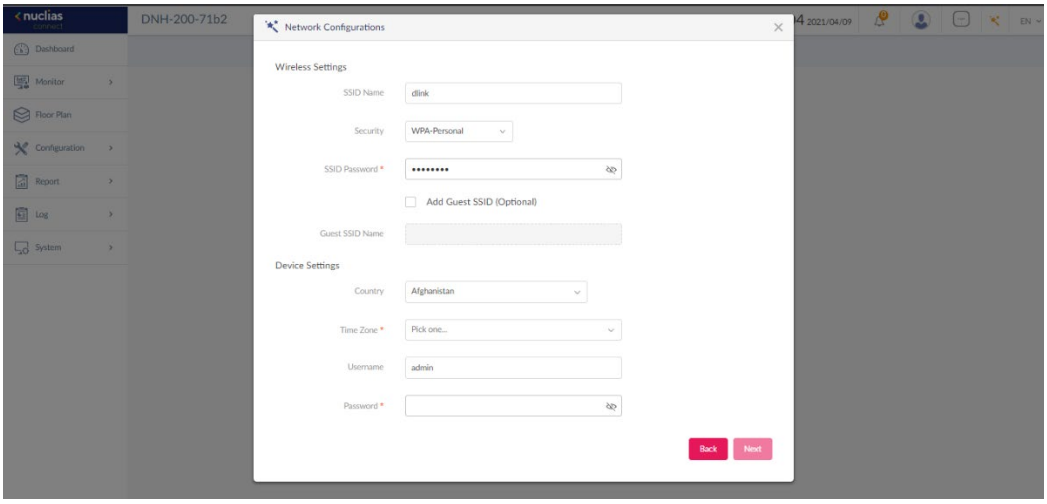
Site: newSite

Network Name: Network1

Network ID:

4. On the **Network Configurations** page, enter the wireless and device settings to set up the wireless network such as the SSID and the device information.

Country	Select your country.
Time Zone	Select the time zone for your device.
Username/Password	Enter the administrative username/password that is used to access the web management interface for all access points on the network.



Network Configurations

Wireless Settings

SSID Name: dlink

Security: WPA-Personal

SSID Password *: ••••••••

□ Add Guest SSID (Optional)

Guest SSID Name:

Device Settings

Country: Afghanistan

Time Zone *: Pick one...

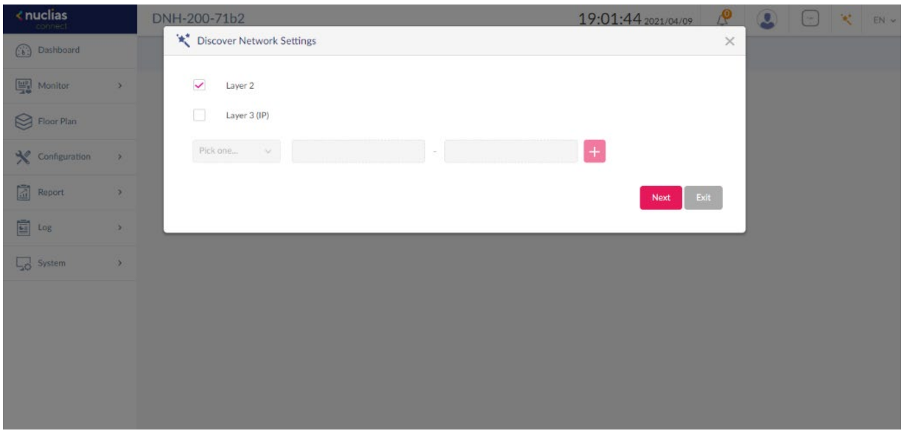
Username: admin

Password *:

Click **Next** to continue. To return to the previous page, click **Back**. Click **Exit** to discontinue the configuration process.

5. On the **Discover Network Settings** page, Select the data link layer (layer 2 or layer 3) to

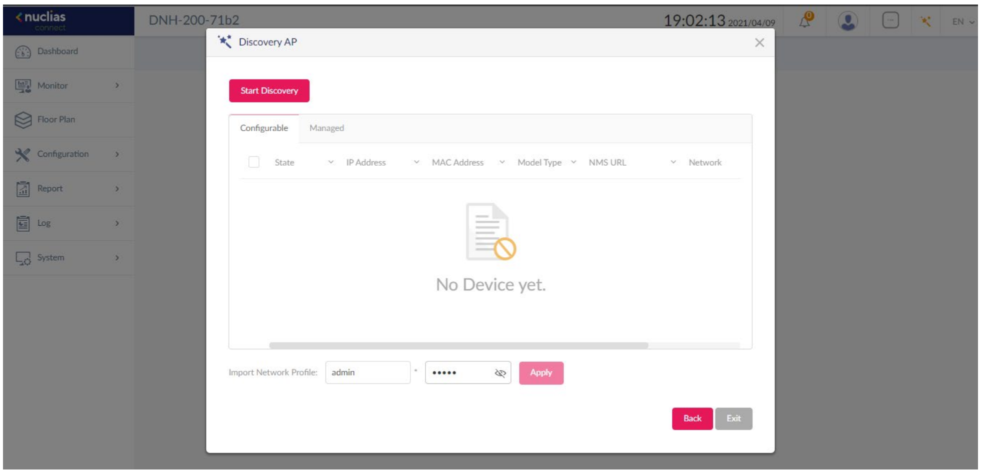
define the type of network in which to find manageable access points. If Layer 3 is selected, click the drop-down menu to define either an IP or a network prefix.



☑ Layer 2

□ Layer 3 (IP)

6. The **Discovery AP** page appears. Click **Start Discovery** to list all available unmanaged devices. If a device is found, select it and click **Apply** to import the network profile. Click the **Managed** tab to select already defined devices and add them to this network. Then click **Exit** to end the wizard.



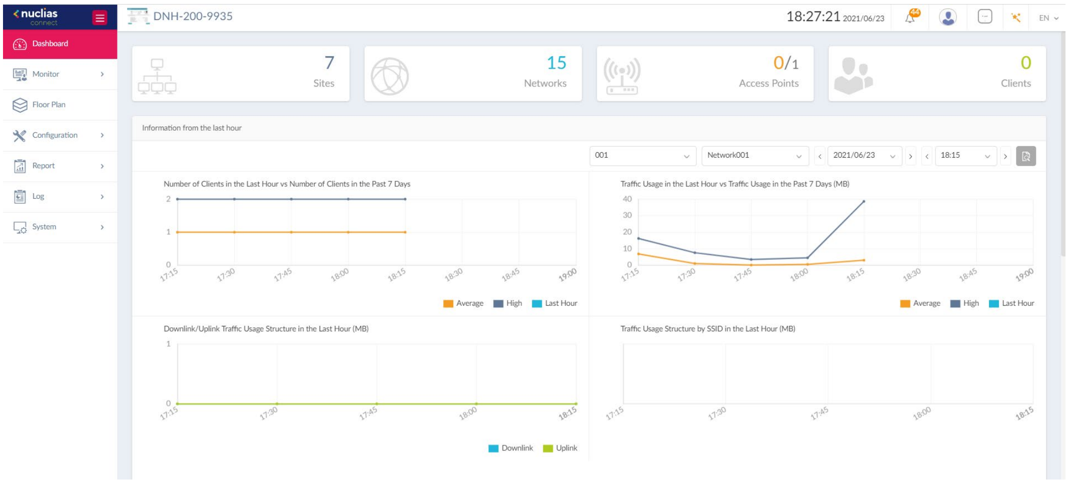
□	State	IP Address	MAC Address	Model Type	NMS URL	Network

No Device yet.

Import Network Profile: admin * •••••

Dashboard

The **Dashboard** page presents a summary of network resources and resource utilization information.



To view the information from the last hour vs. from the past 7 days, select the site and the network, and define the interested date and time. Then click to display the information. The graphs display the relevant information for the last hour of the selected time and any day from the past 7 days.

The following table lists the information presented on the page:

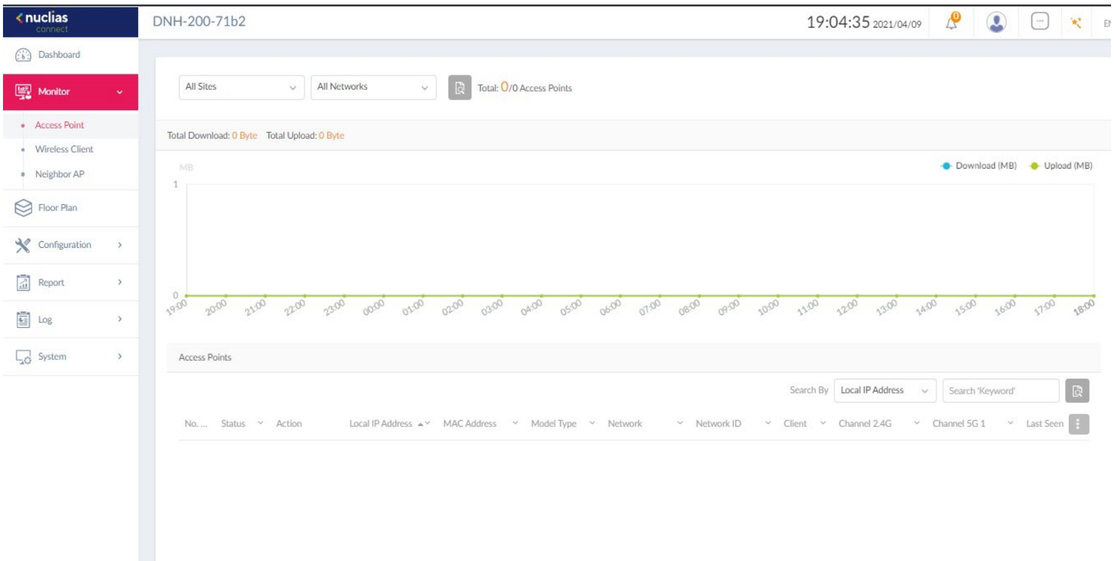
Sites	Displays the number of created profiles,also called sites.
Networks	Displays the total number of created networks.
Access Points	Displays the total number of availableand online access points.
Clients	Displays the total number of currently connected wireless clients.
Information from the Last Hour	Displays log information for the number of clients, traffic usage, downlink/uplink traffic usage, and traffic usage by SSID.
Channel Utilization	Displays the utilization rate for both 2.4 and 5 GHz radio frequencies.
Latest Events	Displays a shortened log version of the latest events across all or selected sites or networks. Click **See More** in the upper-right corner to view the entire report (**Log >** System Event Log).

Monitor

The **Monitor** page provides reports of all or a selected number of wireless clients and networks managed by the application. It contains these menus: **Access Point, Wireless Client,** and **Neighbor AP.**

Access Point

The Access Point page allows you to generate reports based on **Site**, **Network**, and **AP**. For Site and Network, you can generate individual reports for specific sites or networks or aggregate report for all sites or networks. Navigate to **Monitor > Access Point**.



DNH-200-71b2 19:04:35 2021/04/09

All Sites | All Networks | Total: 0/0 Access Points

Total Download: 0 Byte Total Upload: 0 Byte

Search By: Local IP Address | Search 'Keyword'

To generate a report for a site or all sites, select a specific site or **All Sites** from the menu, then select **All Networks** in the second menu. To generate a report for a network or all networks, select the site that the network belongs to, then select a specific network or **All Networks**.

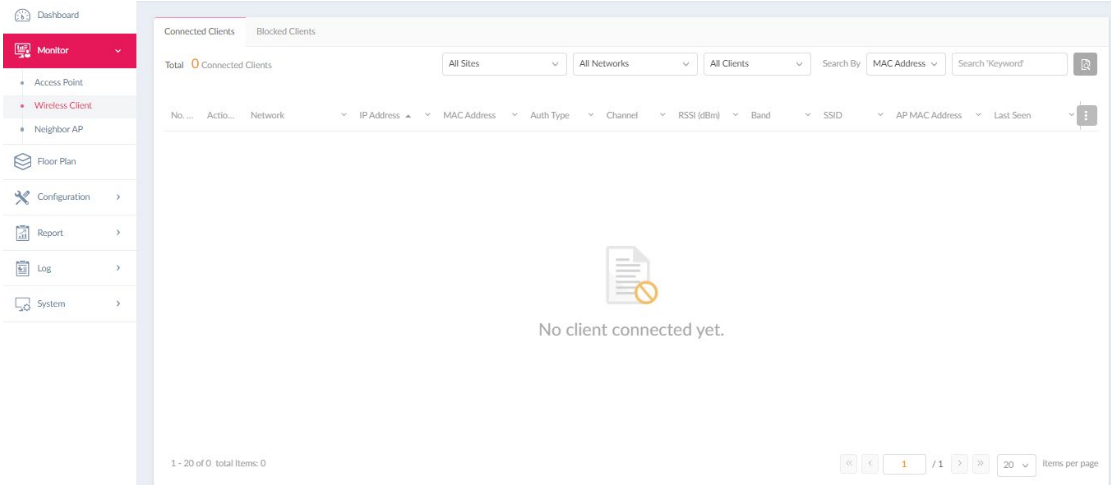
Usage	Displays the total amount of data downloaded and uploaded for the specified site andnetwork.
Total X Access Points	Displays a report listing all detectedwireless clients.

In the **Search By** list, select an attribute (i.e., **Local IP Address**, **Local IPv6 Address**, **NAT IP Address**, **MAC Address**, **Model Type**, **FW Version, Name, Location, Channel 2.4G, Channel 5G, Power 2.4G,** or **Power 5G**) to specify the search condition and enter a keyword in the

Search field. Then click 🔍 to start your search. The results will be displayed below. You can also customize the fields of the report by clicking ⋮. The following field names are available: **Status, Local IP Address, IPv6 Address, MAC Address, Model Type, FW Version, Name, Location, Network, Network ID, Client, Channel 2.4G, Channel 5G 1, Channel 5G 2 (tri-band), Power 2.4G, Power 5G 1, Power 5G 2 (tri-band), Download, Upload, Traffic Usage, Traffic Usage (%), CPU Usage (%), Memory Usage (%), Last Seen,** and **Uptime.**

Wireless Client

The **Wireless Client** page allows you to view reports of all connected clients managed by the application. The statistics can be shown based on **Site**, **Network**, and **Clients**. Navigate to **Monitor > Wireless Client**.



Total 0 Connected Clients

No client connected yet.

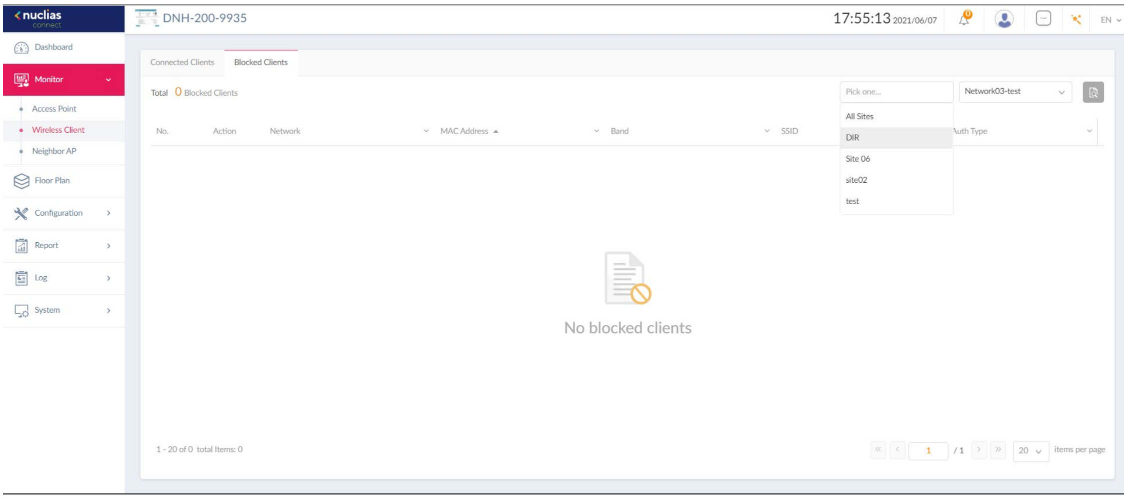
1 - 20 of 0 total Items: 0

Three reports can be generated based on **Site**, **Network**, and **Clients**. To generate a report for a site or all sites, select a specific site or **All Sites** from the menu, then select **All Networks** in the second menu. To generate a report for a network or all networks, select the site that the network belongs to, then select a specific network or **All Networks**. To generate a report for captive portal clients or all clients, select the site that the network belongs to, select a specific network that the clients belong to, and then select **Captive Portal Clients** or **All Clients**. In the **Search By** field, select an attribute (**IP Address** or **MAC Address**) to search by that field and enter a keyword in the **Search** field. Then click 🔍 to start your search. The results will be displayed below.

You can also customize the fields of the report by clicking ⋮. The following fields are available: **Network, IP Address, IPv6 Address, MAC Address, Auth Type, OS, Upload, Download, Channel, RSSI (dBm), SNR (dB), Band, SSID, AP MAC Address, Traffic Usage, Traffic Usage (%), Last Seen,** and **Uptime.**

Blocked Clients

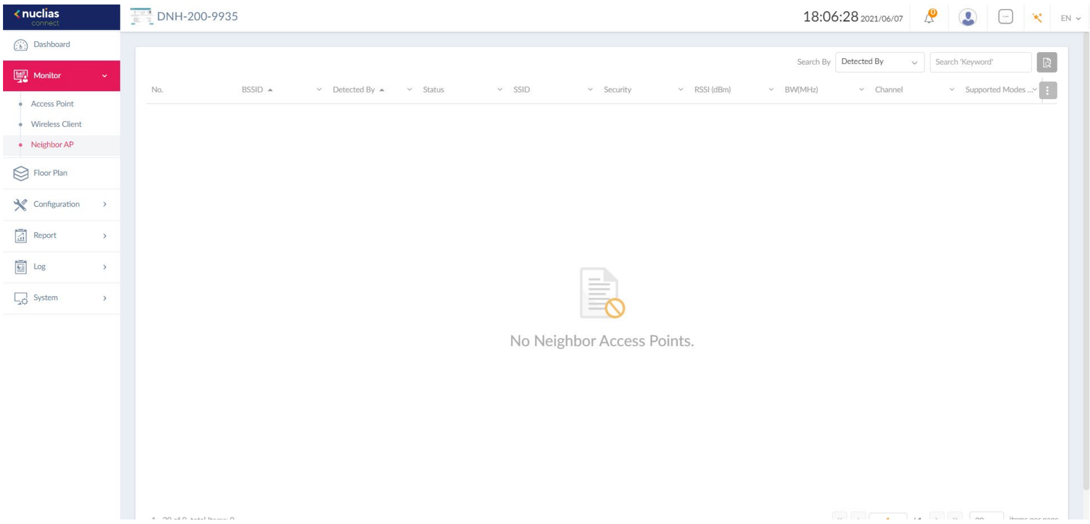
The **Blocked Clients** page allows you to view a report of all blocked clients on the network. This report can be generated based on **Site** and **Network**.



To generate a report, select a specific site or All Sites, select a network or All Networks, then click to start your search. The result displays a list of blocked wireless client connections.

Neighbor AP

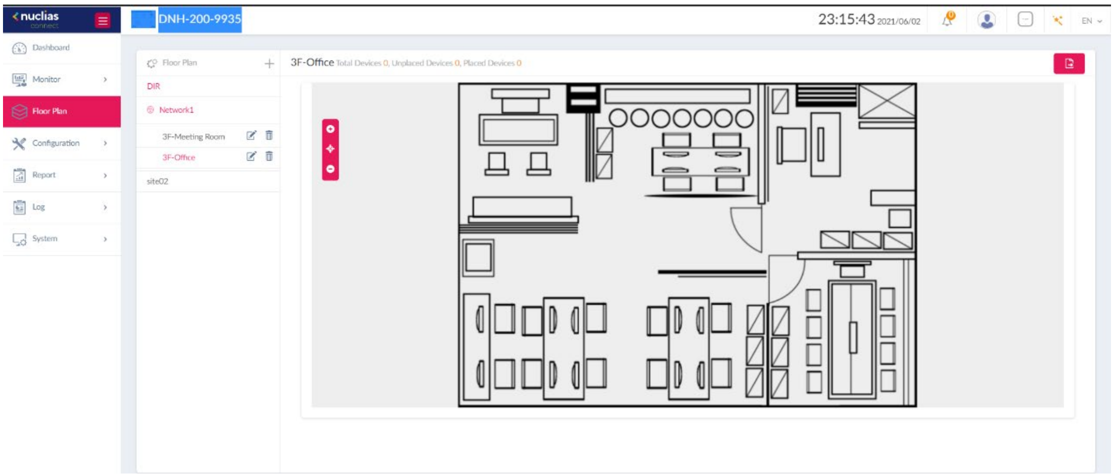
The **Neighbor AP** page allows you to view neighboring access points that are detected on the network. This function is useful if you want to verify the wireless coverage meets your floor plan with the information of APs within the radio range and their signal strength. It can also help detect unauthorized access points in your site to prevent from treats and attacks. Navigate to **Monitor > Neighbor AP**.



To generate a report, select a property in the **Search By** list and enter a keyword. Then click to start your search. The result displays a list of neighbor APs in the radio range that meet the search criteria. You can also customize the fields of the report by clicking ⋮. The following fields are available: **BSSID, Detected By, Status, SSID, Security, RSSI (dBm), BW (MHz), Channel,** and **Supported Modes.**

Floor Plan

The **Floor Plan** page allows you to create geographic representation of your wireless networks. It helps you identify sites and networks quickly for maintenance purposes with visualized locations of the access points.



To create a map for a floor plan, click **+** next to **Floor Plan**. The following parameters should be configured:

Name	Give a name for this map.
Site	Select the site associated with this map.
Network	Select a network that belongs to the site.
Upload Image	Place your image in the area to upload it to the system.

To position an AP, click **Select AP** and drag and drop the selected access point on the map. Then click **Save** to save your changes and update the screen.
You can create multiple maps for a network.

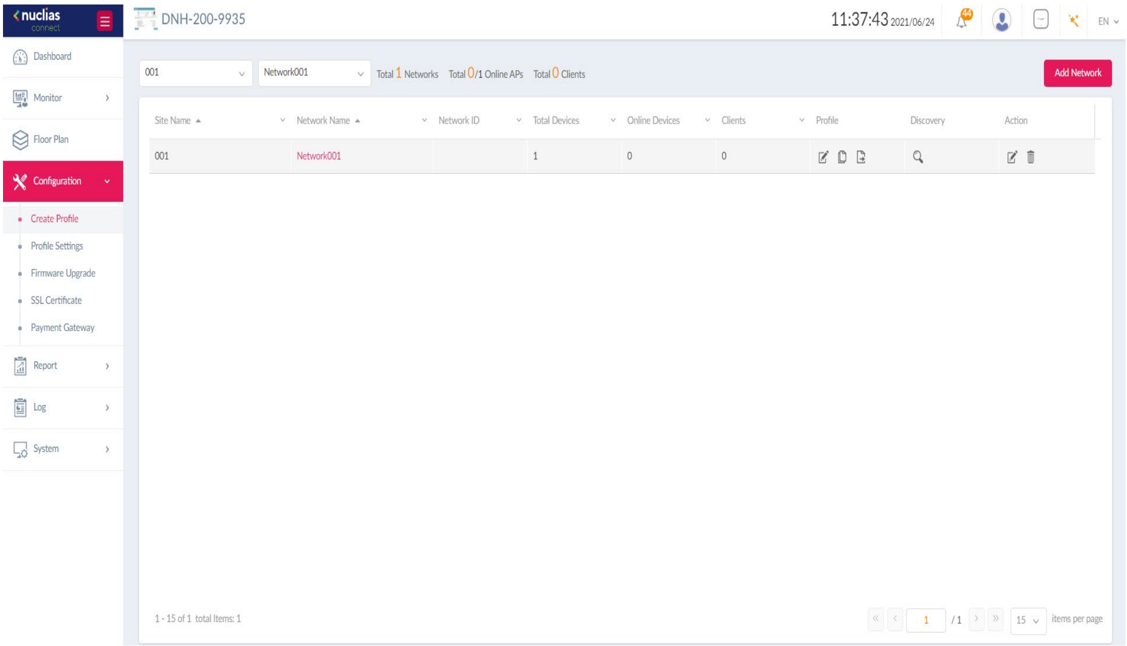
To edit a Floor Plan, select the site name and network, select the map, then click 📝 .

After you are done with a floor plan, you can export it by clicking 🗎.

Configuration

Create Profile

The Create Profile function allows for the creation of new sites and networks. Navigate to **Configuration > Create Profile**.



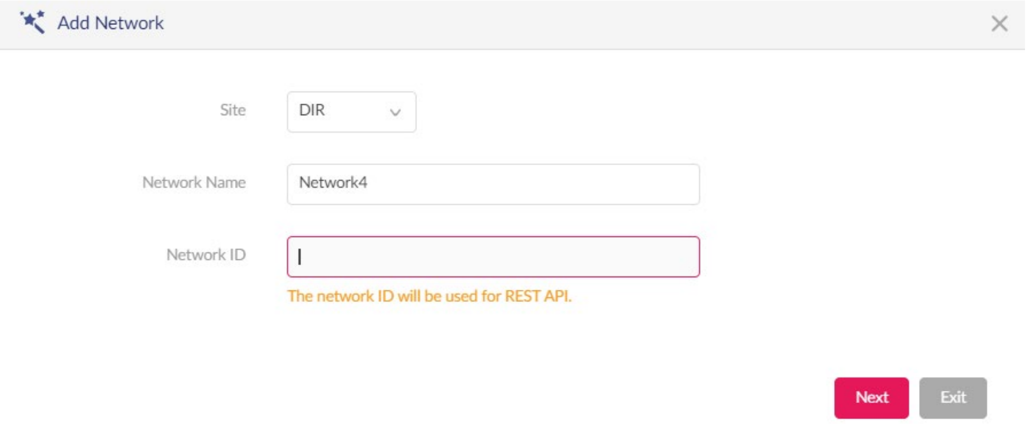
Total 1 Networks Total 0/1 Online APs Total 0 Clients

Site Name	Network Name	Network ID	Total Devices	Online Devices	Clients	Profile	Discovery	Action
001	Network001		1	0	0			

1 - 15 of 1 total Items: 1

To create a new site/network, click **Add Network**.

From the **Site** menu, select an existing site or select **newSite** and enter the name of the site in the text field. In the **Network Name** field, enter a name for the new network. In the **Network ID** field, enter a unique key for REST API data communication credential. Click **Next** to continue.



Add Network

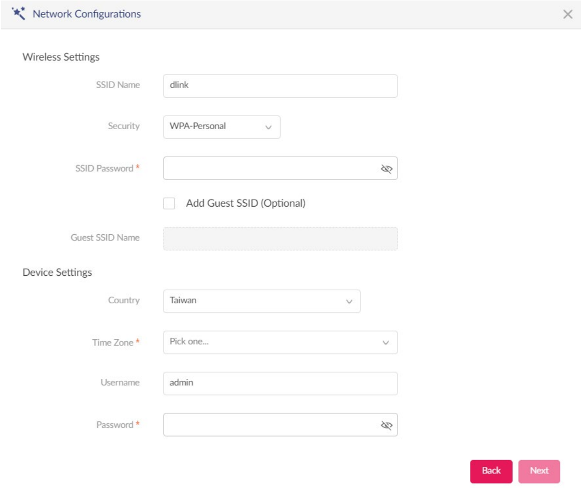
Site: DIR

Network Name: Network4

Network ID: |

The network ID will be used for REST API.

The **Network Configurations** page appears. Enter the Wireless and Device settings to define the wireless network and configure basic information about the device. Click **Next** to continue.



Network Configurations

Wireless Settings

SSID Name: dlink

Security: WPA-Personal

SSID Password *:

□ Add Guest SSID (Optional)

Guest SSID Name:

Device Settings

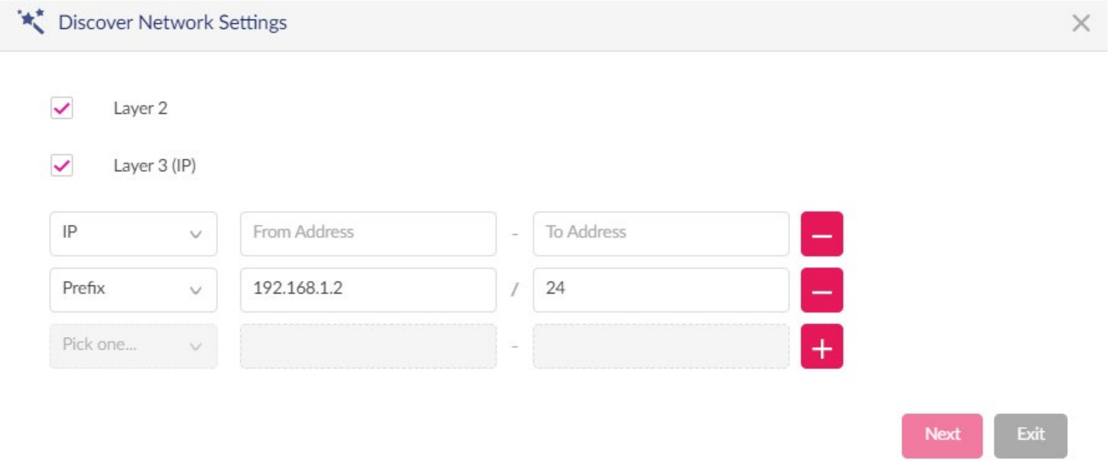
Country: Taiwan

Time Zone *: Pick one...

Username: admin

Password *:

The **Discover Network Settings** page appears. Select the data link layer (layer 2 or layer 3) for the capability of network devices for searching manageable access points. If Layer 3 is selected, click the drop-down menu to define either an IP or a subnet prefix. Click **+** to add additional **IP/prefix** or **Next** to continue. Click **Exit** to discontinue the configuration process.

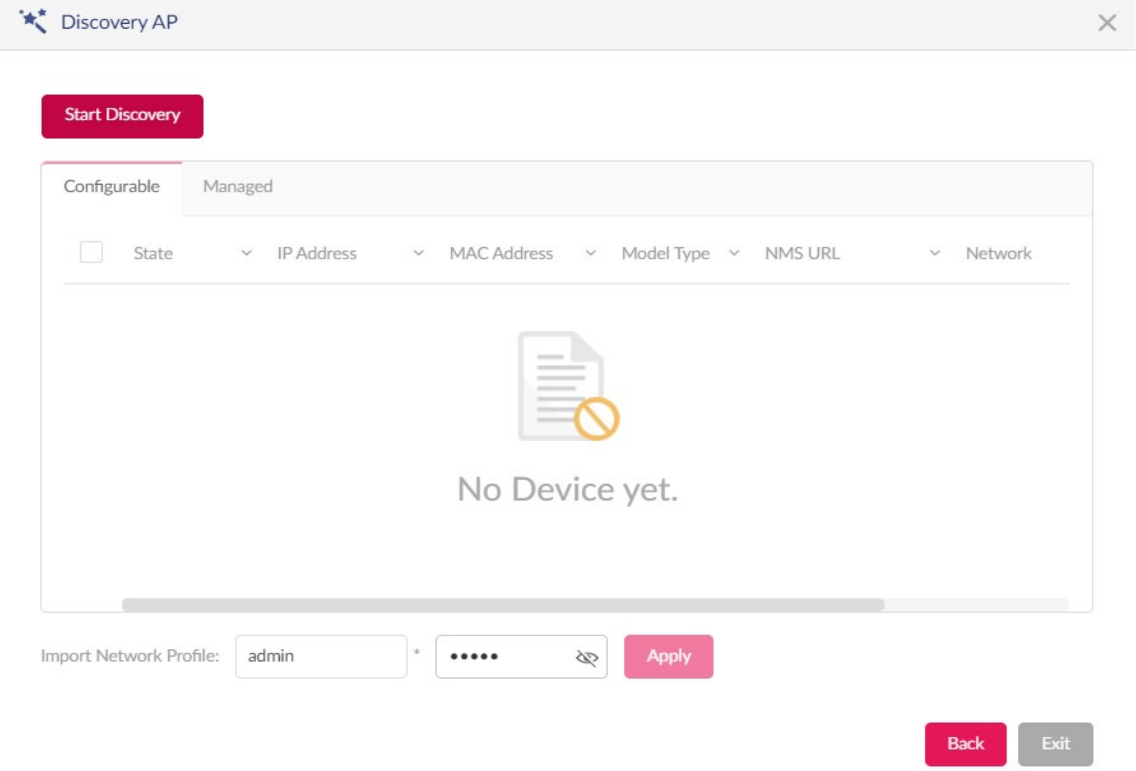

Discover Network Settings

☑ Layer 2

☑ Layer 3 (IP)

IP	From Address	-	To Address
Prefix	192.168.1.2	/	24
Pick one...		-	

The **Discovery AP** page appears. Click **Start Discovery** to list all available unmanaged devices. If a device is found, select it and click **Apply** to import the network profile. Click the **Managed** tab to select already defined devices and add them to the list.


Discovery AP

□	State	IP Address	MAC Address	Model Type	NMS URL	Network

No Device yet.

Import Network Profile: admin * •••••

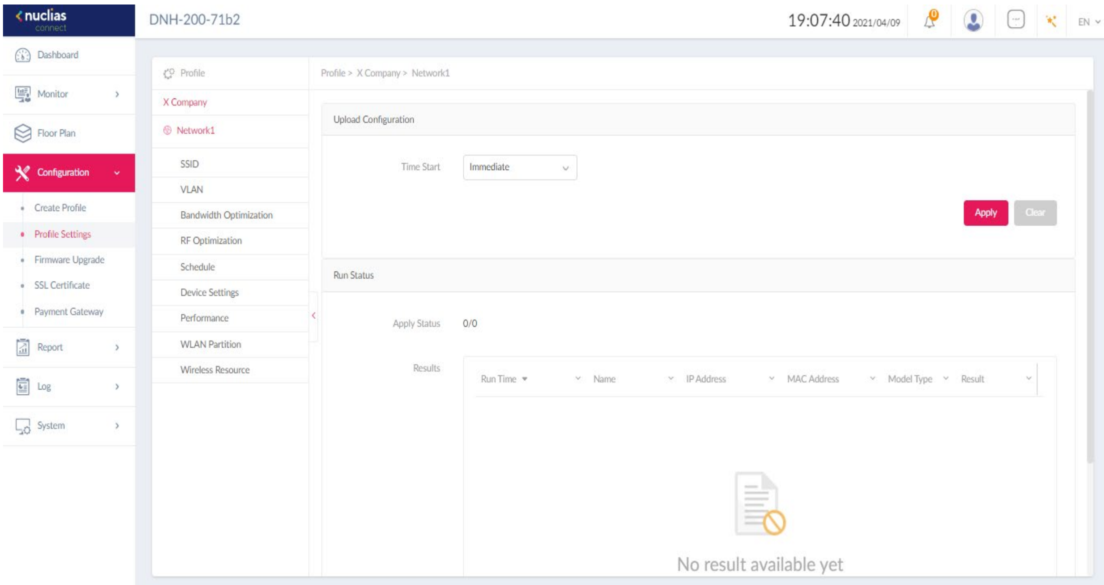
The list should display all sites and networks that have been defined with the following information:

Site Name	The site name of a network.
Network Name	The network name.
Network ID	A unique key for Restful API access.
Total Devices	The total number of access points in this network that belongs to a site.

Online Devices	The total number of access points in this network that are online.
Clients	The total number of clients connected to this network.
Edit Profile	Open **Profile Settings** page. From this page, you can configure more advanced settings for your network such as bandwidth optimization and VLAN.
Copy Profile to this Network	Copy an existing profile to this site and network.
Export Network	Export the selected profile to a file (*.dat) in the local directory.
Discovery	Opens the **Discovery Network Settings** page. From this page, you can search for devices communicated based on L2 protocol layer or specific IP addresses/Prefix subnet. Once the criteria are defined, click **Next**. Click **Start Discovery** to find the results (Configurable and Managed devices) of the search.
Edit Network	Opens the **Edit Network** page. From this page, you can edit the network settings or migrate the network to a new or selected site.
Delete Network	Delete the selected network configuration.

Profile Settings

The **Profile Settings** function allows for the management of existing networks. Navigate to **Configuration > Profile Settings** to view existing sites. Select a site followed by an available network to view all configuration settings: **SSID**, **VLAN**, **Bandwidth Optimization**, **RF Optimization**, **Schedule**, **Device Settings**, **Performance**, **WLAN Partition**, and **Wireless Resource**.



Time Start: Immediate

Apply Status: 0/0

Results

Run Time	Name	IP Address	MAC Address	Model Type	Result

No result available yet

The **Upload Configuration** page will be available when a network is selected.

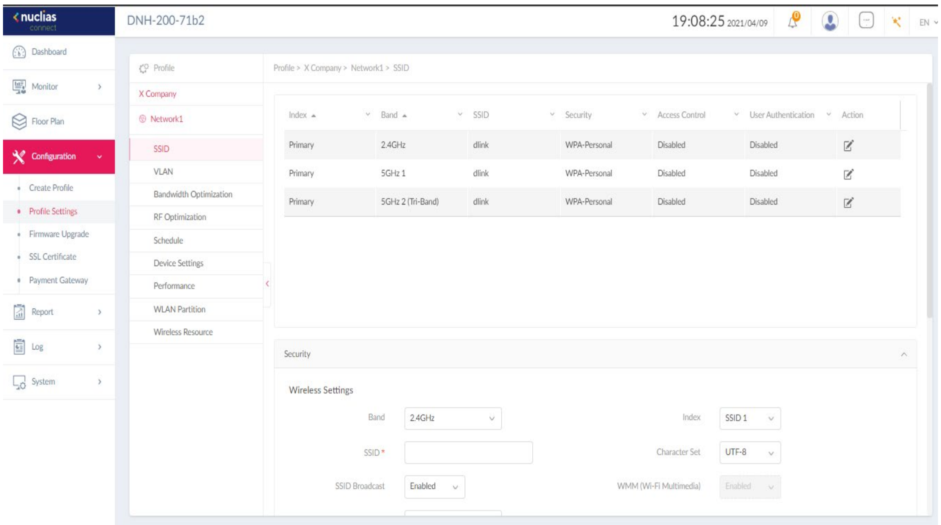
For any updates on network configuration to take effect, the configuration must be uploaded to the access points. In the **Upload Configuration** section, click the **Time Start** menu and select the time (**Immediate** or **Select Time**) to upload the settings immediately or at a configured time.

If **Select Time** is selected, set the date and time to upload the configuration. Then click **Apply** to save your settings.

In the **Run Status** section, the status of the uploads will be listed. Once an update is complete, the results will be displayed in the **Results** area.

SSID

The SSID page displays the properties of a wireless network. Navigate to **Configuration > ProfileSettings > [Site] > [Network] > SSID** to view existing settings.



Index	Band	SSID	Security	Access Control	User Authentication	Action
Primary	2.4GHz	dlink	WPA-Personal	Disabled	Disabled	✎
Primary	5GHz 1	dlink	WPA-Personal	Disabled	Disabled	✎
Primary	5GHz 2 (Tri-Band)	dlink	WPA-Personal	Disabled	Disabled	✎

Band: 2.4GHz
Index: SSID 1
SSID *:
Character Set: UTF-8
SSID Broadcast: Enabled
WMM (Wi-Fi Multimedia): Enabled

To edit the security settings for each radio band of an SSID, click **Edit** under **Action** from the list, and configure the following parameters:

Band	Select wireless frequency.
Index	Select SSID index (Primary and SSID 1 to SSID 7). To create a new SSID, select a new index parameter first.
SSID	Enter the wireless network name. The SSID must be unique for each SSID index.
Character Set	Select the character set to be used in the SSID encoding: UTF-8 or GB2312.
SSID Broadcast	Enable or disable the wireless SSID visibility.
WMM (Wi-Fi Multimedia)	Enable or disable the Wi-Fi Multimedia that facilitates traffic prioritization according to the Access Category.
Security	Select the wireless security standard: Open System (no pre-shared key required), Enhanced Open, Enhanced Open+ Open, WPA-Personal, WPA Enterprise (Radius server required), and 802.1X (Radius server required).
Fast Roaming (802.11 k/v/r)	Enable or disable fast roaming. This function is only available for compatible models and specific software versions.
Encryption	Enable or disable WEP Open System encryption. The function is only available when Security is set as **Open System**.
Key Size (for Open System)	Select the WEP key size: 64 or 128 bits.
Key Type (for Open System)	Select the WEP key type: ASCII or HEX.
Key Value	Enter the open system WEP encryption key. Depending on the key size selected, enter 10 or 26 hexadecimal characters (or 5 or 13 ASCII characters).
Encryption Type	Select the encryption type: Auto, TKIP, or AES (the only option available for WPA3). This option is only available when **Security** is set as **WPA**.
WPA Mode	Select Auto (WPA or WPA2), WPA2 or WPA3, WPA2 Only, or WPA3 Only.
Passphrase	Enter an alphanumeric passphrase. The function is only available when **Security** is set as **WPA-Personal.**
Group Key Update Interval	Enter the WPA group key update interval in seconds.
RADIUS Server/Port/Secret	Enter the RADIUS server's IP address. The function

	is only availablewhen **Security** is **WPA-Enterprise** or **802.1X**. Enter the server's IP address, port number and secret.
Accounting Mode	Enable or disable the use of an accounting server.
Accounting Server/Port/Secret	The RADIUS Server uses an accounting server as a management system to manage users who use a network service. Enter the accounting server's IP address, port number and secret.

Note: Once the settings are updated, the configuration must be uploaded to the access points. See **Create Profile** in the previous section for further information.

In the **Access Control** Section, the following parameters can be configured:

Action	Select the action to be applied to the clients: **Accept** or **Reject**.
MAC Address	Enter the MAC address of the clients that will be allowed or denied access and click **Add**. The maximum number of entries allowed is 512.
Upload MAC Address List	Click **Browser...** to select the MAC address file, located on the local computer, that will be uploaded. Click **Upload** to update the MAC address list. Click **Download** to download the current MAC addresslist. The MAC address list has to be a line break delimited txt file.
IP Filter Settings	Enable or disable **IP Filtering**. The maximum number of entries allowed is 64.
IP Address/ Subnet Mask	Enter the IP address and subnet mask of the clients to which the allow/deny list should be applied.

In the **User Authentication** section, the following parameters can be configured:

Authentication Type	Select the authentication type to be applied to the wireless clients: **Disabled, Web Redirection Only, Username/Password, Remote RADIUS, LDAP, POP3, Passcode, External Captive Portal, MAC Address, Click Through, or Social Login**.
Session/Idle Timeout (2~1440)	Enter the session/idle timeout value.
Enable Simultaneous Login	Check to enable simultaneous login.
Allow (1~720) times	Limit the number of login times per day.

Interval (0~720) minutes	Limit the time interval of a login session.
Enable White List	Check the box to enable the white list function. This function is not available when Authentication Type is **Web Redirection** Only.
MAC Address	Enter the MAC address of the network devices to be in the white list (allow) and click **Add** to add the address to the white list table. The maximum number of entries allowed is 64.
Upload Whitelist File	Click **Browser...** to select the allow list file, located on the local computer, that will be uploaded. Click **Upload** to update the white list. Click **Download** to download the current white list. The MAC address list has to be a line break delimited txt file.
IP Interface Settings	Enable or disable **IP Filtering**.
IP Address/ Subnet Mask	Enter the IP address and subnet mask of the clients to which the allow/deny list should be applied.
IP Interface Settings	Click the drop-down menu to enable or disable the use of the IP interface. Go to **Configuration > Profile Settings >VLAN > Add/Edit IP Interface** to set IP interfaces.
Username	Enter the username. The function is only available when **Authentication Type** is set as **Username/Password**.
Password	Enter the password and click **Add**. Click **Clear** to clear the entered fields. This function is only available when **Authentication Type** is set as **Username/Password**.
Upload Username/Password File	Click **Browser...** to select the username file, located on the local computer, that will be uploaded. Click **Upload** to update the username/password list. Click **Download** to download the current username/password list. The username/password list has to be in excel file format with username and password in adjacent columns.
RADIUS (Primary, 2nd, 3rd) Server/Port/Secret	Enter the RADIUS server's IP address. The function is only available when **Authentication Type** is **Remote RADIUS**. Enter the server's IP address, port number and secret.
Accounting (Primary, 2nd, 3rd) Server/Port	Enter the accounting server's information for keeping the accounting data to complement a RADIUS server.
Remote RADIUS Type	Enter the RADIUS server's type. This option is only available when **Authentication Type** is **Remote RADIUS** or

	MAC Address.
LDAP Server/Port	Enter the LDAP server's IP address and port number. This option is only available when **Authentication Type** is **LDAP**.
LDAP Base DN	Enter the base domain name of the LDAP database. This option is only available when **Authentication Type** is **LDAP**.
Authentication Mode	Select the mode from these options: Simple or TLS.
Account Attribute	Enter an attribute for the account. This option is only available when **Authentication Type** is **LDAP**.
Identity	Enter the identity. This option is only available when **Authentication Type** is **LDAP**.
LDAP Username/Password	Enter the username and password for LDAP server authentication.
POP3 Server/Port	Enter the POP3 server's IP address and port number. This option is only available when **Authentication Type** is **POP3**.
Connection Type	Select the connection type for POP3: None or SSL/TLS.
Passcode List	Displays the configured front desk user accounts that have been assigned to this network and have already generated a passcode from the web login page. This option is only available when **Authentication Type** is Passcode.
External Captive Portal	Select HTTP or HTTPS and enter the URL of the website. This option is only available when **Authentication Type** is External Captive Portal. The captive portal displays a custom web page that authenticates clients for Internet access.
Enable Walled Garden	Before a client can be fully authorized to WLAN connectivity, the wireless connection is only limited to a walled garden. Enable this option to enforce this restriction.
Walled Garden Range	This option allows you to add computers to this walled garden with the following notations: IP address, IP address/subnet or domain name, so a wireless client can be limited to access resources only in the specified range until authorized. The maximum number of entries is 20.
Upload Walled Garden File	Click **Browser...** to select the walled garden list file, located on the local computer, that will be uploaded. Click **Upload**

	to update the walled garden list. Click **Download** to download the current list. The Walled Garden list has to be a line break delimited txt file.
Social Login	Enable login using social media such as Facebook and Google. This option is only available when **Authentication Type** is Social Login.
Web Redirection	Check the box to enable the website redirection function.
Website	Select HTTP or HTTPS. Also, enter the URL of the website as the redirection destination.
Splash Page Authentication Type	Select one of the authentication method to be used on the **Splash Page**: Username/Password, Remote RADIUS, LDAP, POP3, Passcode, Click Through, Social Login, or WiFi4EU Login.
Splash Page Customization Template	Select the login style for wireless network authentication. **Notes:** ● Click **Preview** to preview the selected style. ● Click **Editor** to edit the selected style. ● Click **Upload Login File** to upload a new style. ● Click 🗑 to delete the selected style. ● Click ⭳ to download the selected style.

In the **Hotspot 2.0** section, the following parameters can be configured:

Hotspot 2.0	Enable or disable hotspot 2.0. Configure the following parameters for Hotspot 2.0.
OSEN	Enable online subscription with encryption (OSEN)to indicate that the hotspot uses an OSEN for security support.
Allow Cross Connection	Choose Enable to allow cross connection for clients.
Manage P2P	Choose Enable to allow P2P.
DGAF	This option configures the Downstream Group Addressed Forwarding. Choose Enable to allow AP to forward downstream group addressed frames.
Proxy APR	Choose Enable to allow proxy ARP.
L2TIF	Choose Enable to allow Layer 2 Traffic Inspection and Filtering.
Interworking	Enable or disable the interworking function.

Access Network Type	Choose the access network type.
Internet	Enable or disable Internet access for this network.
ASRA	Choose Enable if the network has Additional Steps Required for Access.
ESR	Choose Enable to indicate that emergency services are reachable through this service.
USEA	Choose to enable or disable Unauthenticated Emergency Service Accessible (UESA).
Venue Group	Specify the venue group (range: 0 to 255).
Venue Type	Specify the type of venue (range: 0 to 255).
Venue Name	Specify the name of the venue. Choose from the list for the language to be used in the name.
HESSID	Specify a homogenous extended service set (ESS) ID that can be used to identify a specific service provider network.
WAN Link Status	Set information about the status of the access point’s WAN connection.
WAN Symmetric Link	Specify whether the WAN link is symmetric (upload and download speeds are the same).
WAN At Capacity	Specify yes if the access point or the network is at its maximum capacity and specify no if not.
WAN Metrics DL Speed (kps)	Set the downlink speed of the WAN connection in kbps. If the downlink speed is not known, set to 0.
WAN Metrics UL Speed (kps)	Set the uplink speed of the WAN connection in kbps. If the uplink speed is not known, set to 0.
Network Auth Type	Choose the network authentication type and specify the web address.
IP Address Type Availability	Choose the IP address version and type that the hotspot operator uses and that would be allocated and available to a mobile device after it has been permitted to the network. You can also delete it from the list.
Domain Name	List one or more domain names for the entity operating the AP.
Roaming Consortium	Add service providers or groups of roaming partners whose security credentials can be used to connect to a network. You can also delete it from the list.
Nai Realm	Specify the name for Network Access Identifier (NAI), which identifies and describes a NAI realm accessible. Click **-** to

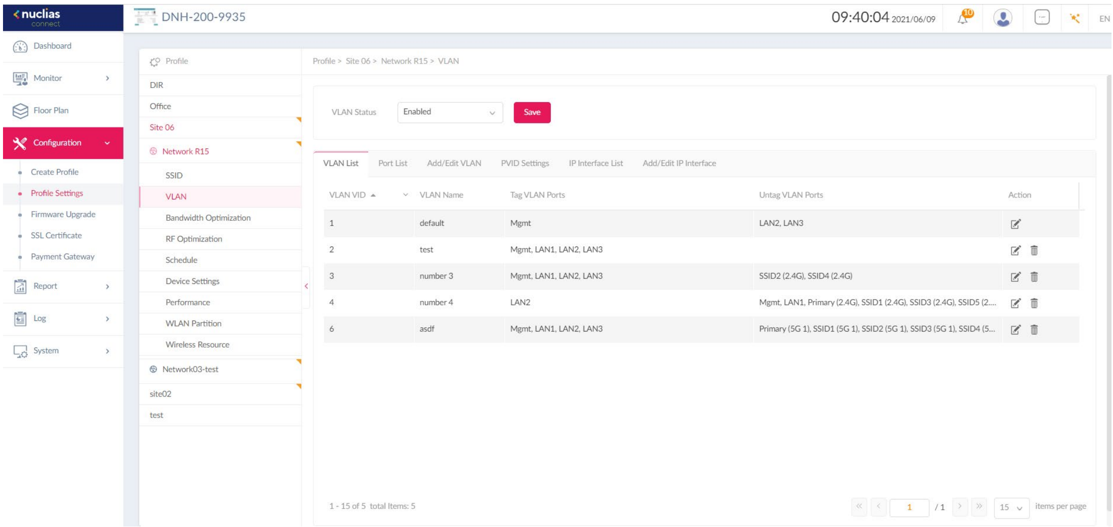
	delete it from the list.
EAP Method	Specify one or more EAP methods and its Authentication ID and Parameter type.
RFC 4282	Enable or disable RFC 4282 for user identification.
3gpp Cellular Network	Specify a list of the 3GPP cellular networks available through the AP. Specify the MCC and MNC, then click **Add**. You can also delete it from the list.
Connection Capability	Specify a list of common IP protocols (TCP, UDP, ICMP) and port number and the status of the IP protocol, then click **Add**. You can also delete it from the list.
Operator Friendly Name	Identify the Hotspot venue operator and choose its language.
OSU SSID	Specify Online Sign-up (OSU) SSID name. It allows a mobile client to choose an available online service and sign up for the online service.
OSU Server URI	Specify OSU Server URI.
OSU Method	Specify a list of OSU methods with its language and the method name, then click **Add**. You can also delete it from the list.
OSU Config	Choose the OSU Configuration.
OSU Language Code	Choose a language.
OSU Friendly Name	Choose a language and specify the OSU friendly name.
OSU Nai	Specify the OSU Network Access Identifier (NAI).
OSU Service Description	Enter a service description for the OSU.
OSU Icon Language Code	Specify the language of the icon.
OSU Icon File Path	Specify the location of the icon file.
OSU Icon File Name	Specify the icon’s file name.
OSU Icon Width	Specify the width of the icon in pixels.
OSU Icon Height	Specify the length of the icon in pixels.
OSU Icon Type	Specify the icon’s file type.
Note: Hotspot 2.0 is only available forcompatible models and specific firmware versions.	

Click **Add** to save the values and update the screen. Click **Clear** to reset all settings. Once the settings are updated, the configuration must be uploaded to the access points. See **Profile Settings** for more information.

VLAN

The VLAN page allows you to create virtual LAN subnets of a physical network. Navigate to

Configuration > Profile Settings > [Site] > [Network] > VLAN to view existing settings.



Profile > Site 06 > Network R15 > VLAN

VLAN Status: Enabled

VLAN VID	VLAN Name	Tag VLAN Ports	Untag VLAN Ports	Action
1	default	Mgmt	LAN2, LAN3	✎
2	test	Mgmt, LAN1, LAN2, LAN3		✎ 🗑
3	number 3	Mgmt, LAN1, LAN2, LAN3	SSID2 (2.4G), SSID4 (2.4G)	✎ 🗑
4	number 4	LAN2	Mgmt, LAN1, Primary (2.4G), SSID1 (2.4G), SSID3 (2.4G), SSID5 (2....	✎ 🗑
6	asdf	Mgmt, LAN1, LAN2, LAN3	Primary (5G 1), SSID1 (5G 1), SSID2 (5G 1), SSID3 (5G 1), SSID4 (5...	✎ 🗑

1 - 15 of 5 total Items: 5

1 / 1 15

VLAN Status

Click the drop-down menu to enable or disable VLANs.

VLAN List

The VLAN List shows a list of created VLANs and their members with Tag/Untag information.

You can click ✎ to modify a selected VLAN or 🗑 to delete a VLAN configuration.

Port List

The **Port List** tab shows the VLAN membership assignment of the ports. It also shows the PVID information of each port.

Add/Edit VLAN

The **Add/Edit VLAN** page allows you to create a new VLAN identified by a VLAN ID and assign ports to that VLAN.

Use the following steps to configure a VLAN:

1. Specify the VLAN ID and the name. The VLAN ID is a unique value assigned to a VLAN. Enter a value between 1 and 4094.
2. Map the listed interfaces and SSIDs for different radio bands to this VLAN with the following options:

   Untagged – Make the interface/SSID untagged from the VLAN. For tagged frames, tags will be removed before being forwarded.

   Tagged – Include the interface/SSID as a member of the VLAN and its frames will be tagged with the VLAN ID. It will only accept frames tagged with the same VID. For untagged frames, they will be tagged with PVID before being forwarded.

   Not Member – Exclude the interface/SSID from the VLAN.

You can also access this tab by clicking **Edit** for an existing VLAN configuration on the **VLAN List** tab.

Note: An SSID can belong to only one Untagged VLAN member. When adding an SSID to a VLAN's Untagged VLAN member, the SSID will be unmembered from another VLAN assigned earlier.

PVID Settings

On the **PVID Settings** tab, you can view and configure the Port VLAN Identifier (PVID) settings for port-based VLAN.

Use the following steps to configure the PVID:

1. Enable or disable **PVID Auto Assign Status**. To manually configure PVID for each SSID, disable this option.
2. Input a VLAN ID for the listed interfaces and SSIDs.

Every untagged frame leaving from the configured port will be assigned a tag to identify its membership.

IP Interface List

The **Port List** tab shows the VLAN ID with the IP settings. It shows the VLAN ID with the IP assignment method and the IP address.

Add/Edit IP Interface

In the **Add/Edit IP Interface** tab, you can assign a VLAN ID (VID) with an IP interface. This is useful when authenticating users for network access through a captive portal. You can configure Captive Portal for each virtual wireless subnet. For other configuration parameters of controlled network access, go to **Configuration > Profile Settings > SSID** and click **User Authentication**.

Use the following procedure to configure an IP interface:

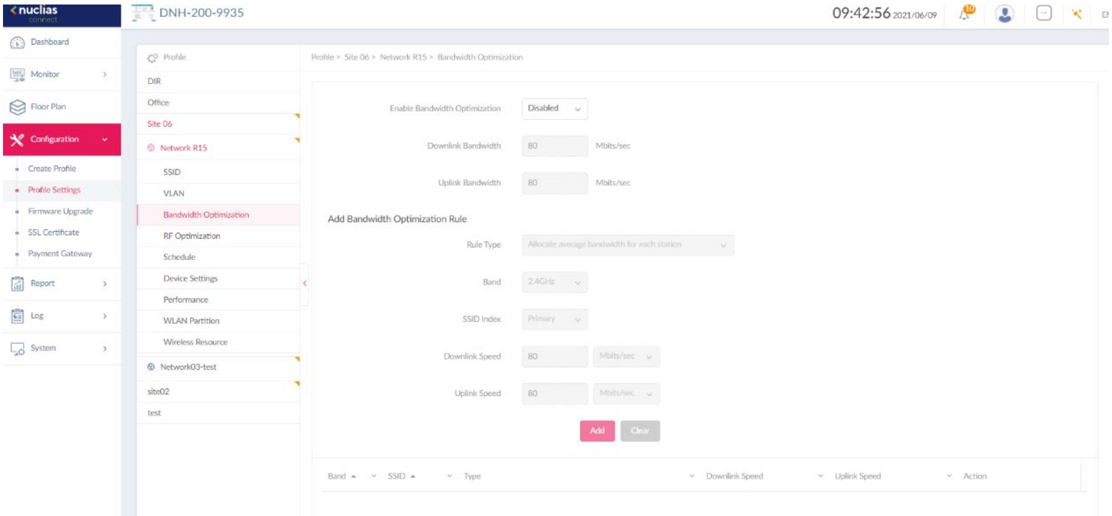
1. Enter a VLAN ID (VID) that has been configured.
2. Select the IP assignment method from the **Get IP Address From** list. If **Static IP Address** is used, enter the **IP Address** and **Subnet Mask** of the IP interface. Then enter the Gateway and DNS server addresses.
3. Click **Add** to add this entry to the IP Interface List. The list also allows you to modify an entry.

Once the settings are updated, the configuration must be uploaded to the access points. See **Profile Settings** for more information.

Bandwidth Optimization

The Bandwidth Optimization page allows you to optimize available bandwidth. Navigate to

Configuration > Profile Settings > [Site] > [Network] > Bandwidth Optimization to view existing settings.



Profile > Site 06 > Network R15 > Bandwidth Optimization

Enable Bandwidth Optimization: Disabled

Downlink Bandwidth: 80 Mbits/sec

Uplink Bandwidth: 80 Mbits/sec

Add Bandwidth Optimization Rule

Rule Type: Allocate average bandwidth for each station

Band: 2.4GHz

SSID Index: Primary

Downlink Speed: 80 Mbits/sec

Uplink Speed: 80 Mbits/sec

Band	SSID	Type	Downlink Speed	Uplink Speed	Action

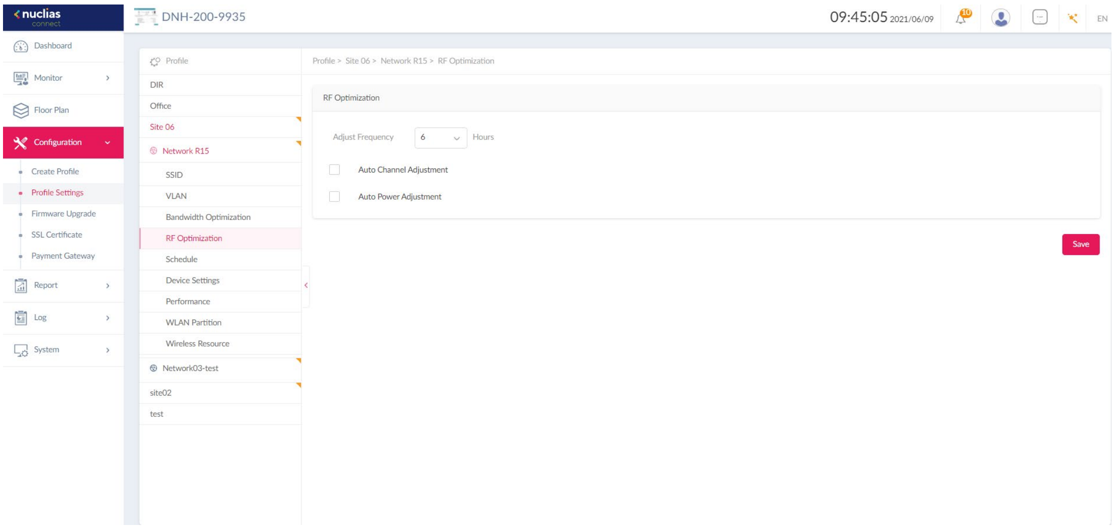
Enable Bandwidth Optimization	Enable or disable bandwidth optimization. Enable this to configure with the following settings.
Downlink Bandwidth	Enter the total downlink bandwidth for the access points in Mbits/sec.
Uplink Bandwidth	Enter the total uplink bandwidth for the access points in Mbits/sec.
Rule Type	Select the rule type: ● Allocate average bandwidth for each station: Optimize bandwidth by averaging the allocated bandwidth for each client. ● Allocate an upper limit of bandwidth for each station: Specify the maximum bandwidth for each connected client, while reserving available bandwidth for other uses. ● Allocate different bandwidth limits for 11a/b/g/n station: The weights of 802.11b/g/n and 802.11a/n clients are 10%/20%/70% and 20%/80% respectively. The AP will distribute different amount of bandwidth for 802.11a/b/g/n clients. ● Allocate specific bandwidth for SSID: All clients share the assigned bandwidth.
Band	Select the wireless frequency band used in the rule.
SSID Index	Select the SSID used in the rule.
Downlink Speed	Enter the downlink speed assigned to each station or the

	specified SSID depending on the rule type.
Uplink Speed	Enter the uplink speed assigned to each station or the specified SSID depending on the rule type.
Add	Click **Add** to add the rule for the network with the designated radio frequency into the Bandwidth Optimization Rules.
Clear	Click **Clear** to clear the entered rule.

Click **Save** to save the values and update the screen.
Once the settings are updated, the configuration must be uploaded to the access points. See **Profile Settings** for more information.

RF Optimization

The RF Optimization page displays the configurable Radio Frequency (RF) settings for the access points of the wireless network. Navigate to **Configuration > Profile Settings > [Site] > [Network] > RF Optimization** to view existing settings.



RF Optimization

Adjust Frequency: 6 Hours

□ Auto Channel Adjustment

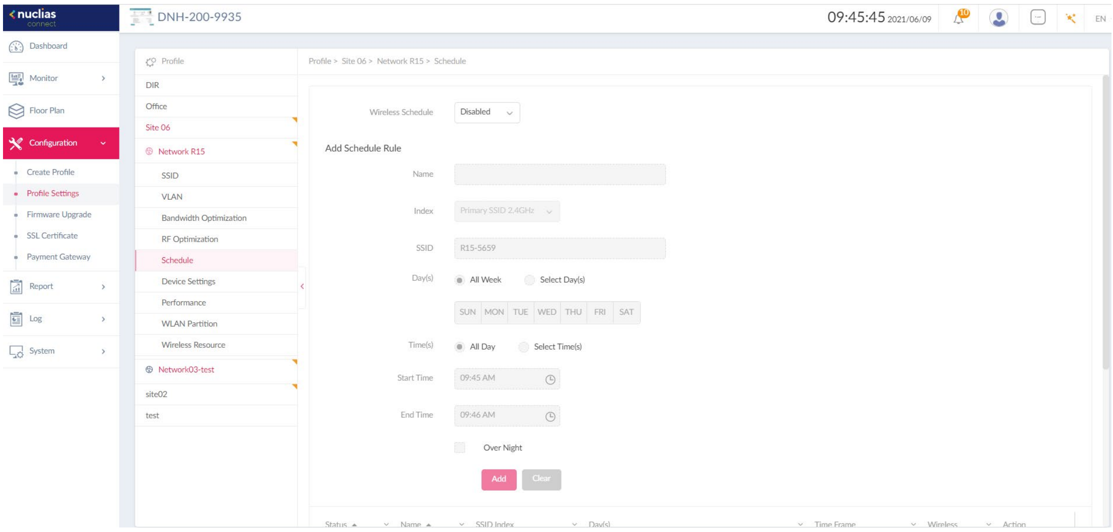
□ Auto Power Adjustment

Adjust Frequency	Set the rate in hours at which the RF frequency is adjusted.
Auto Channel Adjustment	Enable the function to automatically adjust the channel of the client to avoid RF interference.
Auto Power Adjustment	Available if Auto Channel Adjustment is enabled. Enable the feature to automatically adjust AP radio power to optimize coverage when interference is present.

Click **Save** to save the values and update the screen.
Once the settings are updated, the configuration must be uploaded to the access points. See **Profile Settings** for more information.

Schedule

The Schedule page displays the wireless schedule settings. It can be used to enable wireless network in a defined set of schedules. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Schedule** to view existing settings.



Wireless Schedule: Disabled

Add Schedule Rule

Name:

Index: Primary SSID 2.4GHz

SSID: R15-5659

Day(s): ● All Week ○ Select Day(s)

Time(s): ● All Day ○ Select Time(s)

Start Time: 09:45 AM

End Time: 09:46 AM

□ Over Night

Wireless Schedule	Enable or disable the wireless schedule function.
Name	Enter a name for the schedule.
Index	Select the SSID on which the schedule setting will be applied.
SSID	Displays the SSID name.
Day(s)	Select the active days for the schedule. ● All Week: Enable the rule for the whole week. ● Select Day(s): Specify particular day(s) for availability of the wireless network.
Time(s)	Select the active times of the day for the schedule. ● All Day: Enable the rule for the whole day. ● Select Time(s): Specifies a start and end time for availability of the wireless network.
Start Time	If **Select Time(s)** is selected, enter the hours and minutes of the day.
End Time	If **Select Time(s)** is selected, enter the hours and minutes of the day.
Over Night	Check the box to enable overnight activity for the time period with Start Time later than the End Time.
Add	Click **Add** to add the rule into the schedule.
Clear	Click **Clear** to clear the entered rule.

Click ✎ to modify a rule or 🗑 to delete a schedule.

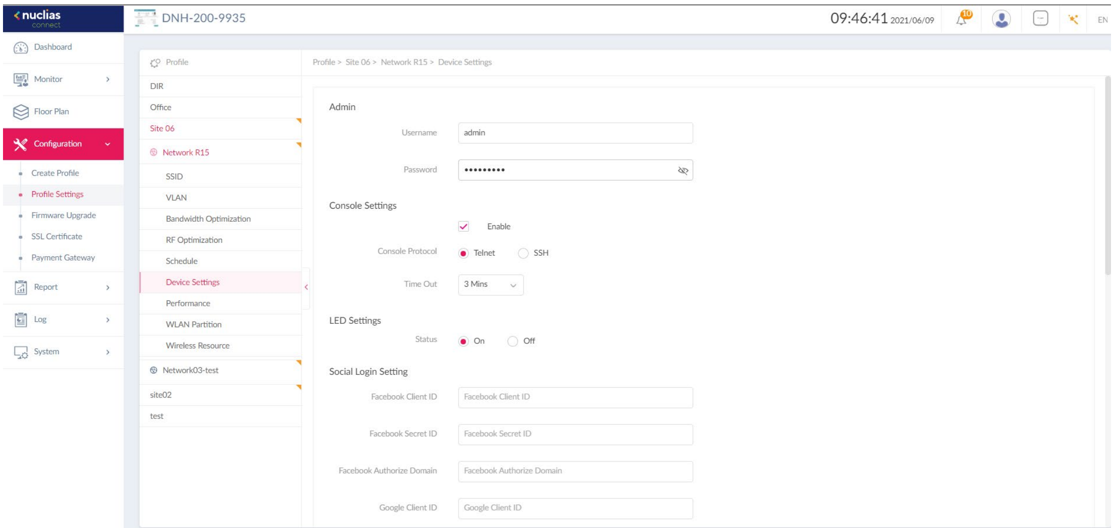
Once the settings are updated, the configuration must be uploaded to the access points. See

Profile Settings for more information.

Device Settings

The Device Settings page allows you to view and configure the login and accessibility settings for access points in this network.

Navigate to **Configuration > Profile Settings > [Site] > [Network] > Device Setting** to view existing settings.



Profile > Site 06 > Network R15 > Device Settings

Admin

Username: admin

Password: •••••••••

Console Settings

☑ Enable

Console Protocol: ● Telnet ○ SSH

Time Out: 3 Mins

LED Settings

Status: ● On ○ Off

Social Login Setting

Facebook Client ID: Facebook Client ID

Facebook Secret ID: Facebook Secret ID

Facebook Authorize Domain: Facebook Authorize Domain

Google Client ID: Google Client ID

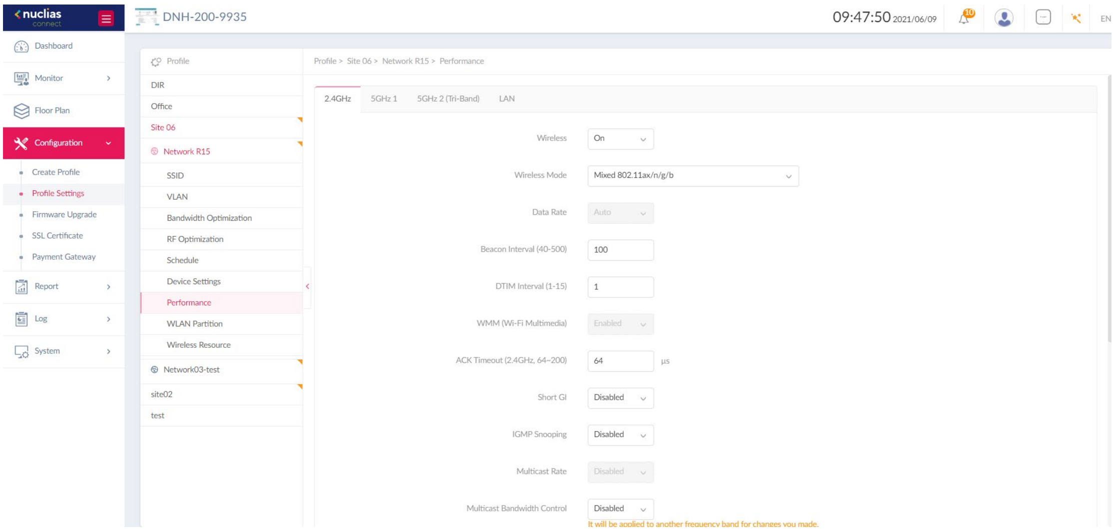
Username	Enter the administrative username that is used to access configuration settings for all access points on the network. Do not use special characters such as %, !, and #.
Password	Enter the administrative password that is used to access configuration settings for all access points on the network. The password must be 8-30 characters and contain both lowercase or uppercase alphabetic characters and numbers.
Console Settings	
Enable	Check the box to enable the console function.
Console Protocol	Select the console protocol that is applied to all access points on the network: Telnet or SSH.
Time Out	Select the active console session time-out value in minutes.
LED Settings	
Status	Turns LED indicator on or off.
Social Login Setting Refer to **Profile Settings > SSID** for **User Authentication** using social login.	
Facebook Client/Secret ID	If using Facebook Sign-in method, enter the client and secret ID.

Facebook Authorize Domain	If using Facebook Sign-in method, enter the authorization domain name.
Google Client ID/Secret ID	If using Google Sign-in method, enter the client and secret ID.
Google Authorize Domain	If using Google Sign-in method, enter the authorization domain name.
Automatic Time Configuration	
Enable NTP Server	Check the box to enable the Network Time Protocol (NTP) for automatic time synchronization.
NTP Server	Enter the IP address or domain name of the NTP server.
Country Settings	
Select Country	Select the country region of APs on the network.
Time Zone	Select the time zone.
Enable Daylight Saving	Check the box to enable daylight saving in your time zone.
DST Start (24HR)	Specify the start date and time for Daylight Saving Time (DST).
DST End (24HR)	Specify the end date and timefor Daylight Saving Time (DST).
DST Offset (minutes)	Specify DST Offset time.
External Syslog Server Settings	
External Syslog Server (Captive Portal Log)	Enter the IP address or domain name of the external syslog server.

Click **Save** to save the values and update the screen.
Once the settings are updated, the configuration must be uploaded to the access points. See **Profile Settings** for more information.

Performance

The Performance page allows you to configure the wireless performance for access points on your network. Advanced wireless settings can be configured on the page for individual 2.4GHz and 5GHz frequency bands. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Performance** to view existing settings.



Profile > Site 06 > Network R15 > Performance

Wireless: On

Wireless Mode: Mixed 802.11ax/n/g/b

Data Rate: Auto

Beacon Interval (40-500): 100

DTIM Interval (1-15): 1

WMM (Wi-Fi Multimedia): Enabled

ACK Timeout (2.4GHz, 64~200): 64 μs

Short GI: Disabled

IGMP Snooping: Disabled

Multicast Rate: Disabled

Multicast Bandwidth Control: Disabled

It will be applied to another frequency band for changes you made.

Wireless	Turn on or off the wireless band forthe network.
Wireless Mode	Select the wireless mode used for the network. For 5GHz, Mixed 802.11n/a, 802.11a Only, 802.11n Only, and Mixed 802.11ax/ac/n/a are available. For 2.4GHz, Mixed 802.11ax/n/g/b, Mixed 802.11g/b, and 802.11n Only.
Data Rate	Select the wireless data rate.
Beacon Interval	Enter the beacon interval value. The default value is 100.
DTIM Interval (1-15)	Enter the Delivery Traffic Indication Message (DTIM) interval value. The default value is 1.
WMM (Wi-Fi Multimedia)	Enable or disable Wi-Fi Multimedia.
ACK Timeout (64~200)	Enter the ACK timeout value. The default value is 64 microseconds.
Short GI	Enable or disable short GI.
IGMP Snooping	Enable or disable the IGMP snooping
Multicast Rate	Select the multicast rate value.
Multicast Bandwidth Control	Enable or disable bandwidth limit for multicast. This setting will be automatically applied to other band frequencies.
Maximum Multicast Bandwidth	If the **Multicast Bandwidth Control** is **Enabled**, enter the maximum multicast bandwidth value. The default value is 100 kbps.
HT20/40 Coexistence	Enable or disable the HT20/40 coexistence function.
Change DHCPOFFER from Broadcast to Unicast	Enable or disable the change of packet type of DHCP offering to unicast. This setting will be automatically

	applied to other band frequencies.
RTS Length (256-2346)	Enter the RTS length value. The default value is 2346.
Fragment Length (256-2346)	Enter the fragment length value. The default value is 2346.
Channel Width	Select the channel width used by the network. For 5GHz, 20MHz, Auto 20/40 MHz, and Auto 20/40/80/160 MHz are available. For 2.4GHz, 20 MHz and Auto 20/40 MHz are available.

LAN

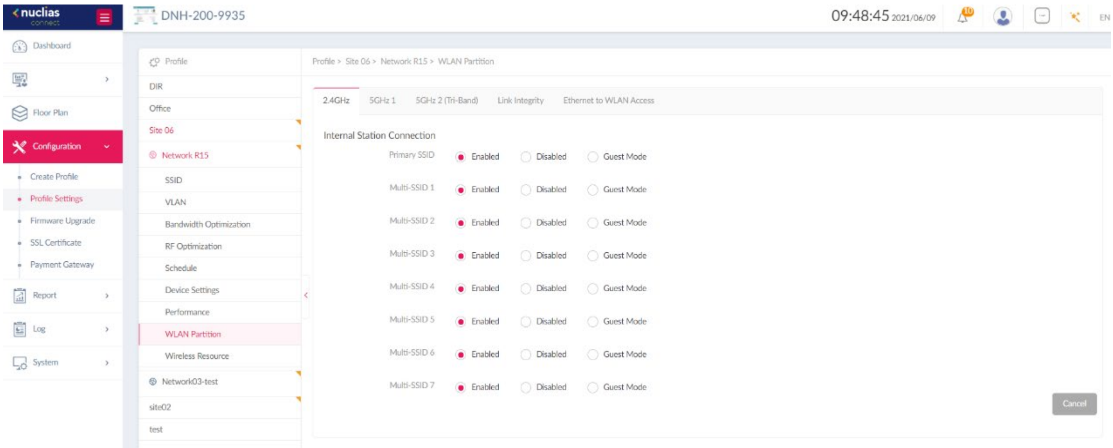
On the LAN tab, you can configure STP (Spanning Tree Protocol). The Spanning Tree Protocol eliminates loops caused by redundant paths.

STP (Spanning tree): Enable this function for access points having multi-LAN ports.

Once the settings are updated, the configuration must be uploaded to the access points. See Profile Settings for more information.

WLAN Partition

The WLAN Partition page displays the wireless partitioning settings that allows you to enable or disable communication among clients within the same SSID or across different SSIDs. Advanced wireless settings can also be configured based on the 2.4GHz or 5GHz frequency band. Navigate to **Configuration > Profile Settings > [Site] > [Network] > WLAN Partition**.



Internal Station Connection

Primary SSID ● Enabled ○ Disabled ○ Guest Mode

Multi-SSID 1 ● Enabled ○ Disabled ○ Guest Mode

Multi-SSID 2 ● Enabled ○ Disabled ○ Guest Mode

Multi-SSID 3 ● Enabled ○ Disabled ○ Guest Mode

Multi-SSID 4 ● Enabled ○ Disabled ○ Guest Mode

Multi-SSID 5 ● Enabled ○ Disabled ○ Guest Mode

Multi-SSID 6 ● Enabled ○ Disabled ○ Guest Mode

Multi-SSID 7 ● Enabled ○ Disabled ○ Guest Mode

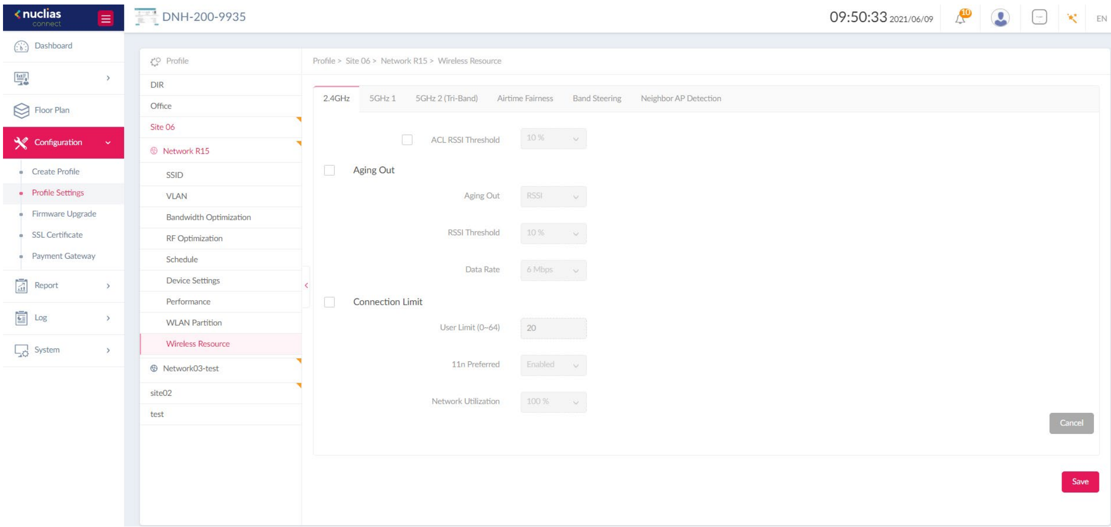
Internal Station Connection	Select **Enable** to permit within-SSID and across-SSID communication. Select **Disable** to prevent within-SSID but permit across-SSID communication. Select **Guest Mode** to prevent within-SSID and across-SSID communication.

Link Integrity	Go to this tab. Click the drop-down menu to enable or disable wireless link integrity. Enable this to disable the wireless network if the AP is not connected with an uplink router.
Ethernet to WLAN Access	Enable or disable Ethernet to WLAN access. If disabled, packets from the Ethernet port(s) could not be forwarded to the Wireless network.

Once the settings are updated, the configuration must be uploaded to the access points. See **Profile Settings** for more information.

Wireless Resource

The Wireless Resource function provides real-time RF management of the wireless network. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Wireless Resource**.



□ ACL RSSI Threshold 10 %
□ Aging Out
Aging Out RSSI
RSSI Threshold 10 %
Data Rate 6 Mbps
□ Connection Limit
User Limit (0~64) 20
11n Preferred Enabled
Network Utilization 100 %

ACL RSSI Threshold	Check the box to enable ACL Received Signal Strength Indicator (RSSI) threshold function and click the menu to select the ACL RSSI threshold percentage.
Aging Out	Select criteria to disconnect wireless clients. Available options are RSSI and Data Rate.
RSSI Threshold	When **RSSI** is selected for Aging out, select a value between 10% and 100%. This parameter sets the minimumRSSI for wireless clients to respond to a probe. If the RSSI of a wireless client is lower than the specified percentage, the wireless client isdisconnected.
Data Rate	Select the data rate in Mbps for connection limit. The option is only available when the **Aging Out** policy is set to **Data Rate**. When the data rate of wireless clients is lower than the specified number, the Hub disconnects the wireless clients.
Connection Limit	Enable or disable the limit on wireless connectivity based on the

	number of clients and bandwidth usage.
User Limit (0~64)	Enter the user connection limit. The default value is 20. When the number of users exceeds this value, no further client association will be allowed.
11n Preferred	Enable or disable the useof 802.11n as the preferred standard. The wireless clients using 802.11n will have higher priority to connect to the device.
Network Utilization	Select the network utilization percentage. When the network utilization exceeds the specified percentage, no further client association will be allowed.

Click **Save** to save the values and update the screen.

Once the settings are updated, the configuration must be uploaded to the access points. See Profile Settings for more information.

Airtime Fairness

Airtime Fairness allows you to boost overall network performance. This function sacrifices network time from the slowest devices to boost overall performance of the network. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Wireless Resource**. Then click the **Airtime Fairness** tab to view the existing settings.

Note: Devices identified as having slow Wi-Fi speed can be slow because of long physical distance from the AP, weak signal strength or legacy hardware.

Check the box to enable or disable the airtime fairness function.Click **Save** to save the values and update the screen.

Once the settings are updated, the configuration must be uploaded to the access points. See **Profile Settings** for more information.

Band Steering

Band Steering technology steers clients capable of both 2.4 GHz and 5GHz frequencies to connect to the less crowded 5GHz network and leave the 2.4GHz network for those clients who support only 2.4GHz. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Wireless Resource**. Click the **Band Steering** tab to view the existing settings.

Click **Save** to save the values and update the screen.

Neighbor AP Detection

Neighboring APs as well as wireless clients can be detected by scanning the radio frequencies. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Wireless Resource**. Then click the **Neighbor AP Detection** tab to view the existing settings.
To view all detected APs, go to **Monitor > Neighbor AP**. From this page, you can see SSID, security, and channel as well as signal strength of the AP neighborhood. This function is useful if you want to verify the wireless coverage meets your floor plan with the information of the neighboring APs and their signal strength. It can also help detect potentially rogue access points in your site to prevent threats and attacks.

Click **Save** to save the values and update the screen.

Firmware Upgrade

The Firmware Upgrade function allows users to perform firmware upgrade. This is a useful feature that prevents future bugs and allows for new features to be added onto your device. Please go to your local D-Link website to see if there is a newer firmware available.
Navigate to **Configuration > Firmware Upgrade** and click **[Site] > [Network]** and configure the following for the selected wireless network.

Online Check Upgrade Firmware	On this tab, you can click **Check for Update** to obtain firmware files online immediately.
Manual Upgrade Firmware	On this tab, you can upload the firmware files to the firmware list area.
Time Start	Select a desired date and time in the future to perform firmware upgrade or update the firmware immediately.

In the **Run Status** section, the firmware update results are displayed.
Click **Apply** to save the changes and for them to take effect.
The **Run Status** area below will display the firmware upgrade results.

SSL Certificate

The SSL Certificate page allows you to install an SSL certificate to secure connections to the AP’s web management interface. The intermediate certificate is used to establish the trust by binding it to the Certificate Authority’s root certificate.

In the **Update SSL Certificate** section, configure the following to import a certificate:

Upload Certificate From File	Click **Browse** to upload and import the certificate from your local drive.
Upload Key From File	Upload the key used with the certificate.

Please reboot your APs after you upload the certificate. The upload status and results will be displayed in Run Status area.

Payment Gateway

The payment gateway allows e-commerce services for network access. The Payment Gateway page shows payment settings and options necessary to enable payment services for network access. It facilitates the **PayPal** service to be used for billing. Navigate to **Configuration > Payment Gateway**. To configure network authentication with payment services, go to **Profile Settings > SSID > Hotspot 2.0**.

Configure the following for payment services:

PayPal Currency	Select the currency code forthe PayPal account.
PayPal Client ID	Enter the username for the PayPal account.
PayPal Secret	Enter the password for the PayPal account.
Options	Enter the duration time in minutes, hours, or days as well as the associated cost for the entry.

Click **Save** to save the values and update the screen.

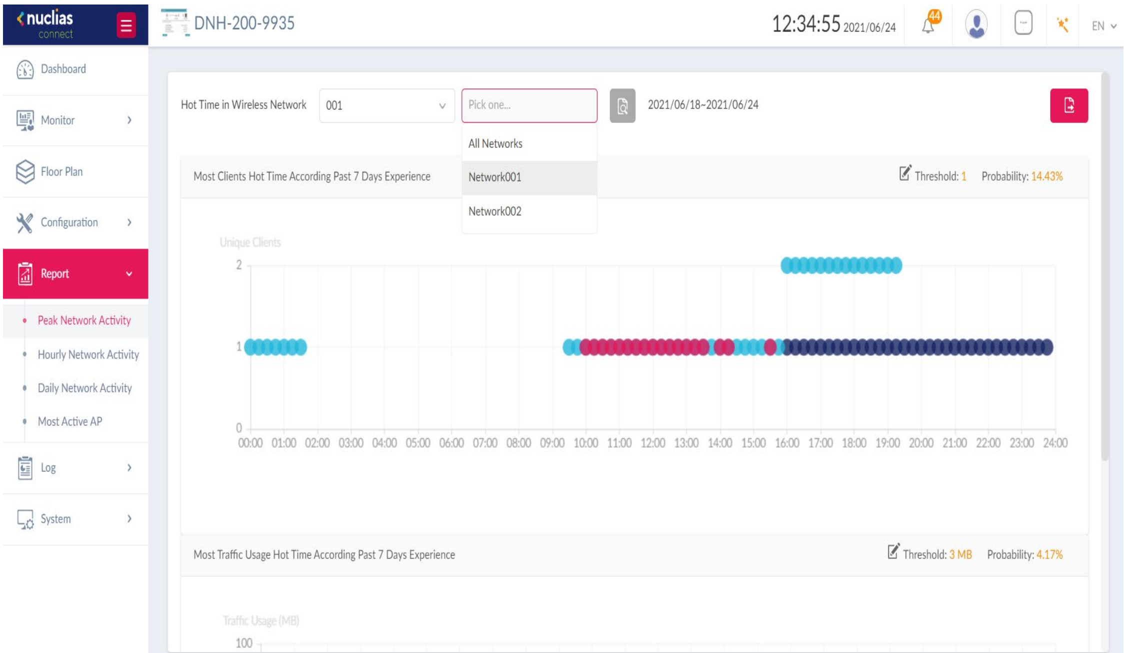
Report

Peak Network Activity

The Peak Network Activity page allows administrators to monitor wireless traffic and gain information about peak usage. Wireless activity for all or selected sites and networks shows the highest number of connected clients and amount of traffic with respect to the hour of a selected day for the past 7 days. Navigate to **Report > Peak Network Activity** to view the information.

To generate a network activity report with peak usage, select the site and network from the corresponding menu and click to viewthe report.

Once a report has been generated, click to export it as a pdf file.



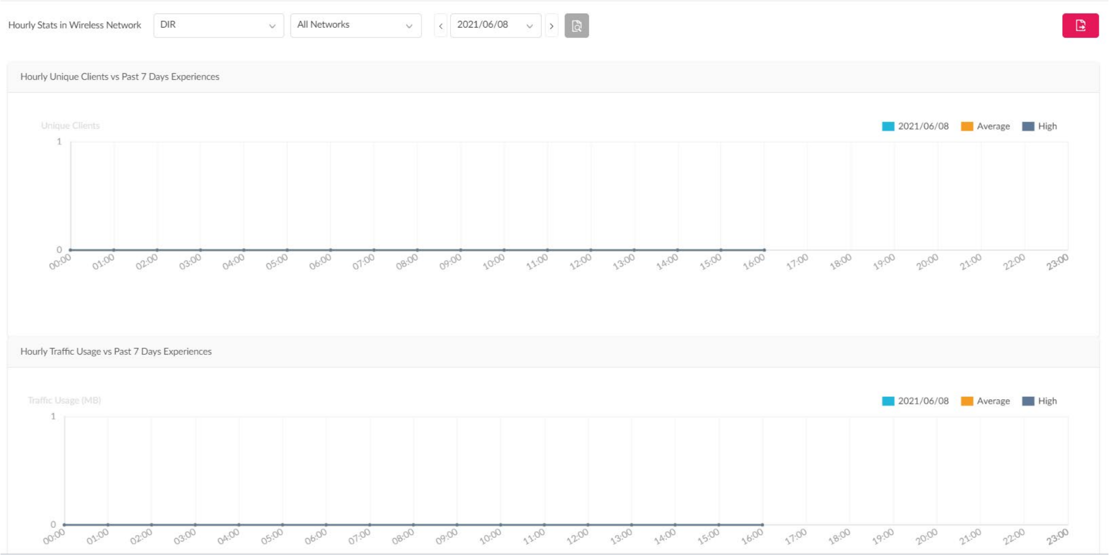
Hourly Network Activity

The Hourly Network Activity page allows administrators to obtain wireless traffic based on the hours of a day for the past 7 days. Wireless activity for all or specific sites and networks shows the number of clients and the amount of traffic (average and highest) with respect to the hour of a selected day.

Navigate to **Report > Hourly Network Activity** to view the report.

To generate an hourly report, select the site and network from the corresponding menu, and select a day from the past 7 days, then click to view the report.

Once a report has been generated, lick to export it as a pdf file.



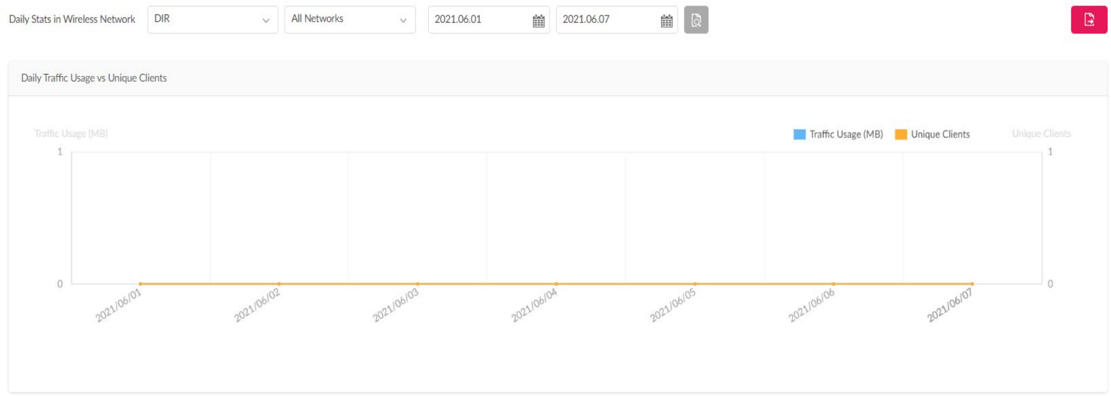
Daily Network Activity

The Daily Network Activity page allows administrators to gain information about wireless traffic each day for the past 7 days. Wireless activity shows the amount of traffic every day for the past 7 days.

Navigate to **Report > Daily Network Activity** to generate and view the report.

To display traffic usage, select a site and network, and specify the start and end dates for your search. Then click to view the report.

Once a report has been generated, click to export it as a pdf file.



Most Active AP

The Most Active AP page displays a visual representation of the wireless network traffic with the location of the access points.

To add a new map representation:

1. Click **+** to open the **Create Map of Most Active APs** window. Enter a name in the **Map Name** field.
2. Upload the location map by dragging and dropping an image (supported image formats: PNG and JPG; max. size: 10M) or browsing your local folder to select an image.
3. Click the **Select AP** menu to select an AP from the list of available APs. Drag the AP to place it on the right spot.
4. Click **Save** to save your changes and update the settings on the screen.

Available maps can be edited or deleted by clicking ✎ or 🗑.

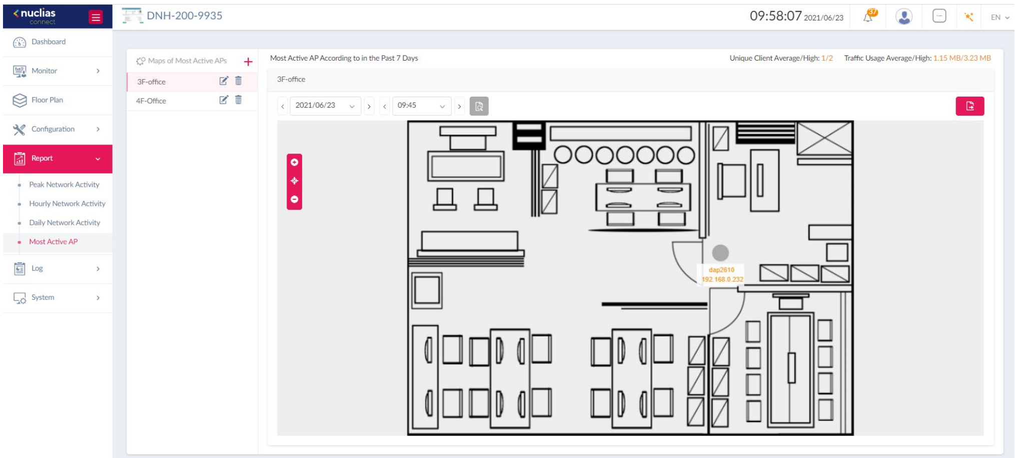
Mouse-over an AP to obtain the following information about it: Device Name, IP Address, MAC Address, Location, Unique Clients, and Traffic Usage.

To view an active map report, select a date and time from the past 7 days, then click 🔍 to view the report.

If an AP on the map is active during the selected time, it will be colored with a number on it indicating the number of connected clients. Different colors represent the high or low amount of traffic. The two numbers in the upper-right corner of the page show the following information:

1. **Unique Client Average/High:** The average number/the highest number of connected clients.
2. **Traffic Usage Average/High:** The average amount/ the highest amount of traffic in MB.

Once a report has been generated, lick 🗎 to export it as a pdf file.



Most Active AP According to in the Past 7 Days

Unique Client Average/High: 1/2

Traffic Usage Average/High: 1.15 MB/3.23 MB

3F-office

2021/06/23

09:45

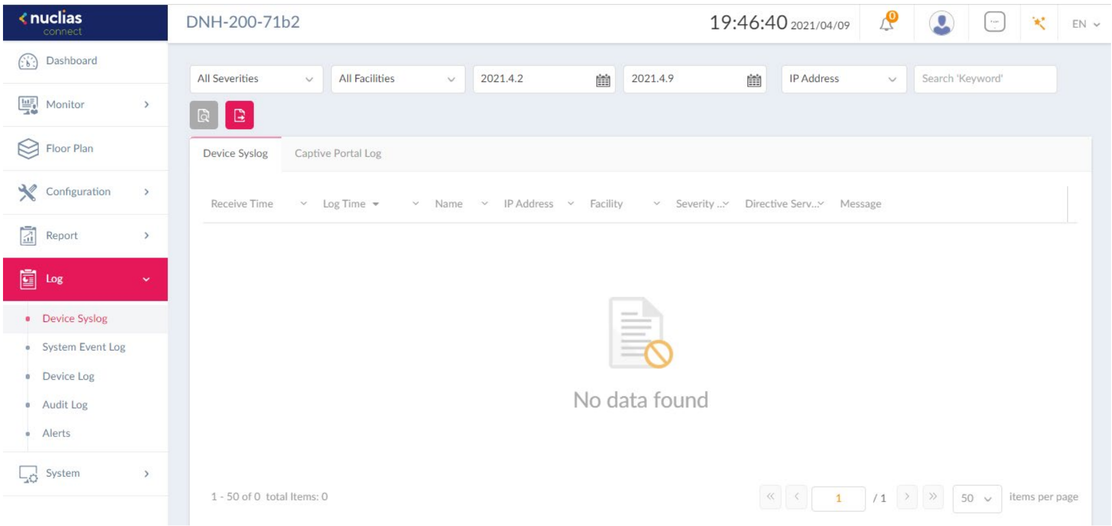
Log

The Log page stores the activities of wireless devices and the log entries are grouped into the following categories: **Device Syslog, System Event Log, Device Log, Audit Log,** and **Alerts**. To navigate among log types, select the respective tab. In each log window, you can apply type-specific filters to see log entries of your interest, for example, IP and MAC address.

Device Syslog

The Syslog function allows administrators to view alert messages for events concerning system operations such as services and daemons running on the system.. Navigate to **Log > Device Syslog** to view the relevant information.

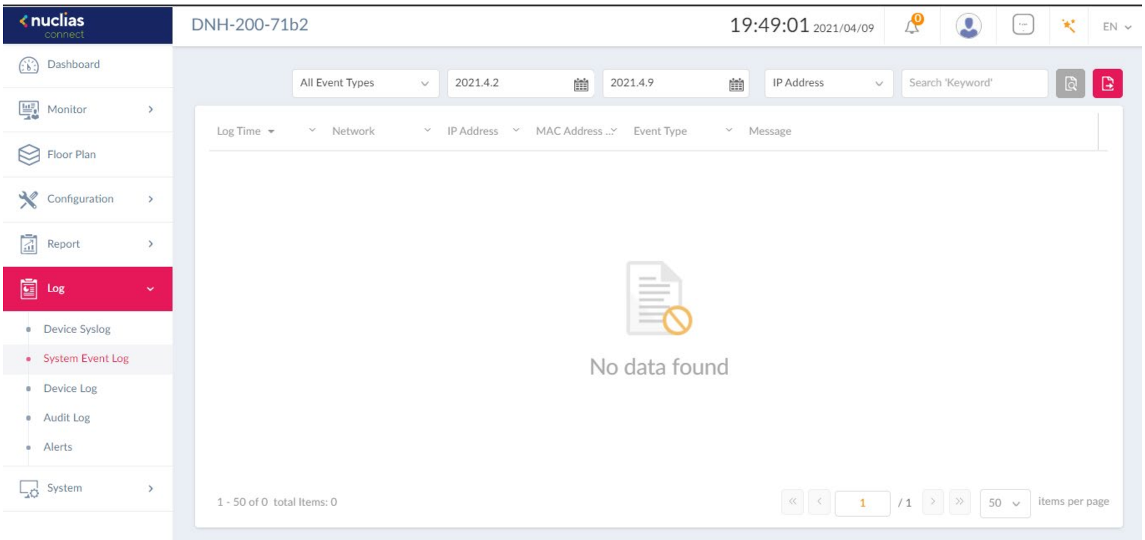
To start a syslog report, select the event severity and facility system/subsystems, define the time period, and choose either IP Address or Message as the filtering criteria. Then enter a keyword and click 🔍 to view the report. Once a report has been generated, click 📤 to export it as a local CSV file. The file will be saved in your browser's download directory and will be named as follows: *Nuclias_Connect_Log Type_YYYY_MMDD_HHMMSS*.



System Event Log

The System Event Log allows administrators to view alerts such as connection requests and events related to device management that may require attention and necessary action to keep smooth operation and to prevent failures. Navigate to **Log > System Event Log** to view relevant information.

To generate a System Event Log report, select an event type, define the time period, and choose either IP address or Message as the filtering criteria. Then enter a keyword to filter the results and click 🔍 to view the report. Once a report has been generated, click 📄 to export it as a local CSV file. The file will be saved in your browser's download directory and will be named as follows: *Nuclias_Connect_Log Type_YYYY_MMDD_HHMMSS*.



DNH-200-71b2 19:49:01 2021/04/09

All Event Types | 2021.4.2 | 2021.4.9 | IP Address | Search 'Keyword'

Log Time	Network	IP Address	MAC Address	Event Type	Message

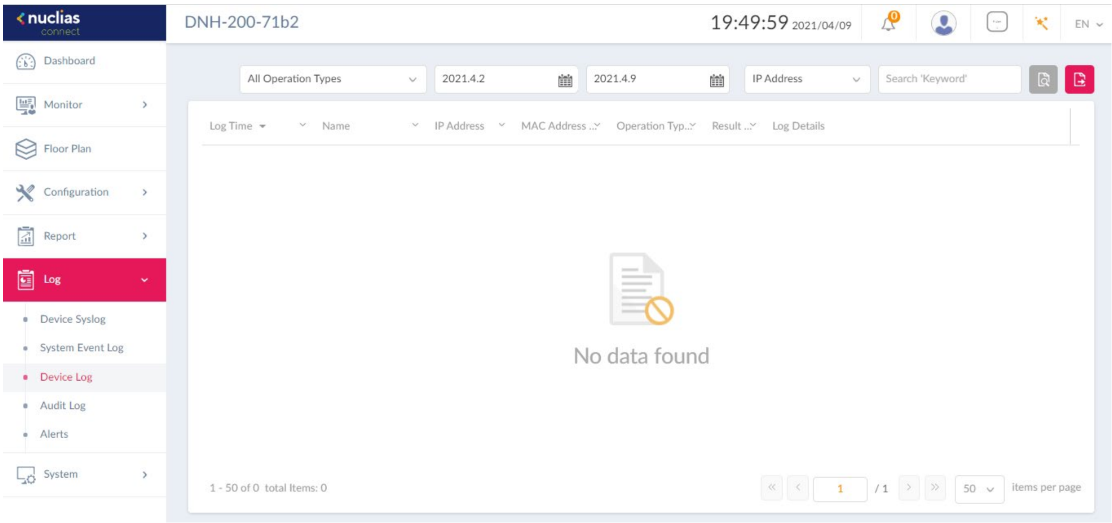
No data found

1 - 50 of 0 total Items: 0 1 / 1 50 items per page

Device Log

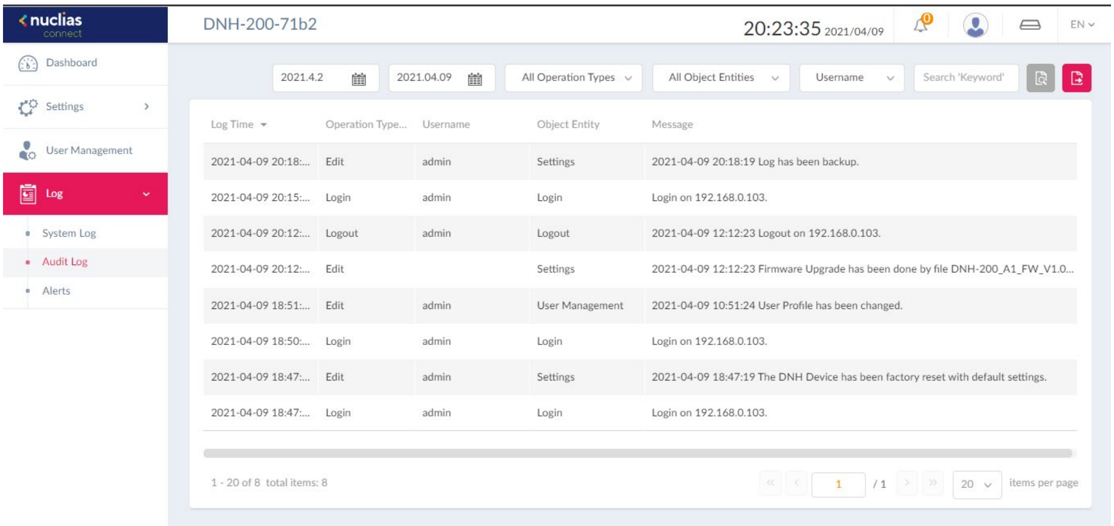
The Device Log allows administrators to view alert messages concerning changes or management tasks performed on the system. The log messages include a time stamp and operation type, e.g., device settings synchronization, firmware upgrade, or configuration upload. Navigate to **Log > Device Log** to obtain such information.

To generate a Device Log report, select an operation type, define the time period, and choose either IP address or Log Details as the filtering criteria. Then enter a keyword to filter the log messages and click 🔍 to display the results. Once a report has been generated, click to export it as a local CSV file. The file will be saved in your browser's download directory and will be named as follows: *Nuclias_Connect_Log Type_YYYY_MMDD_HHMMSS*.



Audit Log

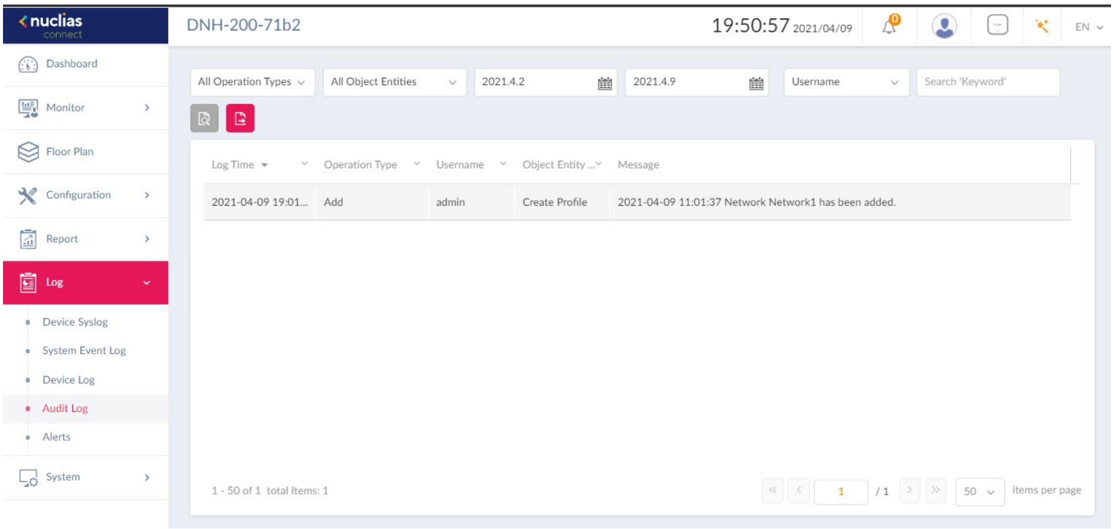
This type of log records user activities that can be performed on an object entity such as profile and network creation or deletion.



Log Time	Operation Type...	Username	Object Entity	Message
2021-04-09 20:18:...	Edit	admin	Settings	2021-04-09 20:18:19 Log has been backup.
2021-04-09 20:15:...	Login	admin	Login	Login on 192.168.0.103.
2021-04-09 20:12:...	Logout	admin	Logout	2021-04-09 12:12:23 Logout on 192.168.0.103.
2021-04-09 20:12:...	Edit		Settings	2021-04-09 12:12:23 Firmware Upgrade has been done by file DNH-200_A1_FW_V1.0...
2021-04-09 18:51:...	Edit	admin	User Management	2021-04-09 10:51:24 User Profile has been changed.
2021-04-09 18:50:...	Login	admin	Login	Login on 192.168.0.103.
2021-04-09 18:47:...	Edit	admin	Settings	2021-04-09 18:47:19 The DNH Device has been factory reset with default settings.
2021-04-09 18:47:...	Login	admin	Login	Login on 192.168.0.103.

To generate an Audit Log report, select the entries by Operation Type (operations that performed on the object entities) and Object Entity (i.e., the objects associated with the functional tabs in the left pane), define the time period, and select Username or Message as the filtering criteria. Then enter a keyword and click to display the search results.

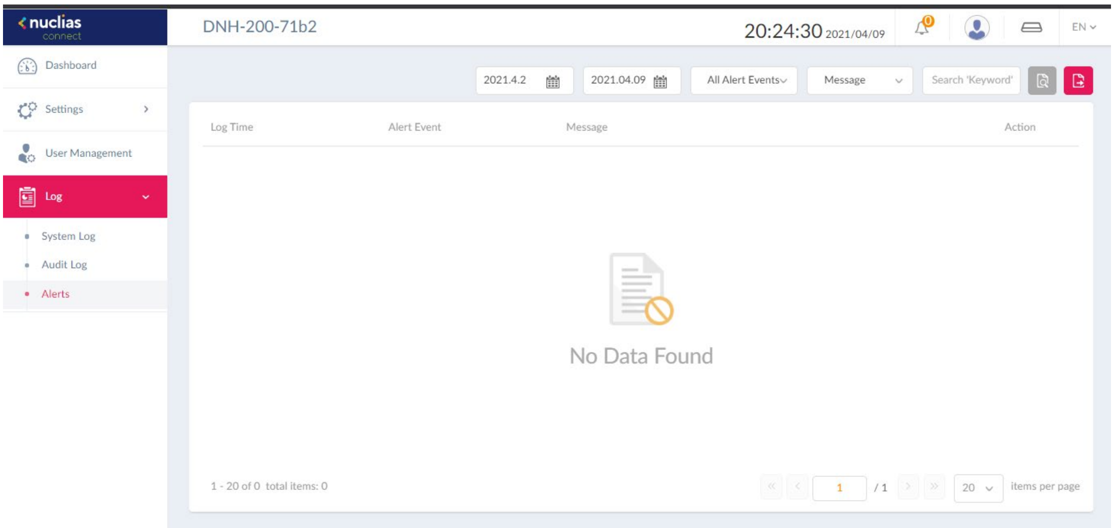
Once a report has been generated, click to export it as a local CSV file. The file will be saved in your browser's download directory and will be named as follows: *Nuclias_Connect_Log Type_YYYY_MMDD_HHMMSS*.



Log Time	Operation Type	Username	Object Entity ...	Message
2021-04-09 19:01...	Add	admin	Create Profile	2021-04-09 11:01:37 Network Network1 has been added.

Alerts

This type of log abnormal or critical events for alert, e.g., firmware update failure, port linked or blocked, and device online or offline.



To generate an Alert report, select the alert events, define the time period, and select IP Address or Message as the filtering criteria. Then enter a keyword and click to display the search results. Once a report has been generated, click to export it as a local CSV file. The file will be saved in your browser's download directory and will be named as follows: *Nuclias_Connect_Log Type_YYYY_MMDD_HHMMSS*.

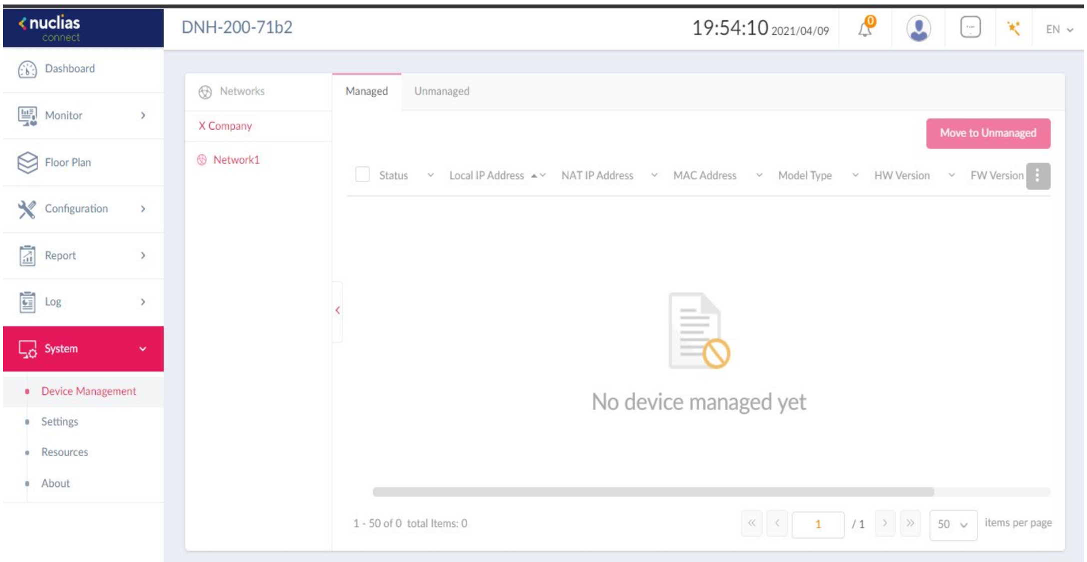
System

Device Management

The Device Management page allows you to view the list of all devices on a selected network for both managed and unmanaged devices. Navigate to **System > Device Management >[Site] > [Network]**. For a selected network, click the managed or unmanaged tab to view devices under each category.

To move devices to **Unmanaged** or the other way, use the **Move** tab in the upper-right corner. You can also click on an entry to launch its web management interface.
To delete a managed AP device, you need to move it to the Unmanaged List first.

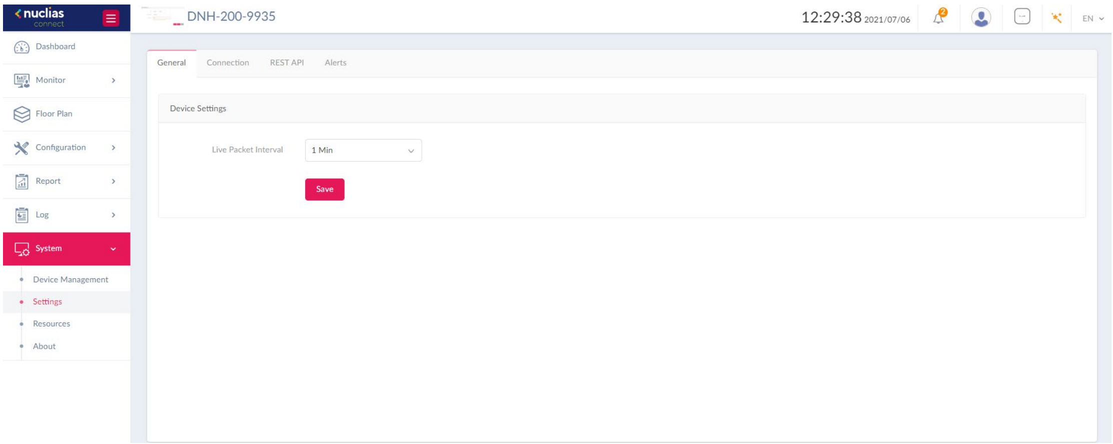
The list provides the following information: **Status, Local IP Address, NAT IP Address, MAC Address, Model Type, HW Version, FW Version, Managed Time,** and **Backup FW Version**. To customize the displayed fields, click ⋮. To order by a field, click the field name at the top of the list. To reverse the order, click the field name again.



No device managed yet

Settings

The Settings page allows you to configure settings such as access ports of the web management and alert events and contains these tabs: **General**, **Connection, Rest API,** and **Alerts**.



Device Settings

Live Packet Interval: 1 Min

General

The General tab allows you to set the **Live Packet Interval**. Click the menu to select the live packet interval in minutes (range: 1-5 mins). It determines how often the managed APs should report their status and related information to the Hub.

Click **Save** to save the values and update the screen.

Connection

The connection tab provides connection settings such as the network address and port number for communication. Navigate to **System > Settings** and click the **Connection** tab. The following can be configured for device connection:

Device Access Address	The current IP address of Nuclias Connect Server application is displayed. Click **Other** to modify it. If this IP is changed, you need to perform AP discovery gain.
Device Access Port	Enter the port number for communication between an AP and the Hub. The default value is 8443. For remote AP management behind a firewall or router, use this port information for setting port forwarding.

Click **Save** to save the values and update the screen.

REST API

The API key is required for sending requests about the wireless networks managed by the Hub. Navigate to **System > Settings** and click the **REST API** tab. Configure the following to obtain an API key:

REST API	Enable or disable information requests through REST API.
REST API Key	Click Generate/Regenerate Key to generate an API key to be used for API data request authentication. Then copy this key in your application when initiating sessions with the Hub.

Click **Save** to save the values and update the screen.

Alerts

The Alerts tab allows you to configure the alert event types. Check the types of events that should generate an alert. Navigate to **System > Settings** and click the **Alerts** tab. To view generated alerts**,** go to **Log > Alerts** to view alerts.

Configure whether alerts or email notifications should be generated for the following events:	
Site/Network Events	Firmware Upgraded Failed, Device Has Been Removed From Network, Profile Has Been Changed, and Profile Failed To Be Applied.
Device Events	Device Restarted, Device Offline, Device Online, Port Link Down, and Port Blocked.

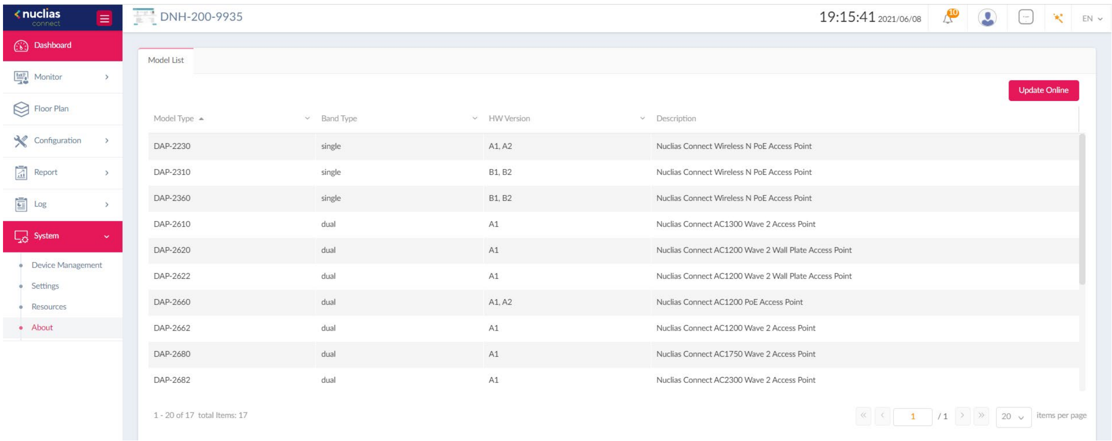
Click **Save** to save the values and update the screen.

Resources

The Resource page allows you to browse the online documents for quick setup, implementation guidelines, and troubleshooting tips. Navigate to **System > Resources.**

About

The About page displays compatible access points that you can manage and monitor on the Hub. Navigate to **System > About**. The list can be updated by clicking **Update Online**.



Model Type	Band Type	HW Version	Description
DAP-2230	single	A1, A2	Nuclias Connect Wireless N PoE Access Point
DAP-2310	single	B1, B2	Nuclias Connect Wireless N PoE Access Point
DAP-2360	single	B1, B2	Nuclias Connect Wireless N PoE Access Point
DAP-2610	dual	A1	Nuclias Connect AC1300 Wave 2 Access Point
DAP-2620	dual	A1	Nuclias Connect AC1200 Wave 2 Wall Plate Access Point
DAP-2622	dual	A1	Nuclias Connect AC1200 Wave 2 Wall Plate Access Point
DAP-2660	dual	A1, A2	Nuclias Connect AC1200 PoE Access Point
DAP-2662	dual	A1	Nuclias Connect AC1200 Wave 2 Access Point
DAP-2680	dual	A1	Nuclias Connect AC1750 Wave 2 Access Point
DAP-2682	dual	A1	Nuclias Connect AC2300 Wave 2 Access Point

1 - 20 of 17 total Items: 17

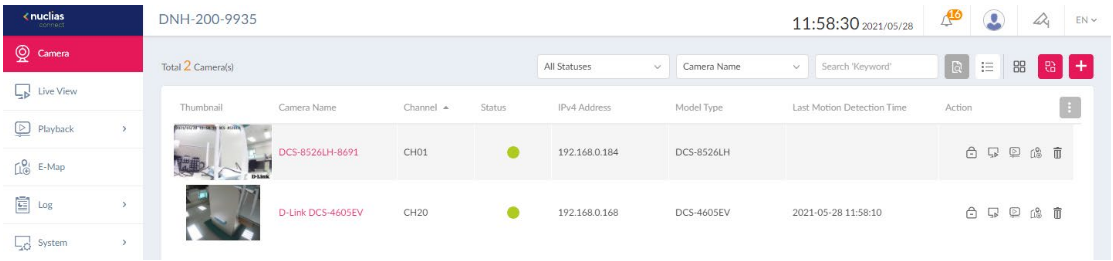
1 / 1 20 items per page

Camera Surveillance

The DNH-200 is also a centralized surveillance platform that manages and monitors supported D-Link network cameras up to a maximum of 20 cameras. Live streams can be recorded and saved locally with the internal hard drive and they can be retrieved with the playback function. This centralized surveillance platform is also capable of instant alert triggered by motion, digital input, or camera disconnection.

Camera

The Camera page shows general information about the connected cameras such as their names and IP addresses.

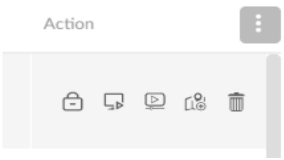


Total 2 Camera(s)

Thumbnail	Camera Name	Channel	Status	IPv4 Address	Model Type	Last Motion Detection Time	Action
	DCS-8526LH-8691	CH01	●	192.168.0.184	DCS-8526LH		
	D-Link DCS-4605EV	CH20	●	192.168.0.168	DCS-4605EV	2021-05-28 11:58:10	

The following table describes the information in detail:

Camera Name	The displayed camera name for identification, which can be modified by clicking on it.
Thumbnail	A snapshot of the camera feed.
Channel	Camera channel number, which can be assigned as well as modified manually.
Status	The operating status of the network camera: online, offline, or authentication failed.
IPv4 Address	The IP address of the network camera in IPv4 addressing scheme.
IPv6 Address	The IP address of the network camera in IPv6 addressing scheme.
MAC Address	The MAC address of the network camera.
Model Type	The model number of the network camera.
FW Version	The firmware version of the network camera.
HW Version	The hardware version of the network camera.

Last Motion Detection Time	The time of the latest motion detected if motion detection is supported by the camera and is enabled in the system.
Action  	It provides a quick link to the following functions: Camera Password, Live View, Playback - Timeline, E-Map, and Delete. Note that the camera password will be modified after being added successfully; it will be reset to its factory default value after being removed from the camera list.
Note: To order a list by a field, click the field name at the top of the column. To reverse the order, click the field name again.	

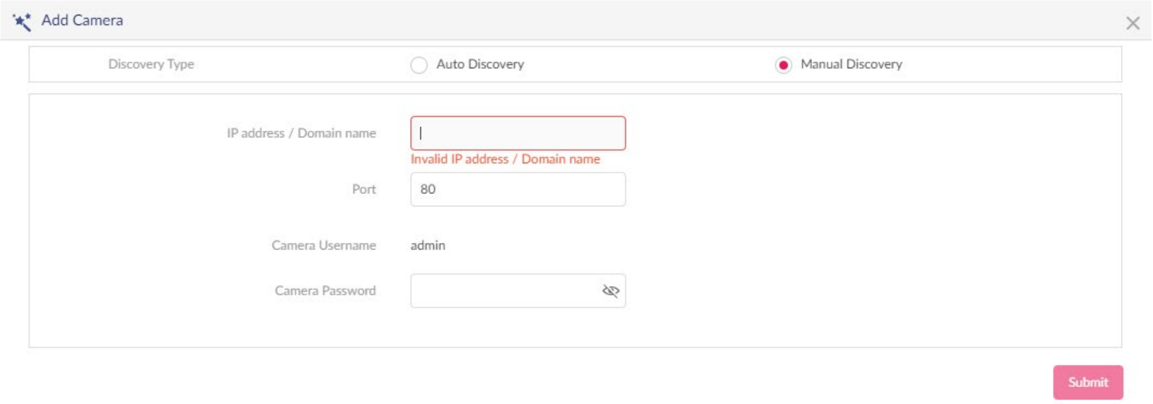
To add a camera to the list, click +. The Add Camera screen appears. You can select **Auto Discovery** to let the system find network cameras in the LAN or **Manual Discovery** to enter camera information manually:

IP address / Domain name: the IP address or domain name of the network camera.

Port: the port number for accessing the web management page. The default is 80.

Camera Username: the username with connection privilege.

Camera Password: the password of the user. Click 👁 to show or hide the input characters.



Add Camera

Discovery Type ○ Auto Discovery ● Manual Discovery

IP address / Domain name: |

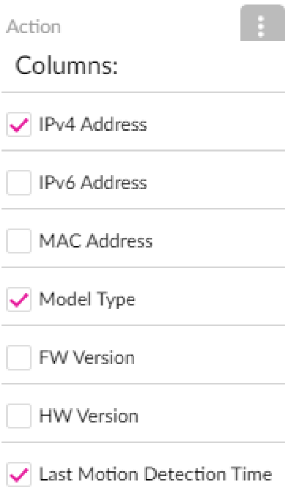
Invalid IP address / Domain name

Port: 80

Camera Username: admin

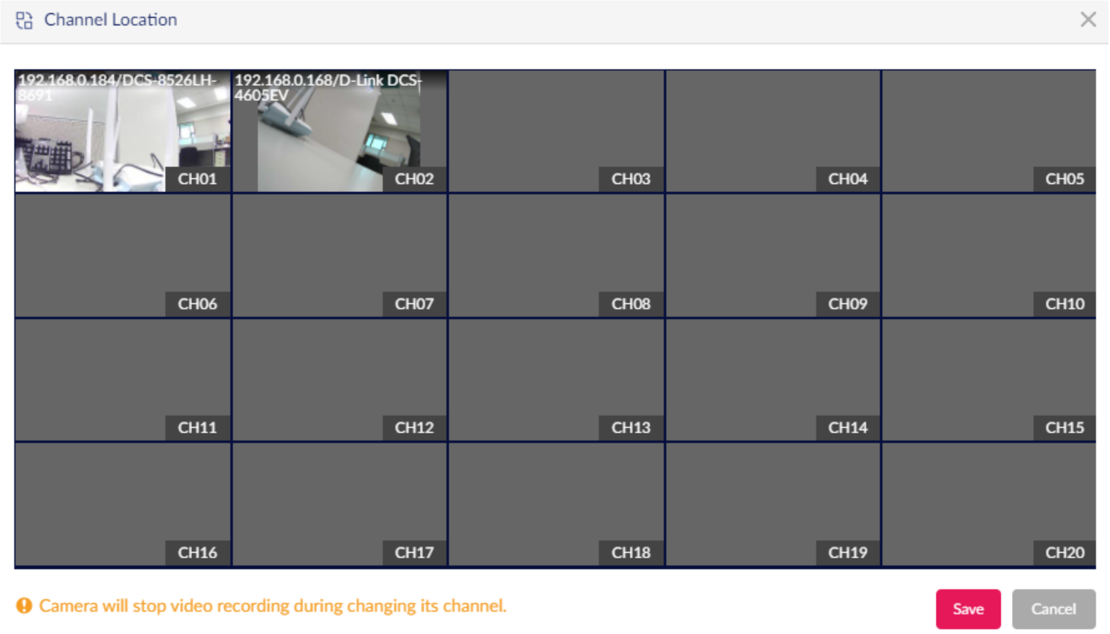
Camera Password:

To customize the fields of camera information, click ⋮ and select the desired properties to display.



☑ IPv4 Address
□ IPv6 Address
□ MAC Address
☑ Model Type
□ FW Version
□ HW Version
☑ Last Motion Detection Time

To assign channel numbers to cameras, click . A screen of available channels appears, and it allows you to drag and drop your camera to the desired slot (channel). Then click **Save** to apply your settings.



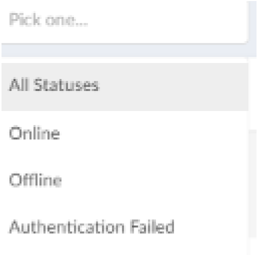
Camera will stop video recording during changing its channel.

Notes:

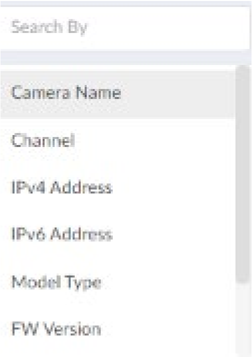
1. A camera will stop video recording during changing its channel.
2. Please verify and reconfigure the settings in System after a camera has been assigned by a different channel. The recording and event settings in **System** is configured based on the channel number and the designated camera will be altered once its channel has been modified.
3. The **Add Camera**, **Delete Camera**, and **Channel Location** functions can only be performed by users with the **Root Admin** or **System Admin** role.

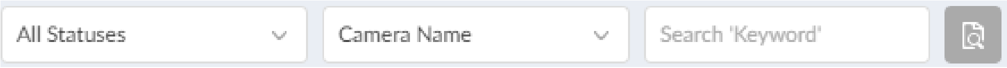
To switch between the list mode and graphic mode of the display of the network cameras, click ☰ and ⊞ respectively.

The search bar at the top of the page can be used to display the cameras of your interest. To show cameras with only certain status, click the **Statuses** menu and select one of these options: **All Statuses**, **Online**, **Offline,** and **Authentication Failed**.



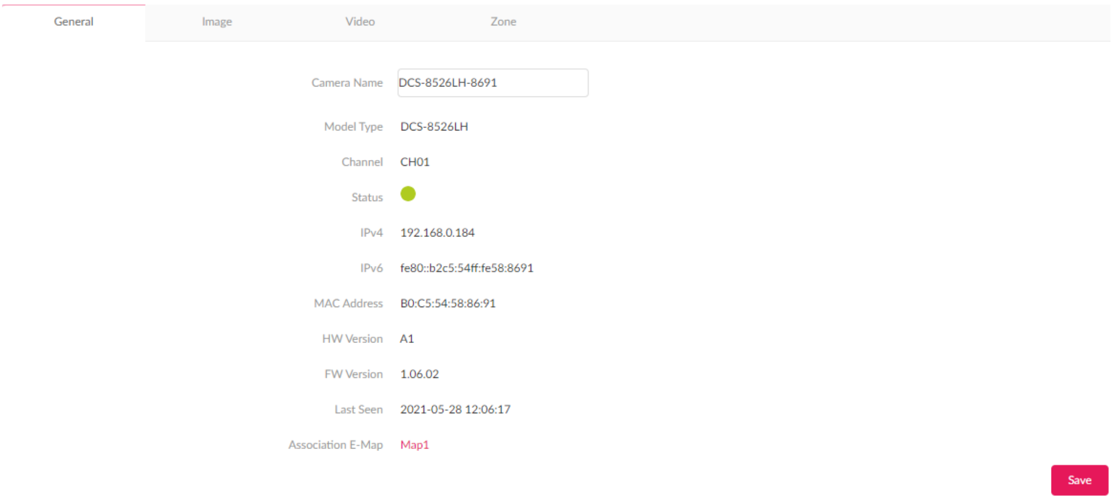
To search cameras by the pre-defined fields, first select one of the pre-defined fields (i.e., Camera Name, Channel, IPv4 Address, IPv6 Address, Model Type, FW Version, HW Version, or MAC Address) and enter a keyword, then click 🔍 to start your search. Note that you can enter only one keyword at a time.





You can perform more operations with the camera by clicking its **Camera Name**. Note that only users with administrative roles can modify the settings of the following camera detail tabs, i.e., **System Admin, Root Admin** and **Local Admin** (for authorized channels only).

General: This tab displays the camera information as shown with the list version but with all available fields. You can also click the Camera Name text field to modify its name.



Camera Name: DCS-8526LH-8691

Model Type: DCS-8526LH

Channel: CH01

Status: ●

IPv4: 192.168.0.184

IPv6: fe80::b2c5:54ff:fe58:8691

MAC Address: B0:C5:54:58:86:91

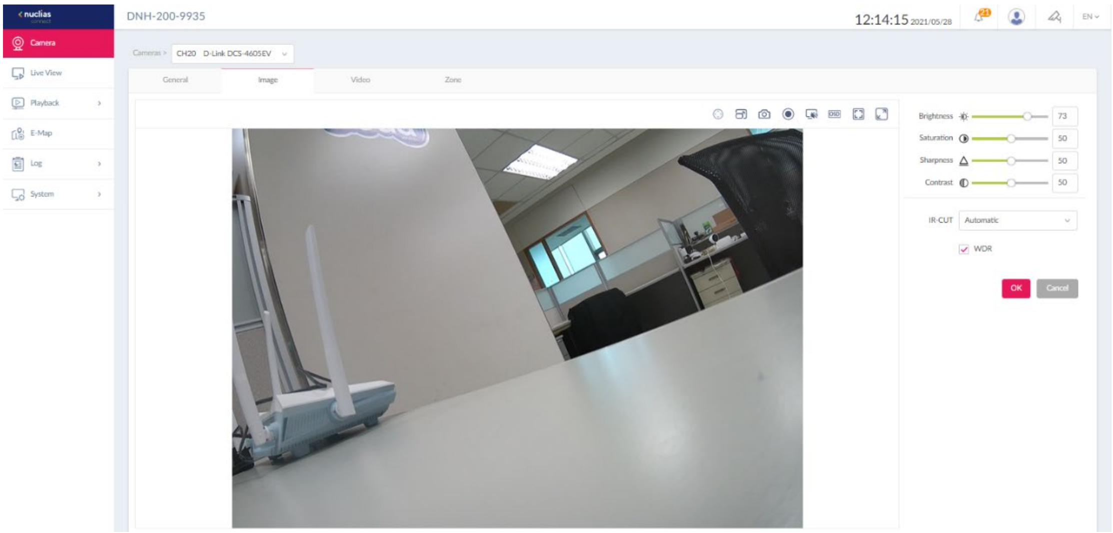
HW Version: A1

FW Version: 1.06.02

Last Seen: 2021-05-28 12:06:17

Association E-Map: Map1

Image: This tab provides live view video and associated actions.



Brightness: 73

Saturation: 50

Sharpness: 50

Contrast: 50

IR-CUT: Automatic

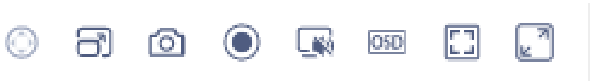
☑ WDR

Use the slider to adjust the image quality with the following settings:

Brightness	Adjust image brightness (value range: 0~100).
Saturation	Adjusts image color saturation. Use the slider to make colors more vivid or duller (value range: 0~100).
Sharpness	Adjusts image sharpness (value range: 0~100).
Contrast	Adjusts the difference in brightness between light and dark areas of the live video. A low-contrast image retains detail whereas a high-contrast image loses detail (value range: 0~100).
IR-CUT	Controls the operation of infrared light (IR) on the network camera. It enhances image brightness during nighttime. When in auto mode, it will be turned on automatically at night and off during the day. Select Automatic for automatic switch between Day Mode and Night Mode depending on the amount of light detected.

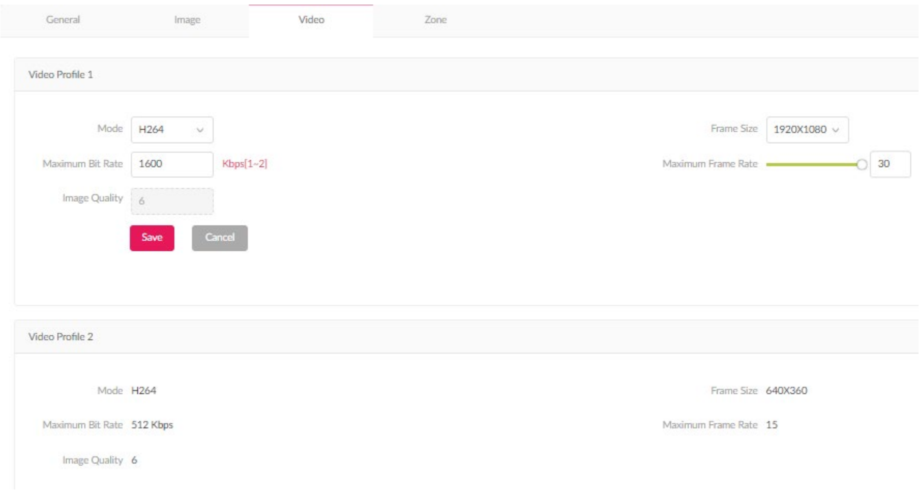
	Select Night Mode to display image in black and white. Select Day Mode to display image in color.
WDR	This technology improves image visibility when both a high brightness area and a relatively low-brightness area exist on the same screen. Turn on this function if such condition exists on the image.
Note: The availability of image settings varies depending on the support of the camera model.	

Mouse over the live view screen for available actions:



PTZ	Control the movement of the camera lens if the camera supports this function. Use onscreen pan, tilt, and zoom control to move the camera’s lens with the desired direction.
Video Quality	Choose different video quality: low or high. The streaming quality can be found by referring to the **Video** tab.
Snapshot	Take a snapshot. The snapshot will be saved in your browser’s download directory in PNG format.
Browser Speaker	Receive sound via the camera’s microphone with the application’s (browser) support.
Manual Recording	Start/Stop recording of the camera’s video. If the camera is currently recording, it will display a red dot in the upper-right corner of the live view window.
OSD (On-Screen Display)	Display selected information on the screen. Refer to **System** > **Display Settings** > **OSD Settings** for more information.
Standard Size	Enable standard or actual size display.
Full Screen	Enable full screen display.

Video: This tab provides video quality settings.



Video Profile 1

Mode: H264

Frame Size: 1920X1080

Maximum Bit Rate: 1600 Kbps[1~2]

Maximum Frame Rate: 30

Image Quality: 6

Video Profile 2

Mode: H264

Frame Size: 640X360

Maximum Bit Rate: 512 Kbps

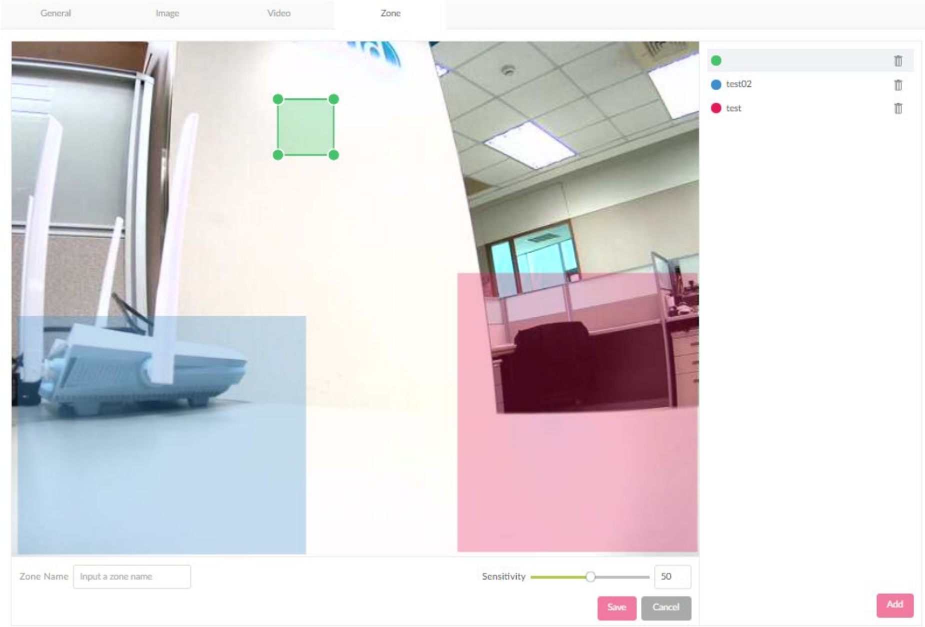
Maximum Frame Rate: 15

Image Quality: 6

You can also modify the streaming settings here: **Mode** (H.265 as the most advanced and efficient codec), **Maximum Bit Rate**, **Image Quality** (range: 1 to 100), **Frame Size** (the resolution offered by the camera), and **Maximum Frame Rate** (range: 1 to 30).

Note: The available values for Video Profile parameters depend on the camera's specifications, e.g, Max. Frame rate@Resolution and the codecs. However, experiment and adjust the above settings based on your streaming quality requirements and traffic conditions. The higher the streaming quality, the more bandwidth will be consumed. The streaming parameters of Video Profile 2 are fixed at 640x 360@15FPS, 512Kbits/sec.

Zone: Zones are areas that can be set for motion detection. They are useful for detecting people and moving objects.



Zone Name: Input a zone name

Sensitivity: 50

Drag to define a zone for motion detection. Different zones can be defined with different sensitivity (the maximum number of zones varies by camera model). To define a window-type detection zone (cell-type zone is also supported depending on camera model):

1. Click **Add**. A square appears in the preview window.
2. Enter a name in the **Zone Name** text box for this zone.
3. Adjust the size of the square by dragging its corners. The squares can be overlapped to accommodate irregular shapes.
4. Configure **Sensitivity**: 0 (not sensitive to motion) the lowest and 100 the highest. The higher the sensitivity, the more sensitive the camera is to movements. Lower sensitivity would require larger moving objects or bigger movements covering larger regions in the defined zone to trigger an alert.
5. Click **Save** to apply your settings.

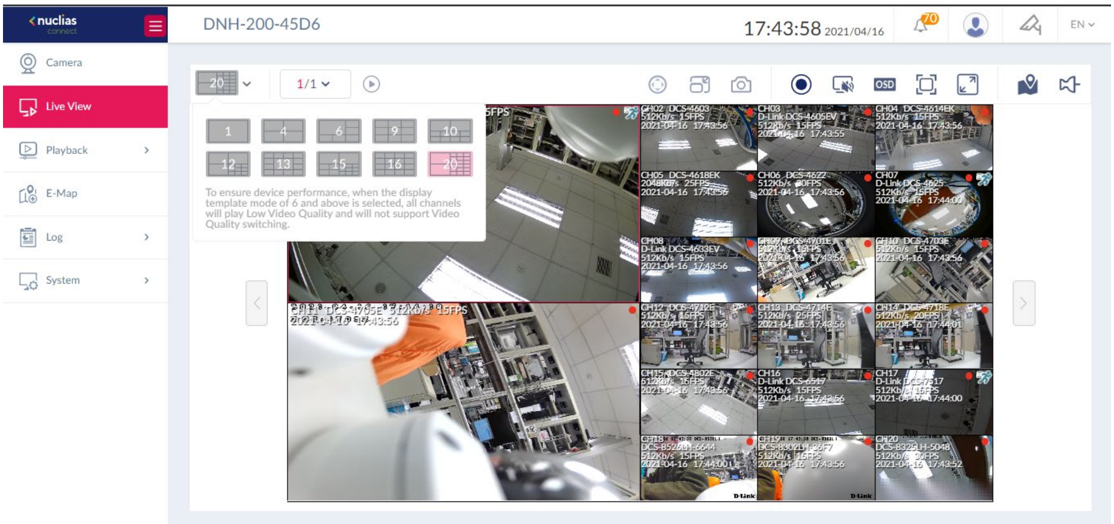
After the zones have been set, whenever there is a movement in the camera, a person with running posture will be displayed on the live video.

Notes:

1. To enable motion detection, at least one zone has to be set.
2. Motion Detection is only available on cameras that support this function through ONVIF protocol. Please refer to the camera's specifications for details.

Live View

This screen displays the live videos of all cameras connected to the DNH-200.


nuclias connect
DNH-200-45D6
17:43:58 2021/04/16
EN
Camera
Live View
Playback
E-Map
Log
System
20
1/1
1
4
6
9
10
12
13
15
16
20
To ensure device performance, when the display template mode of 6 and above is selected, all channels will play Low Video Quality and will not support Video Quality switching.

You can select your desired channel layout by selecting the layout menu 4 in the upper-left corner. If the grid does not accommodate all channels in one screen, select 1/2 to switch among screens. You can also enable automatic swapping among the screens by clicking **Auto Scan** ▶ to the right.

To arrange channel display, drag and drop the selected camera on one of the channels on the grid. To fix a channel on the grid, click in the upper-right corner of the Action toolbar.

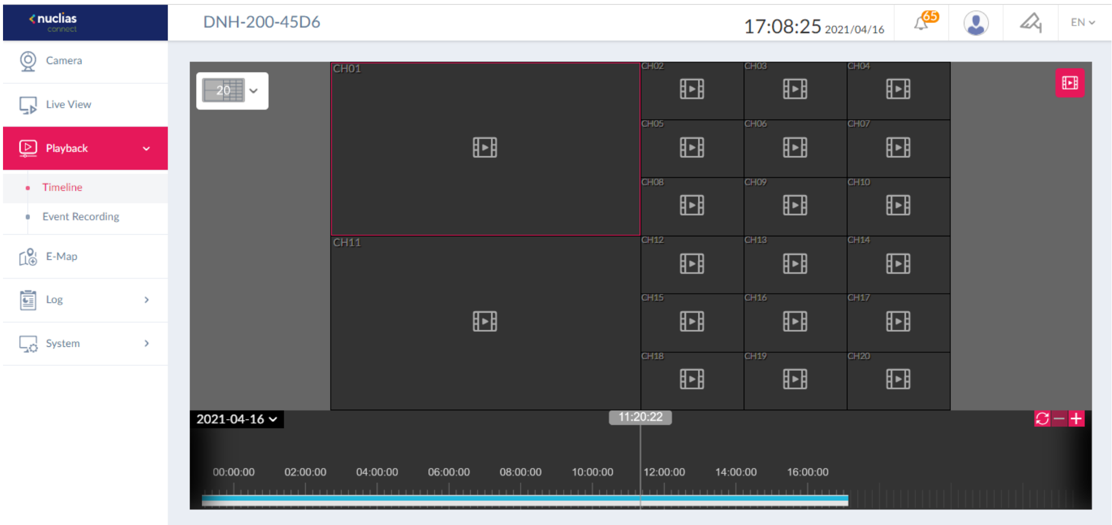
The following table describes the functions that can be performed on the selected channel on the grid.

PTZ	Control the movement of the camera lens if the camera supports this function.
Video Quality	Choose low or high video resolution (the exact resolutions vary by the camera's specifications). Refer to **Video Profile** settings in the **Camera** tab.
Snapshot	Take a snapshot. It will be saved as a JPG file in your browser's download directory.
Browser Speaker	Receive sound via the camera's microphone through the browser's support.

Manual Recording ◉	Start/Stop recording of the camera's video. If the camera is currently recording, it will display a red dot in the upper-right corner of the live view window. Note that only users with administrative roles can perform recording, i.e., **System Admin, Root Admin** and **Local Admin** (for authorized channels only).
OSD (On-Screen Display) OSD	Display selected information on the screen. Refer to **System** > **Display Settings** > **OSD Settings** for more information.
Standard Size ⛶	Switch the display in standard or actual size.
Full Screen ⤢	Enable full screen or actual size display.
Show/Hide E-Map	Display the relative E-Map of the camera. The E-map will pop out from the lower-left corner. It shows the camera's geographic data.
Hotspot	Fix a channel on the grid.

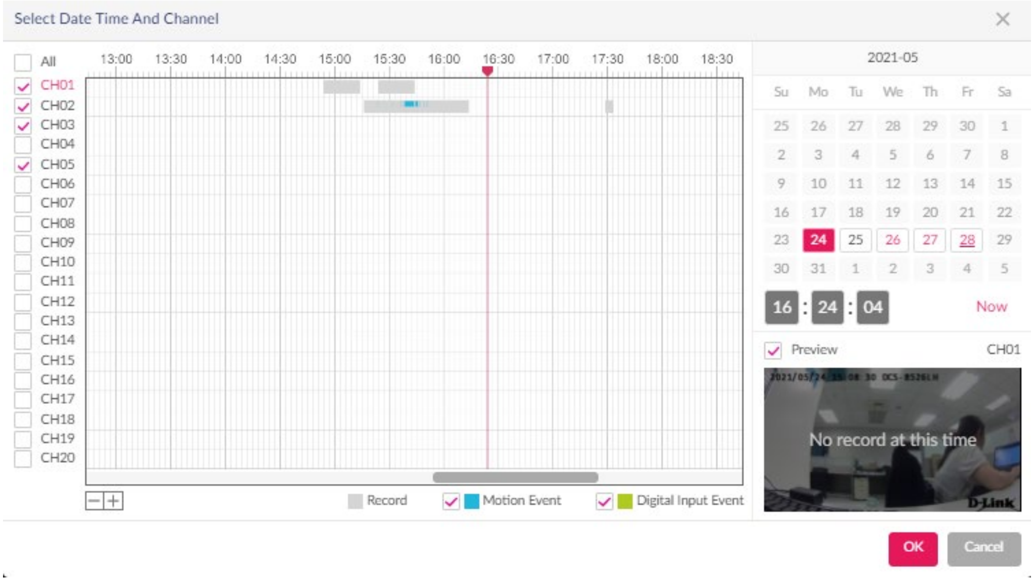
Playback

The Playback tab allows you to play back video recordings stored in the HDD. You can browse and play back the recordings directly from the screen.



Timeline

This function retrieves video recordings based on date and time. To play a recording with the specified date and time, click 🎞.



The **Select Date Time Add Channel** screen appears. Select the interested channel on the left. The dates having recordings can be selected on the calendar in the right-hand side. Specify the time below or click **Now** to fill in the current time automatically. You can also specify the time in the visualized timeline by dragging the red line across to the desired hour (0-24) and minute (in unit of 3 minutes). Select the option box to distinguish the type of event recording: **Motion Event**, **Digital Input Event** and regular **Recording** in the displayed timeslot. Then click **OK** to save your settings and return to the playback screen.

The available recordings of the selected channels will be displayed in the timeline.
To control the playback of the selected recording and channel:

1. Click **Play** on the control bar to start playing back the video.
2. You can also skip 15s forward or backward to move forward or backward the playback timeline in the unit of 15 seconds.
3. On the timeline, click **+** to increase the granularity of timespan or – to decrease the granularity of timespan. Click to refresh the current playback screen. You can also drag the timeline to play a recording indicated across the timeline.
4. To control the speed of the playback, click and select the speed: 1 (slowest), or 2 (fastest).
5. Click On-screen Display OSD to show or hide camera information.
6. To take a snapshot during the playback, click . The snapshot will be saved as a png file in your browser’s download directory.
7. To change the video quality, click . The exact resolution and relevant streaming parameters depend on the support of the camera. Refer to **Video Profile** settings in the **Camera** tab for video parameters and values.
8. To export a recording, click and select **Export**. Click **Download** and select whether to export the video with the OSD displayed information as well as the video quality. Click **OK** to save your settings. The recording will be saved as an MP4 file in your browser’s download directory. Note the default duration of the recording to be saved is 3 minutes, to lengthen it, drag the left or right arrow further on the timeline.
9. To remove a recording, click and select **Remove**. The recording with the specified time frame with duration will be deleted.
10. Click or to switch between standard or actual size display.

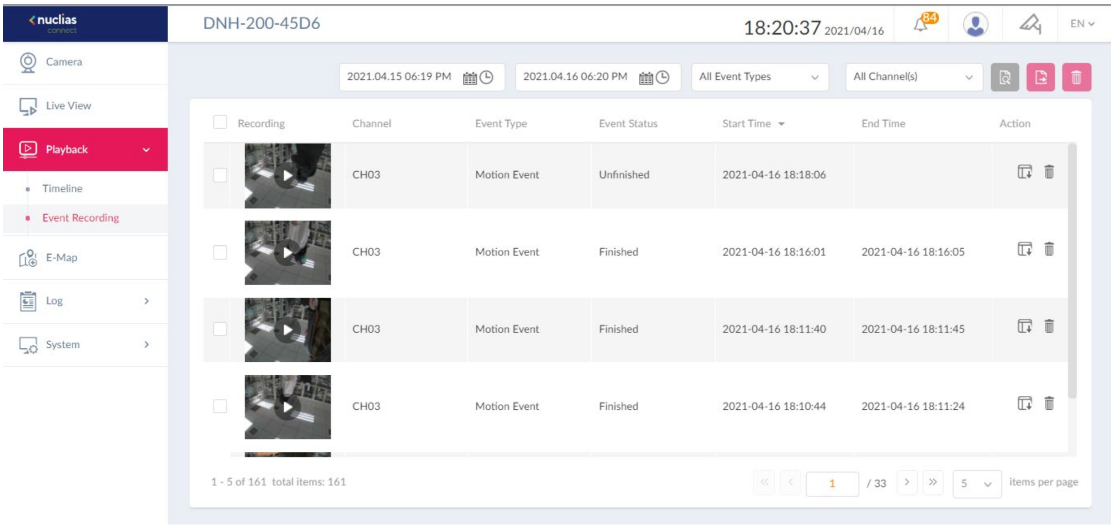
11. Click to enable the sound of the video clip by adjusting the volume of the speaker through the browser's support.

Notes:

1. The naming rule of the recorded file is **CH#_YYYYMMDD_HHMMSS_to_YYYYMMDD_HHMMSS_xxx** (where xxx is a unique serial number from 001 to 999 for this recording in the selected timespan)**.** You can use media players that can open MP4 file to play exported recordings.
2. The maximum duration of a single recording file is 60 minutes.
3. Only users with administrative roles can perform recording export or removal, i.e., **System Admin, Root Admin** and **Local Admin** (for authorized channels only).

Event Recording

This function retrieves video recordings triggered by motion or digital input.



2021.04.15 06:19 PM | 2021.04.16 06:20 PM | All Event Types | All Channel(s)

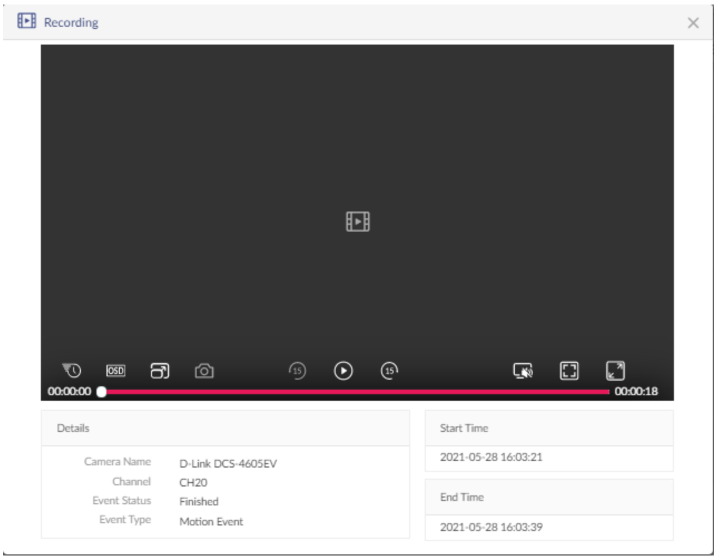
Recording	Channel	Event Type	Event Status	Start Time	End Time	Action
□	CH03	Motion Event	Unfinished	2021-04-16 18:18:06		
□	CH03	Motion Event	Finished	2021-04-16 18:16:01	2021-04-16 18:16:05	
□	CH03	Motion Event	Finished	2021-04-16 18:11:40	2021-04-16 18:11:45	
□	CH03	Motion Event	Finished	2021-04-16 18:10:44	2021-04-16 18:11:24	

1 - 5 of 161 total items: 161 « ‹ 1 / 33 › » 5 items per page

To search a recording:

1. Click to select the start and end date and time as the search time period.
2. Select **Event Types** from the following options: All Event Types, Motion Event, or Digital Input Event.
3. Select the **Channel Number**.
4. Click to start the search.

In the event list, check to select the video recording and click 📄 to export and download it to your browser's download directory. The default video format is MP4. You can also delete the selected recordings by clicking 🗑. To play a recording, click ▶ and the options for playback control will be presented. Refer to **Playback** for more information.



Details

Camera Name	D-Link DCS-4605EV
Channel	CH20
Event Status	Finished
Event Type	Motion Event

Start Time

2021-05-28 16:03:21

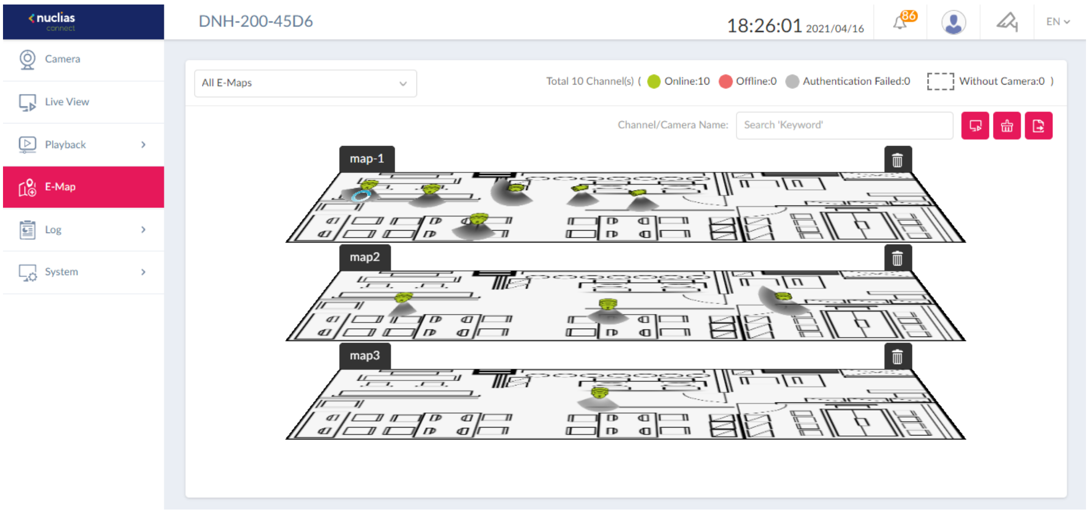
End Time

2021-05-28 16:03:39

Note: Only users with administrative roles can perform recording export and removal, i.e., **System Admin, Root Admin** and **Local Admin** (for authorized channels only).

E-Map

The E-Map tab allows you to visualize the location of the camera on the map. It helps visualize the geographic data of IP cameras to allow for quick identification of the location of each IP camera, especially when an alert occurs.



Total 10 Channel(s) (● Online:10 ● Offline:0 ● Authentication Failed:0 ⬚ Without Camera:0)

To create an E-Map:

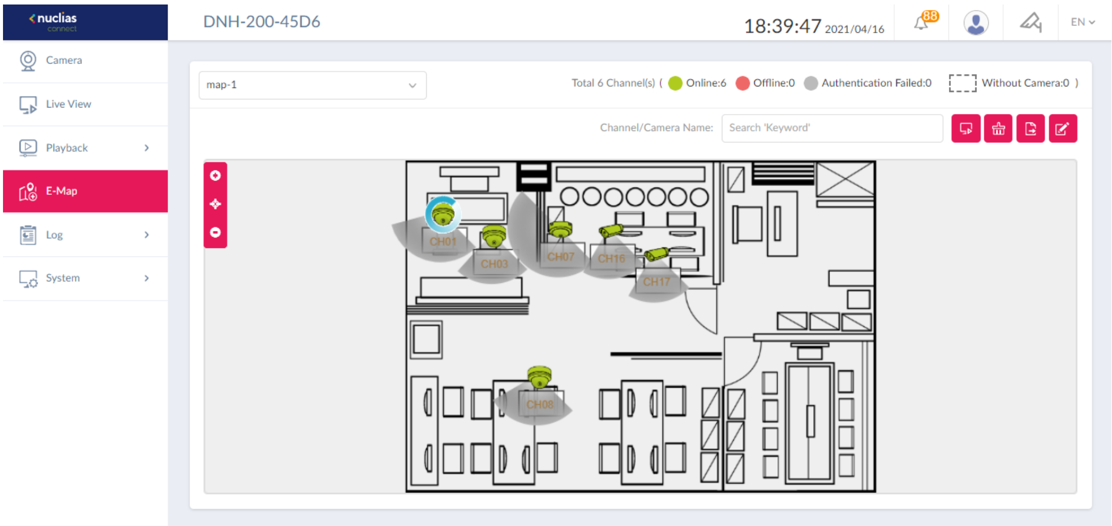
1. Click +. The screen shows a default floor map.

2. To change the default geographic scene, click to upload an image of the monitoring location from your local drive.

3. Click to select camera channels and drag and drop the camera icon to the right place on the map.

Once you are done with the E-map creation, click to export the list of maps as a pdf file. Up to 3 E-Maps can be created.

Click an E-Map (or click the E-Map drop-down list in the left-hand corner) to view the selected E-Map and modify its settings.



On the E-Map you can perform the following with the selected channel:

Live View: Shows the live video of the camera.

Clear Event: Reset the flashing alert of the camera.

Edit: Unlock the position of the camera to change its position.

To obtain detailed information of the camera, mouse over the camera and the following will be displayed: channel number, camera name, status, IP address, view angle, and last seen, which shows the information of the Camera and the last time that the camera was accessed from the Live View.

To search an E-Map:

Enter a keyword in the search field to search E-maps by camera name or channel.

E-map Alert

Once an alert event happens (i.e., motion or digital input detection), the camera icon will flash to alert you immediately to take necessary actions.

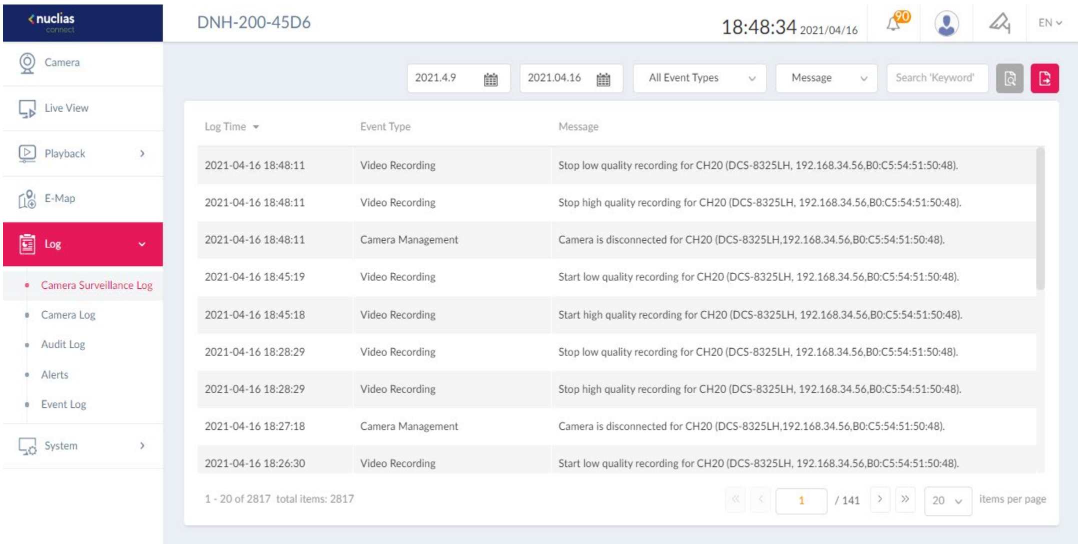
To reset the flashing alert, click **Clear Event**. To enable the flashing alert of events, please enable motion detection notification for E-Map. Refer to **Systems** > **Event Settings** > **Motion Detection** > **E-Map**.

Notes:

1. The event recordings (**Playback** > **Event Recording**) will not be erased with the **Clear Event** function.
2. The **Add, Delete**, **Edit,** and **Export E-Map** functions can only be performed by users with the administrative roles, i.e., **System Admin, Root Admin** and **Local Admin** (for authorized channels only).

LOG

The Log tab stores the activities of cameras and the log entries are grouped into the following categories: **Camera Surveillance Log, Camera Log, Audit Log, Alerts,** and **Event Log**. To navigate among log types, select a respective tab. In each log window, you can apply type-specific filters to see log entries of your interest, for example, channel or username.



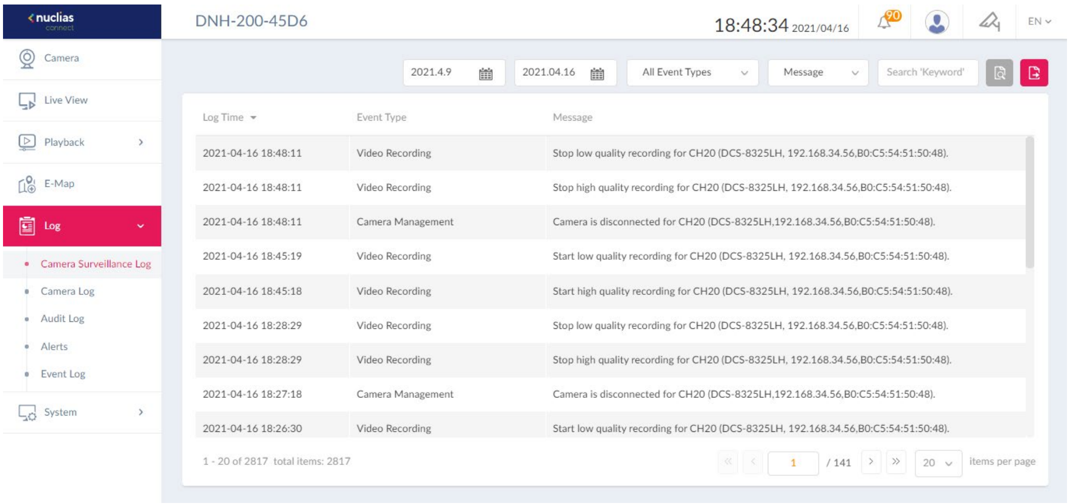
Log Time	Event Type	Message
2021-04-16 18:48:11	Video Recording	Stop low quality recording for CH20 (DCS-8325LH, 192.168.34.56,B0:C5:54:51:50:48).
2021-04-16 18:48:11	Video Recording	Stop high quality recording for CH20 (DCS-8325LH, 192.168.34.56,B0:C5:54:51:50:48).
2021-04-16 18:48:11	Camera Management	Camera is disconnected for CH20 (DCS-8325LH,192.168.34.56,B0:C5:54:51:50:48).
2021-04-16 18:45:19	Video Recording	Start low quality recording for CH20 (DCS-8325LH, 192.168.34.56,B0:C5:54:51:50:48).
2021-04-16 18:45:18	Video Recording	Start high quality recording for CH20 (DCS-8325LH, 192.168.34.56,B0:C5:54:51:50:48).
2021-04-16 18:28:29	Video Recording	Stop low quality recording for CH20 (DCS-8325LH, 192.168.34.56,B0:C5:54:51:50:48).
2021-04-16 18:28:29	Video Recording	Stop high quality recording for CH20 (DCS-8325LH, 192.168.34.56,B0:C5:54:51:50:48).
2021-04-16 18:27:18	Camera Management	Camera is disconnected for CH20 (DCS-8325LH,192.168.34.56,B0:C5:54:51:50:48).
2021-04-16 18:26:30	Video Recording	Start low quality recording for CH20 (DCS-8325LH, 192.168.34.56,B0:C5:54:51:50:48).

1 - 20 of 2817 total items: 2817 1 / 141 20 items per page

Camera Surveillance Log

This type of log records surveillance related management and events such as video recording start and stop time and disconnection of cameras.

For Camera Surveillance Log, you can filter the entries by the event type and message content.



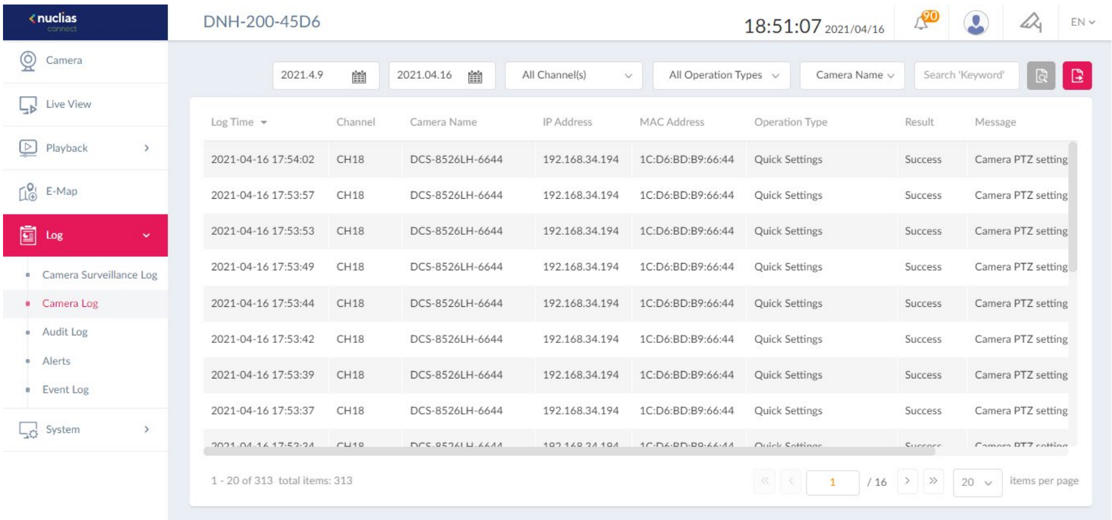
Log Time	Event Type	Message
2021-04-16 18:48:11	Video Recording	Stop low quality recording for CH20 (DCS-8325LH, 192.168.34.56,B0:C5:54:51:50:48).
2021-04-16 18:48:11	Video Recording	Stop high quality recording for CH20 (DCS-8325LH, 192.168.34.56,B0:C5:54:51:50:48).
2021-04-16 18:48:11	Camera Management	Camera is disconnected for CH20 (DCS-8325LH,192.168.34.56,B0:C5:54:51:50:48).
2021-04-16 18:45:19	Video Recording	Start low quality recording for CH20 (DCS-8325LH, 192.168.34.56,B0:C5:54:51:50:48).
2021-04-16 18:45:18	Video Recording	Start high quality recording for CH20 (DCS-8325LH, 192.168.34.56,B0:C5:54:51:50:48).
2021-04-16 18:28:29	Video Recording	Stop low quality recording for CH20 (DCS-8325LH, 192.168.34.56,B0:C5:54:51:50:48).
2021-04-16 18:28:29	Video Recording	Stop high quality recording for CH20 (DCS-8325LH, 192.168.34.56,B0:C5:54:51:50:48).
2021-04-16 18:27:18	Camera Management	Camera is disconnected for CH20 (DCS-8325LH,192.168.34.56,B0:C5:54:51:50:48).
2021-04-16 18:26:30	Video Recording	Start low quality recording for CH20 (DCS-8325LH, 192.168.34.56,B0:C5:54:51:50:48).

1 - 20 of 2817 total items: 2817 1 / 141 20 items per page

Camera Log

This type of log records camera management and operations such as motion detection zone setting and other parameter setting.

For Camera Log, you can filter the entries by channel number, operation type (i.e., operations performed on the camera), and camera information such as name, IP address, MAC address, and message.



DNH-200-45D6

18:51:07 2021/04/16

2021.4.9 | 2021.04.16 | All Channel(s) | All Operation Types | Camera Name | Search 'Keyword'

Log Time	Channel	Camera Name	IP Address	MAC Address	Operation Type	Result	Message
2021-04-16 17:54:02	CH18	DCS-8526LH-6644	192.168.34.194	1C:D6:BD:B9:66:44	Quick Settings	Success	Camera PTZ setting
2021-04-16 17:53:57	CH18	DCS-8526LH-6644	192.168.34.194	1C:D6:BD:B9:66:44	Quick Settings	Success	Camera PTZ setting
2021-04-16 17:53:53	CH18	DCS-8526LH-6644	192.168.34.194	1C:D6:BD:B9:66:44	Quick Settings	Success	Camera PTZ setting
2021-04-16 17:53:49	CH18	DCS-8526LH-6644	192.168.34.194	1C:D6:BD:B9:66:44	Quick Settings	Success	Camera PTZ setting
2021-04-16 17:53:44	CH18	DCS-8526LH-6644	192.168.34.194	1C:D6:BD:B9:66:44	Quick Settings	Success	Camera PTZ setting
2021-04-16 17:53:42	CH18	DCS-8526LH-6644	192.168.34.194	1C:D6:BD:B9:66:44	Quick Settings	Success	Camera PTZ setting
2021-04-16 17:53:39	CH18	DCS-8526LH-6644	192.168.34.194	1C:D6:BD:B9:66:44	Quick Settings	Success	Camera PTZ setting
2021-04-16 17:53:37	CH18	DCS-8526LH-6644	192.168.34.194	1C:D6:BD:B9:66:44	Quick Settings	Success	Camera PTZ setting
2021-04-16 17:53:34	CH18	DCS-8526LH-6644	192.168.34.194	1C:D6:BD:B9:66:44	Quick Settings	Success	Camera PTZ setting

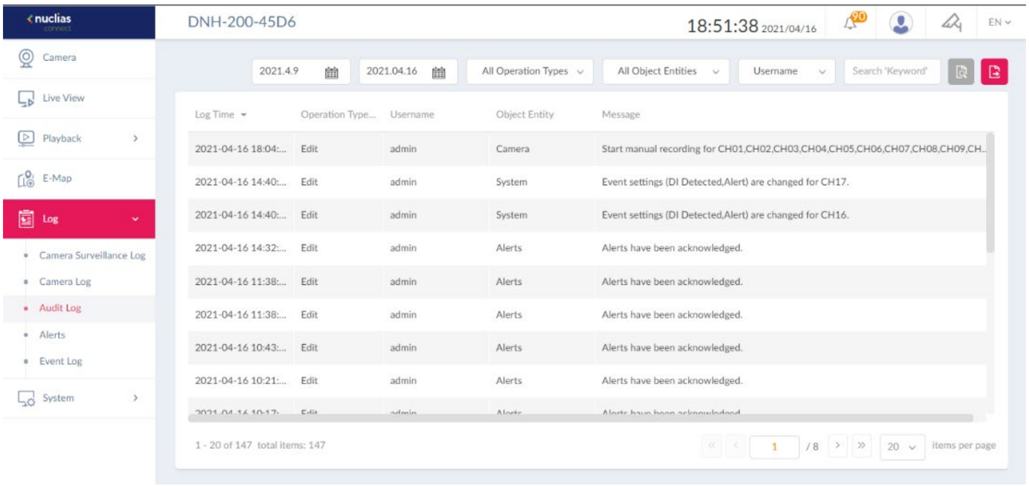
1 - 20 of 313 total items: 313

1 / 16 | 20 items per page

Audit Log

This type of log records user activities such as event trigger settings, video export and start and stop of manual recording. The Audit Log is only available to users with the **System Admin** and **Root Admin** role.

For Audit Log, you can filter the entries by operation type (operations that performed on the object entities) and object entity (i.e., the objects associated with the functional tabs on the left side), and username.



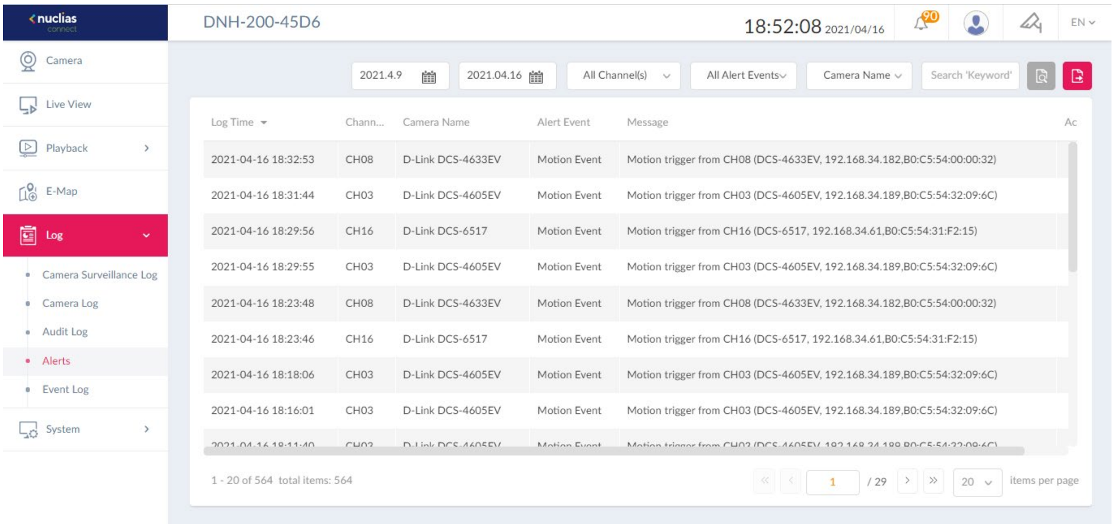
Log Time	Operation Type...	Username	Object Entity	Message
2021-04-16 18:04:...	Edit	admin	Camera	Start manual recording for CH01,CH02,CH03,CH04,CH05,CH06,CH07,CH08,CH09,CH...
2021-04-16 14:40:...	Edit	admin	System	Event settings (DI Detected,Alert) are changed for CH17.
2021-04-16 14:40:...	Edit	admin	System	Event settings (DI Detected,Alert) are changed for CH16.
2021-04-16 14:32:...	Edit	admin	Alerts	Alerts have been acknowledged.
2021-04-16 11:38:...	Edit	admin	Alerts	Alerts have been acknowledged.
2021-04-16 11:38:...	Edit	admin	Alerts	Alerts have been acknowledged.
2021-04-16 10:43:...	Edit	admin	Alerts	Alerts have been acknowledged.
2021-04-16 10:21:...	Edit	admin	Alerts	Alerts have been acknowledged.
2021-04-16 10:17:...	Edit	admin	Alerts	Alerts have been acknowledged.

1 - 20 of 147 total items: 147 1 / 8 20 items per page

Alerts

This type of log records events activities for alert, i.e., Motion Event, Digital Input Event, and Connection Lost Event.

For Alerts, you can filter the entries by channel number, event type (motion, digital input or connection lost), and camera name or message content. The number of unread alerts will be indicated in the upper-right corner by 🔔3 .



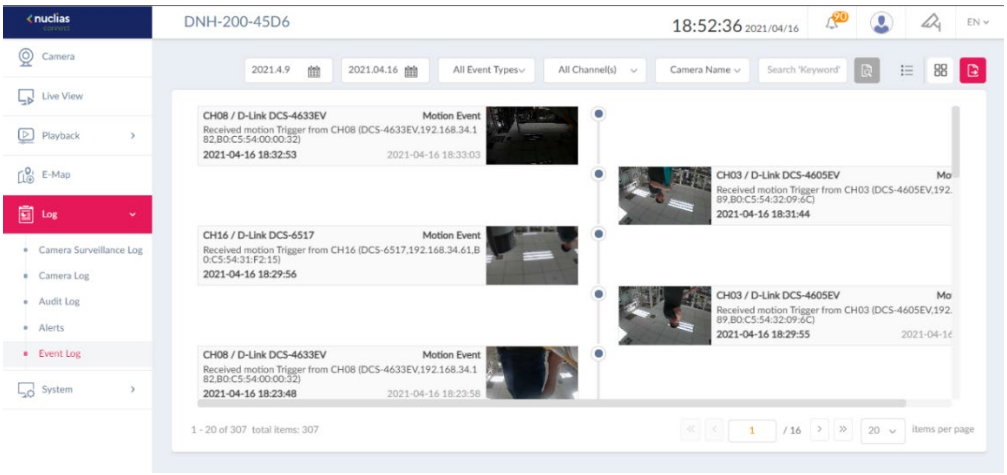
Log Time	Chann...	Camera Name	Alert Event	Message	Ac
2021-04-16 18:32:53	CH08	D-Link DCS-4633EV	Motion Event	Motion trigger from CH08 (DCS-4633EV, 192.168.34.182,B0:C5:54:00:00:32)	
2021-04-16 18:31:44	CH03	D-Link DCS-4605EV	Motion Event	Motion trigger from CH03 (DCS-4605EV, 192.168.34.189,B0:C5:54:32:09:6C)	
2021-04-16 18:29:56	CH16	D-Link DCS-6517	Motion Event	Motion trigger from CH16 (DCS-6517, 192.168.34.61,B0:C5:54:31:F2:15)	
2021-04-16 18:29:55	CH03	D-Link DCS-4605EV	Motion Event	Motion trigger from CH03 (DCS-4605EV, 192.168.34.189,B0:C5:54:32:09:6C)	
2021-04-16 18:23:48	CH08	D-Link DCS-4633EV	Motion Event	Motion trigger from CH08 (DCS-4633EV, 192.168.34.182,B0:C5:54:00:00:32)	
2021-04-16 18:23:46	CH16	D-Link DCS-6517	Motion Event	Motion trigger from CH16 (DCS-6517, 192.168.34.61,B0:C5:54:31:F2:15)	
2021-04-16 18:18:06	CH03	D-Link DCS-4605EV	Motion Event	Motion trigger from CH03 (DCS-4605EV, 192.168.34.189,B0:C5:54:32:09:6C)	
2021-04-16 18:16:01	CH03	D-Link DCS-4605EV	Motion Event	Motion trigger from CH03 (DCS-4605EV, 192.168.34.189,B0:C5:54:32:09:6C)	
2021-04-16 18:11:40	CH03	D-Link DCS-4605EV	Motion Event	Motion trigger from CH03 (DCS-4605EV, 192.168.34.189,B0:C5:54:32:09:6C)	

1 - 20 of 564 total items: 564 1 / 29 20 items per page

Event Log

This type of log records events, i.e., Motion Event and Digital Input Event.

For Event Log, you can filter the entries by channel number, even type (motion or digital input), and camera name or message content. To switch between list and graphic mode, click ☰ and ⊞ respectively. The graphic mode will present the events centered on a vertical timeline with the thumbnails of the events to help you track and spot a particular event especially if you have multiple cameras on the scene. Mouseover the event thumbnail to view it in a bigger picture.



2021.4.9 | 2021.04.16 | All Event Types | All Channel(s) | Camera Name

CH08 / D-Link DCS-4633EV Motion Event
Received motion Trigger from CH08 (DCS-4633EV,192.168.34.182,B0:C5:54:00:00:32)
2021-04-16 18:32:53 2021-04-16 18:33:03

CH03 / D-Link DCS-4605EV Mo
Received motion Trigger from CH03 (DCS-4605EV,192.89,B0:C5:54:32:09:6C)
2021-04-16 18:31:44

CH16 / D-Link DCS-6517 Motion Event
Received motion Trigger from CH16 (DCS-6517,192.168.34.61,B0:C5:54:31:F2:15)
2021-04-16 18:29:56

CH03 / D-Link DCS-4605EV Mo
Received motion Trigger from CH03 (DCS-4605EV,192.89,B0:C5:54:32:09:6C)
2021-04-16 18:29:55 2021-04-16

CH08 / D-Link DCS-4633EV Motion Event
Received motion Trigger from CH08 (DCS-4633EV,192.168.34.182,B0:C5:54:00:00:32)
2021-04-16 18:23:48 2021-04-16 18:23:58

1 - 20 of 307 total items: 307 | 1 / 16 | 20 items per page

Filter Logs

Filtering logs helps you extract logs of your interest especially from a large number of log entries. To filter log entries, select the start and end time for the search time period and click the filtering options specific for a log type, enter the keyword for the selected field, then click 🔍 to start your search. To order the list of entries by field, click the field name at the top of the list and click it again to reverse the order.

Export logs

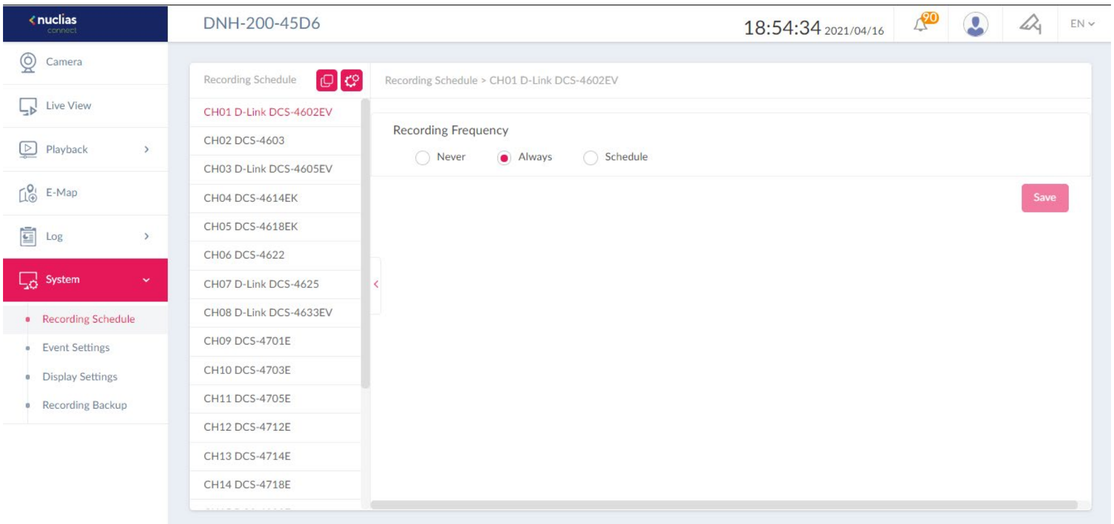
Exporting logs helps you save log entries beyond the system's log retention period. Up to 100,000 log entries can be saved in the system. The exported log will be in excel format with a name: Camera_Surveillance_Log Type_YYYY_MMDD_HHMMSS.

To export a log, simply click ⇥ in each log window. The exported file will be saved in your browser's download directory.

Note: Only users with administrative roles can perform log export, i.e., **System Admin, Root Admin** and **Local Admin**.

System

This tab provides management functions for the surveillance system and it contains the following configurations: **Recording Schedule, Event Settings, Display Settings,** and **Recording Backup**.



CH01 D-Link DCS-4602EV
CH02 DCS-4603
CH03 D-Link DCS-4605EV
CH04 DCS-4614EK
CH05 DCS-4618EK
CH06 DCS-4622
CH07 D-Link DCS-4625
CH08 D-Link DCS-4633EV
CH09 DCS-4701E
CH10 DCS-4703E
CH11 DCS-4705E
CH12 DCS-4712E
CH13 DCS-4714E
CH14 DCS-4718E

Recording Frequency
○ Never ● Always ○ Schedule

Recording Schedule

The Recording Schedule tab allows you to schedule automatic recording based on frequency and event type.

Before scheduling a recording, configure the global Recording Configuration by clicking ⚙.

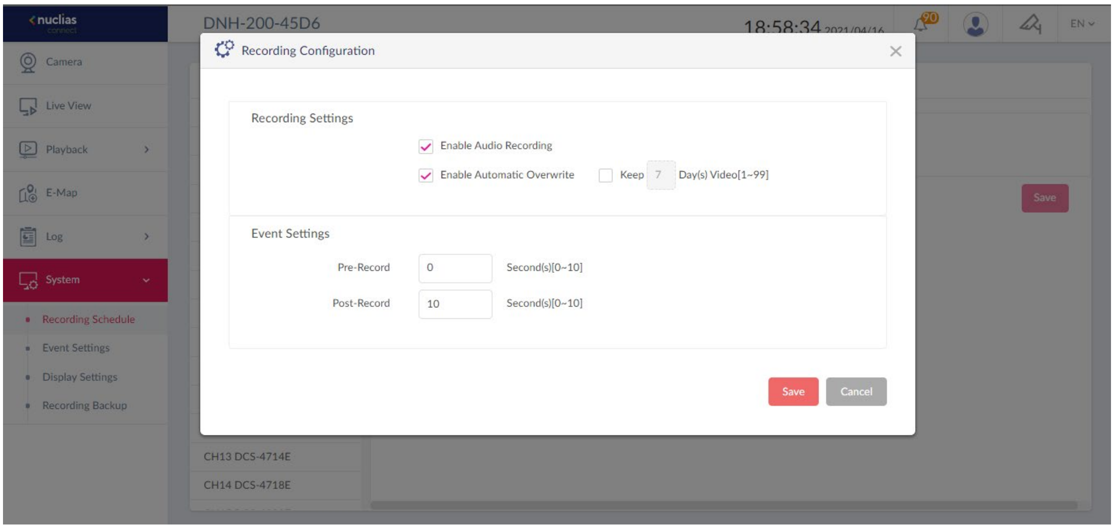
Recording Settings

Enable Audio Recording: Enable or disable audio recording to have sound in video clips. The default is disabled.

Enable Automatic Overwrite: Enable this function to overwrite old recordings and save storage space. Enter the number of days for maximum recording retention (range: 1-99). The default is disabled.

Event Settings: For event recording, the system can record in advance before the actual event triggers the recording function (Pre-Record) as well as record after the event takes place (Post-Record). Enter the time (range: 0-10 seconds) for both Pre-Record (default: 0 second) and Post-Record time (default: 10 seconds). They are useful when you want to record the activities preceding or following an event that triggers recording.

Note: Only users with administrative roles can configure Recording Schedule, i.e., **System Admin, Root Admin** and **Local Admin** (for authorized channels only).



Recording Configuration

Recording Settings

☑ Enable Audio Recording

☑ Enable Automatic Overwrite □ Keep 7 Day(s) Video[1~99]

Event Settings

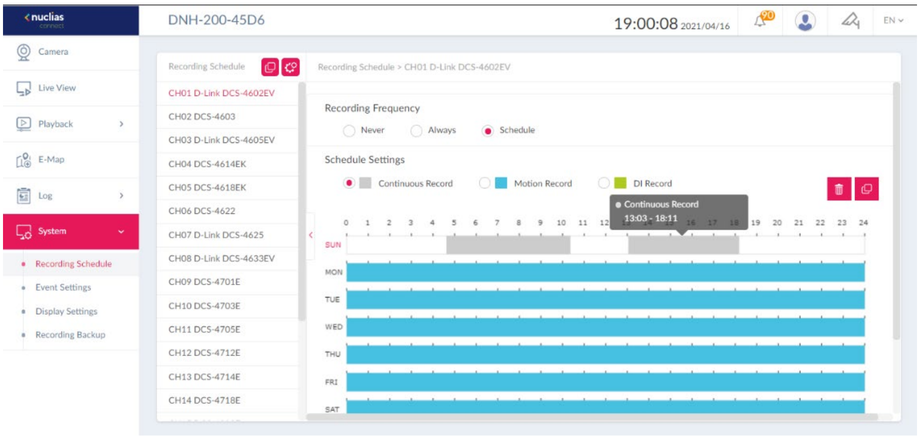
Pre-Record 0 Second(s)[0~10]

Post-Record 10 Second(s)[0~10]

Save Cancel

To schedule a recording:

1. Click a channel to set automatic recording on the left pane.
2. Select the **Recording Frequency** from these options: Never, Always, or Schedule.
3. If Schedule is selected, select **Schedule Settings** to record based on one of these conditions: **Continuous Record**, **Motion Record**, **Digital Input Record**.
4. Click the start time and drag to the end time of the selected days of the week to specify the time period for this type of recording. Note that you can define different time periods for different recording conditions for each day of the week.
5. Click 🗑 to delete the set schedules for the selected day.
6. To replicate the settings among the days of the week, click ⧉ on the upper-right side of the page.
7. Click **Save** at the bottom of the page to apply your settings.



Recording Schedule > CH01 D-Link DCS-4602EV

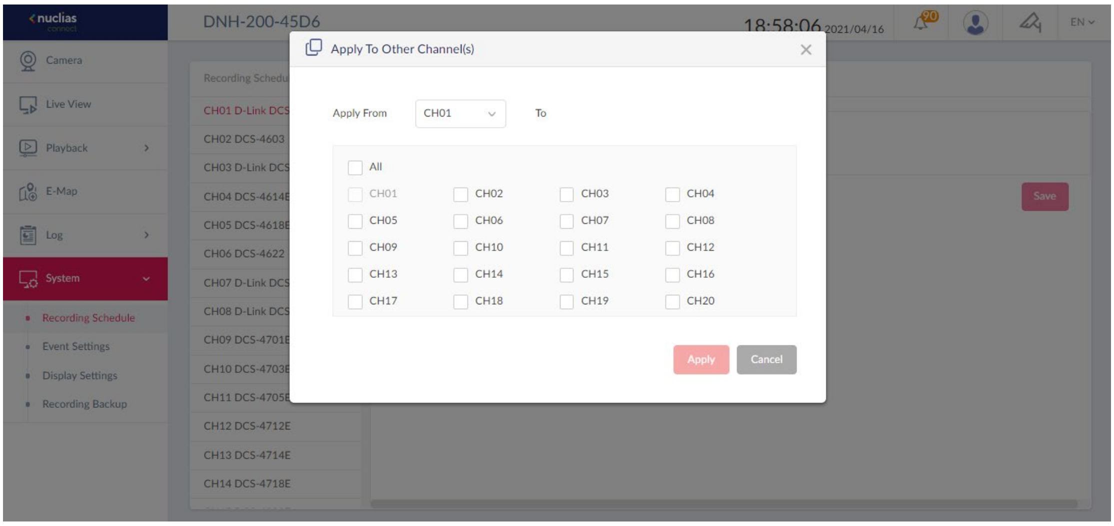
Recording Frequency

○ Never ○ Always ● Schedule

Schedule Settings

● Continuous Record ○ Motion Record ○ DI Record

Once a recording schedule for a channel is configured, you can replicate the settings among the channels by clicking ⧉ in the upper-right hand side of the left pane.



Apply To Other Channel(s)

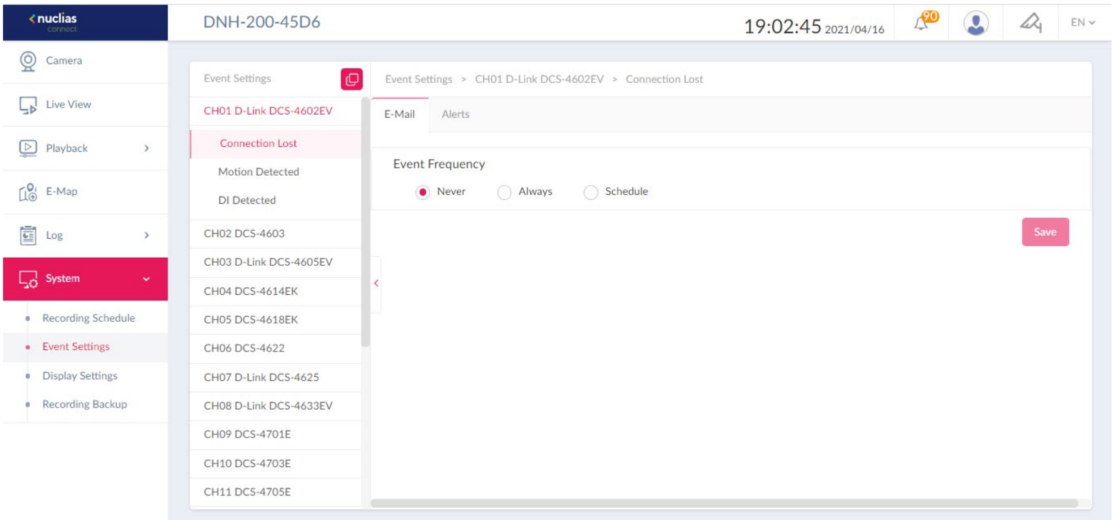
Apply From CH01 To

□ All

□ CH01	□ CH02	□ CH03	□ CH04
□ CH05	□ CH06	□ CH07	□ CH08
□ CH09	□ CH10	□ CH11	□ CH12
□ CH13	□ CH14	□ CH15	□ CH16
□ CH17	□ CH18	□ CH19	□ CH20

Event Settings

The Event Settings tab allows you to configure automatic notifications based on event type.



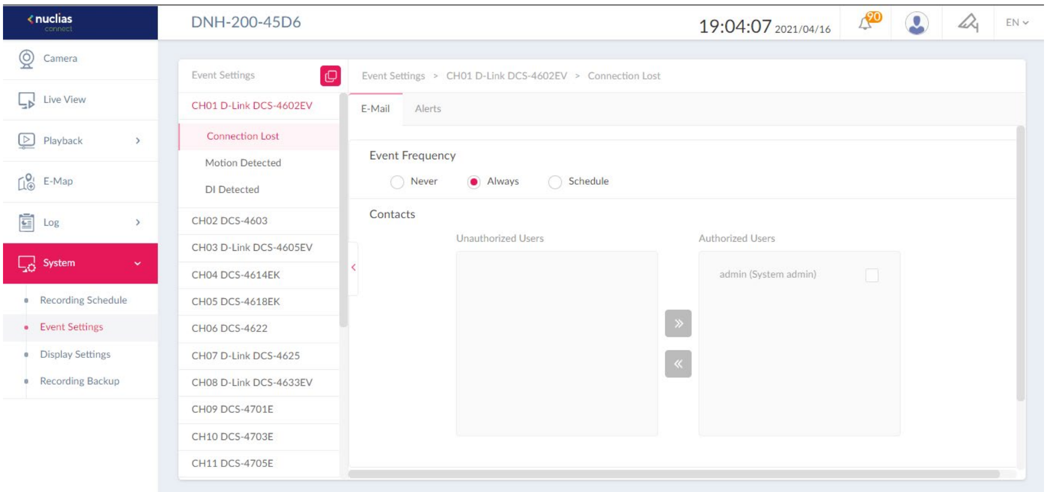
Event Frequency

● Never ○ Always ○ Schedule

To configure an event notification:

1. Select a channel for event settings in the left pane. 3 subtabs representing different categories of events appear, i.e., Connection Lost, Motion Detection, and Digital Input Detection.
2. For Connection Lost, you can configure both email notifications and system alerts. To configure an E-mail Notification:

3. Select the notification **Frequency** from these options: Never, Always, or Schedule.
4. If Never is selected, no email notifications will be sent for this type of event.
5. If Always is selected, also select users to receive email notifications whenever the event happens by keeping them in the **Authorized Users** list.
6. If Schedule is selected, click the start time and drag to the end time of the selected days of a week to specify the time period for this type of event monitoring. Note that you can define multiple time periods for each day of a week.
7. You can replicate the scheduled time periods among different days of the week by clicking ⧉.
8. Under Contacts, select users to receive email notifications whenever the event happens in the specified time periods by keeping them in the **Authorized Users** list.
9. Click **Save** to apply your settings.



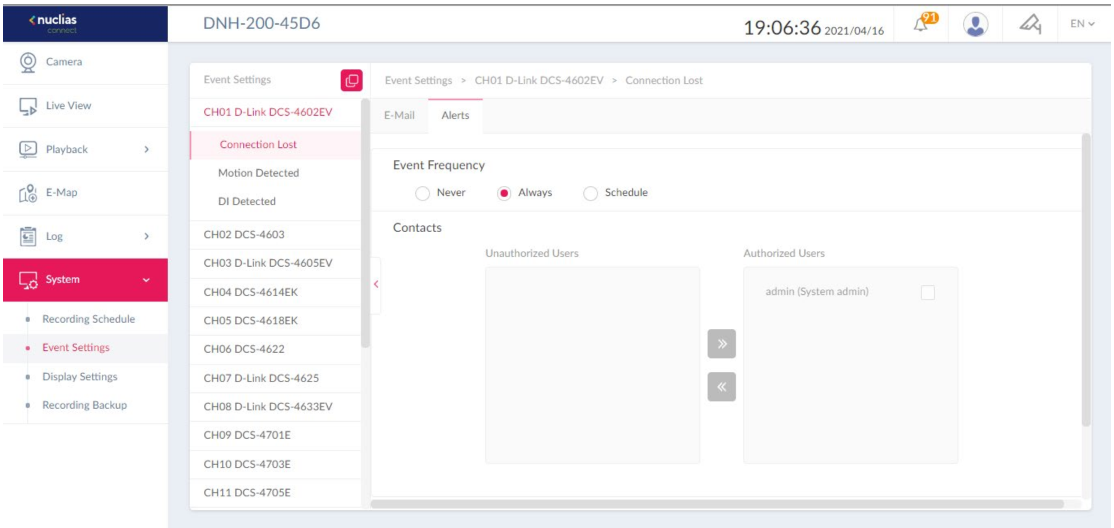
Event Frequency ○ Never ● Always ○ Schedule

Authorized Users: admin (System admin) □

Notes:

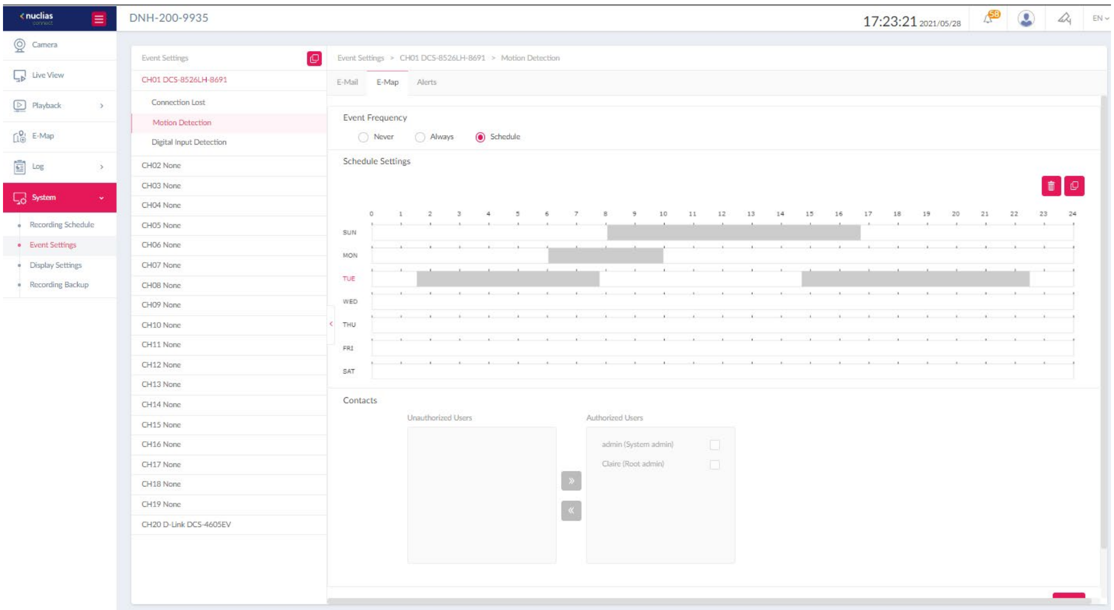
1. The Authorized/Unauthorized Users List is obtained from the users list of **User Management** of **System Settings**. For email notifications, the emails are obtained from the entered email addresses of the User's List. Please refer to **System Settings** > **User Management** for more information.
2. Only users with administrative roles can configure Event Settings, i.e., **System Admin, Root Admin** and **Local Admin** (for authorized channels only).

To configure alert notifications, click the **Alerts** tab and follow the same steps for setting E-mail Notifications above. The alert messages can be viewed in **Log > Alerts**.



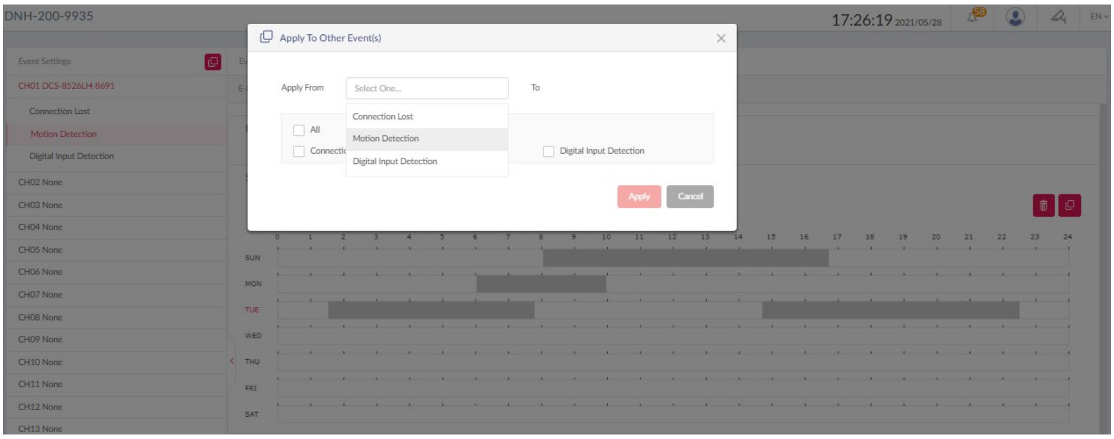
Event Frequency ○ Never ● Always ○ Schedule

For **Motion** and **Digital Input Detection** event types, configure an additional E-Map notification method with schedules and contacts. Refer to the above **E-mail Notifications** for detailed instructions on Event Frequency setting. And refer to **E-Map** for flashing alert on the E-map.



Event Frequency ○ Never ○ Always ● Schedule

You can replicate the settings among different event types by clicking ⧉ in the upper-right corner of the left pane.



DNH-200-9935 17:26:19 2021/05/28

Event Settings

CH01 DCS-8526LH-8691

Connection Lost

Motion Detection

Digital Input Detection

CH02 None

CH03 None

CH04 None

CH05 None

CH06 None

CH07 None

CH08 None

CH09 None

CH10 None

CH11 None

CH12 None

CH13 None

Apply To Other Event(s)

Apply From: Select One...
- Connection Lost
- Motion Detection
- Digital Input Detection

To

□ All

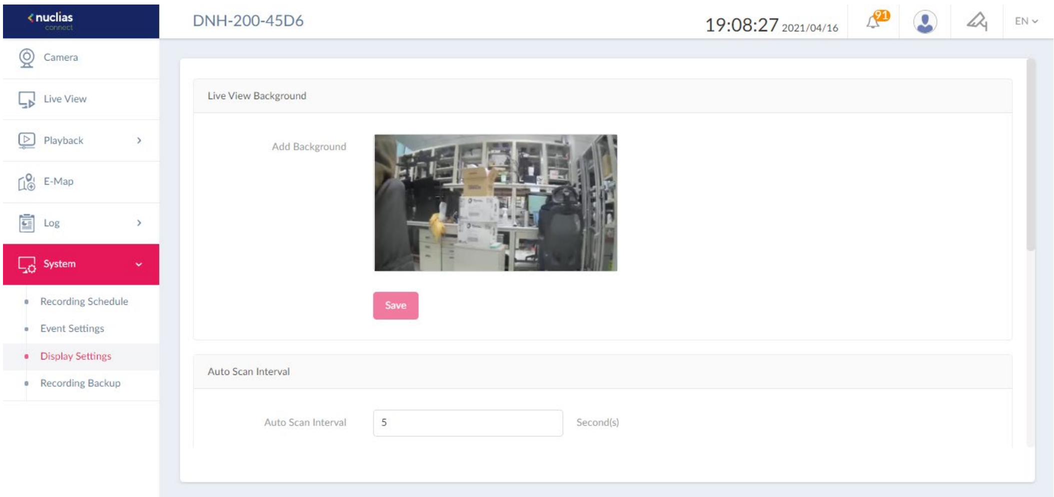
□ Connectio

□ Digital Input Detection

Apply Cancel

Display Settings

This tab allows you to customize the display of live videos such as the background image.



DNH-200-45D6 19:08:27 2021/04/16

Live View Background

Add Background

Save

Auto Scan Interval

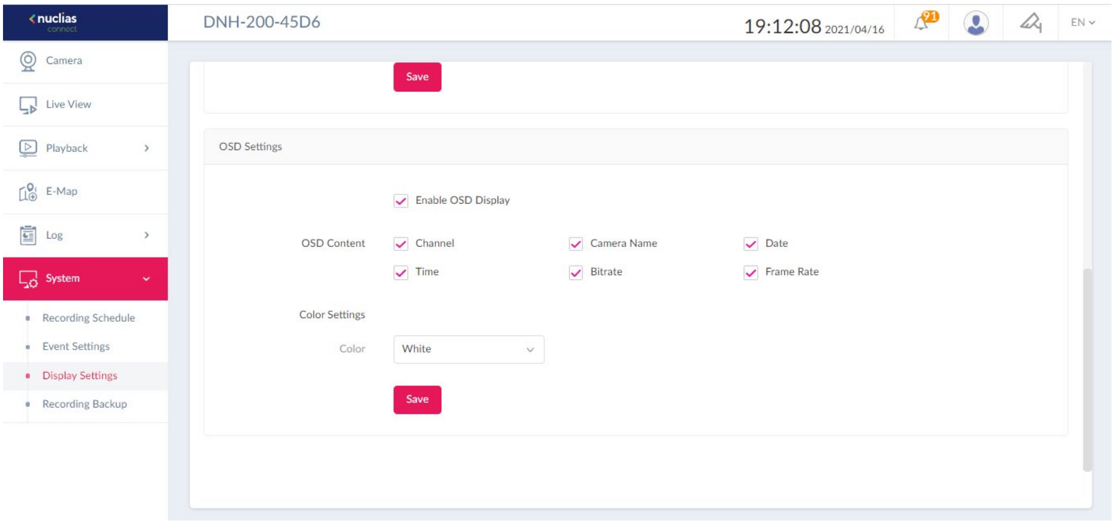
Auto Scan Interval: 5 Second(s)

To configure a customized live view setting:

1. **Live View Background**: Upload a picture to the upload area to add a background to all channels of the system.
2. **Auto Scan Interval:** Enter the interval for scanning channel (Range: 3~99 seconds). The Auto Scan is for automatic swapping among the screens of different channels. Refer to Live View for more information.

OSD Settings: To configure On-screen Display, first enable it. Select the information to be displayed from the following: Channel Number, Channel Name, Date, Time, Bitrate, and Frame Rate. Then select the color of the text.

The OSD can be dynamically displayed on the live and recorded (exported) videos as well as snapshot images as an option.



OSD Settings

☑ Enable OSD Display

OSD Content: ☑ Channel ☑ Camera Name ☑ Date ☑ Time ☑ Bitrate ☑ Frame Rate

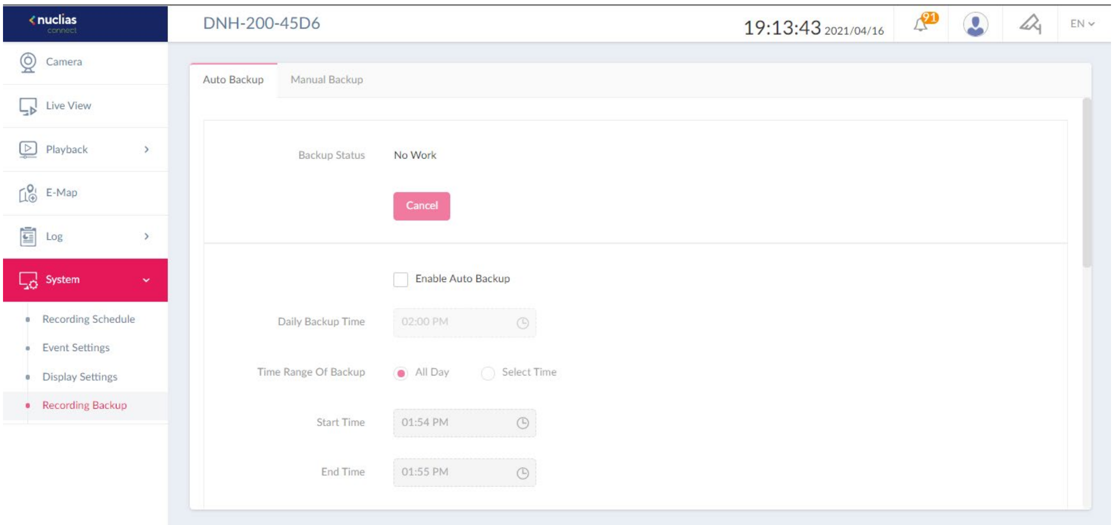
Color Settings

Color: White

Note: Only users with administrative roles can configure Display Settings, i.e., **System Admin, Root Admin** and **Local Admin**.

Recording Backup

This tab allows you to back up recorded videos automatically or manually. You can save recording files to a USB drive or an FTP server.



Backup Status: No Work

□ Enable Auto Backup

Daily Backup Time: 02:00 PM

Time Range Of Backup: ● All Day ○ Select Time

Start Time: 01:54 PM

End Time: 01:55 PM

To configure an **Auto Backup**:

1. Select **Enable Auto Backup**.
2. Select the time to execute **Daily Backup Time**.
3. Select the **Time Range of Backup** with the Start time and End Time for running automatic backup.
4. Select the **Channels** for backup operation.

5. Select **Backup Type**: **USB** or **FTP**.

   To upload video clips to an FTP site, enter the FTP Server’s IP Address or Domain Name, Port number, the FTP directory and folders (use ‘/’ to specify directories). Enter the Username and Password to connect with the FTP Server. You can click Test to test the connection with an FTP server.
6. Click **Save** to apply the settings.

To configure a **Manual Backup**:

1. Select **Day of Backup** to back up recordings for this date.
2. Select the **Time Range of Backup** with the Start time and End Time for the recording timespan of the videos.
3. Select the **Channels** for backup operation.
4. Select **Backup Type**: **USB** or **FTP**.

   To upload video clips to an FTP site, enter the FTP Server’s IP Address or Domain Name, Port number, the FTP directory and folders (use ‘/’ to specify directories). Enter the Username and Password to connect with the FTP Server. You can click **Test** to test the connection with an FTP server.
5. click **Start** to start backup immediately.

We recommend that you regularly make backups of video recordings as a data protection measure.

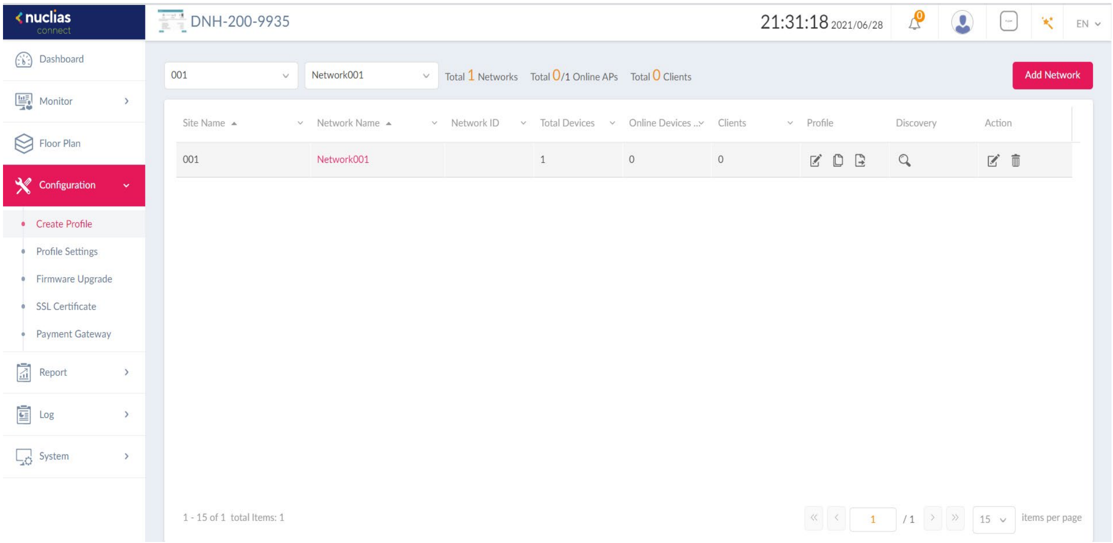
Note: Only users with the **System Admin** or **Root Admin** role can configure the Recording Backup settings.

Nuclias Connect App

With the Nuclias Connect app, users can manage sites and network remotely and easily by accessing the tool through a smart device. This section provides information on exporting the required network profiles from the Hub for managing the connected APs.

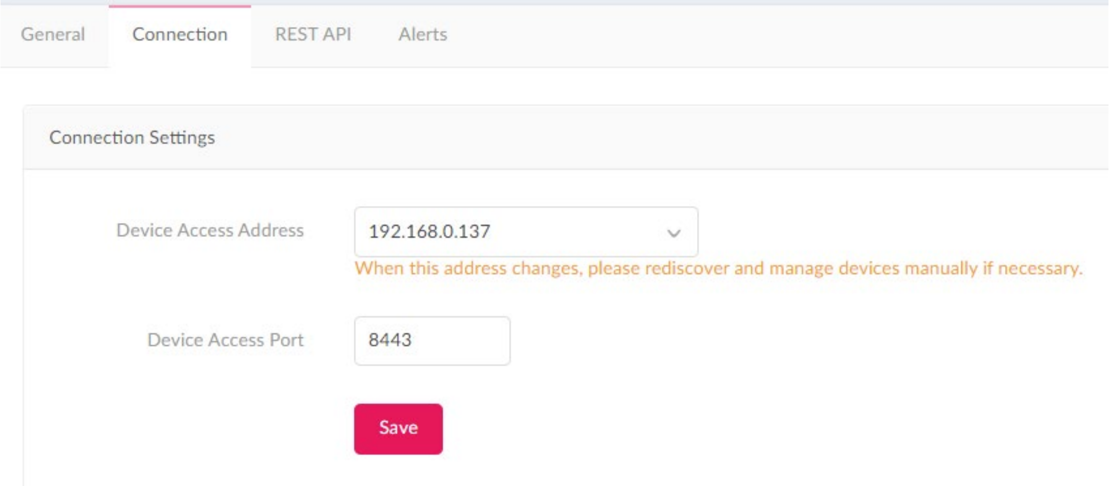
Export Network Profiles

To add new access points to the Hub, you must first export the required network profile from the Hub. The network profile contains the authentication key and the IP address of the controller. Select **Configuration** and then click the **Export** icon to export the network profile to your computer.



Site Name	Network Name	Network ID	Total Devices	Online Devices ...	Clients	Profile	Discovery	Action
001	Network001		1	0	0			

When access points are located on a public network and you are accessing the Hub remotely, you must ensure the Hub uses a public IP address or domain name. To verify the Hub's IP address, go to **AP Network > System > Settings > Connection**.



Device Access Address: 192.168.0.137

When this address changes, please rediscover and manage devices manually if necessary.

Device Access Port: 8443

Discover and Configure APs Using the Nuclias Connect App

The Nuclias Connect app is a mobile tool that provides easy management of single or multiple sites and networks from your smartphone or tablet. With the Nuclias Connect app, you can quickly deploy standalone APs to the Hub, scan a network for D-Link access points or configure individual APs.

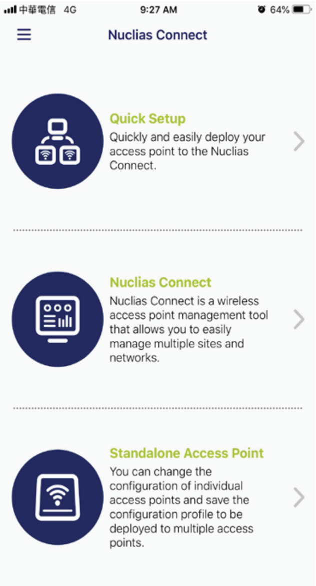
Note:

Before attempting to import a network profile, ensure that you have access to the Hub.
The Nuclias Connect app is available for both iOS and Android smart devices. The following functions are available:

- Quick Setup: Quickly and easily deploy your standalone AP to the Hub.
- Nuclias Connect: Manage your current sites and networks through Nuclias Connect.
- Standalone Access Point: You can change the configuration of individual APs and save the configuration profile to be deployed to multiple APs.

Quick Setup

After opening the Nuclias Connect app, the following window will appear. Tap **Quick Setup** to begin the deployment of a standalone AP to the Hub.



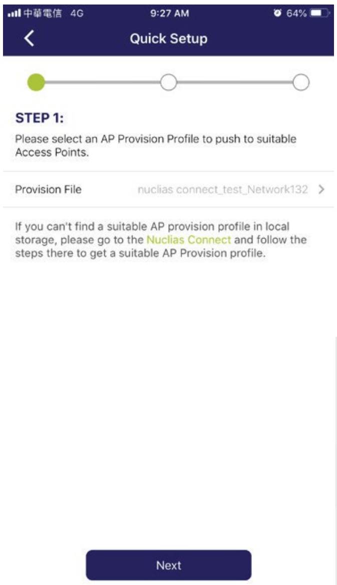
Quick Setup
Quickly and easily deploy your access point to the Nuclias Connect.

Nuclias Connect
Nuclias Connect is a wireless access point management tool that allows you to easily manage multiple sites and networks.

Standalone Access Point
You can change the configuration of individual access points and save the configuration profile to be deployed to multiple access points.

1. Select an AP provision profile. The profile is used to push to the selected APs. Tap **Quick Setup** to begin the deployment of a standalone AP to the Hub.

2. Tap **Provision File** to display a list of available local profiles. If no locally stored profile exists, a pop-up page will appear with further instructions on how to download a profile.
3. Tap **Download profile** to specify a connection to the Hub.

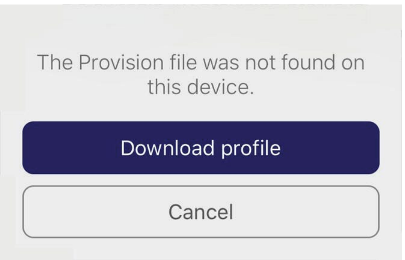


STEP 1:

Please select an AP Provision Profile to push to suitable Access Points.

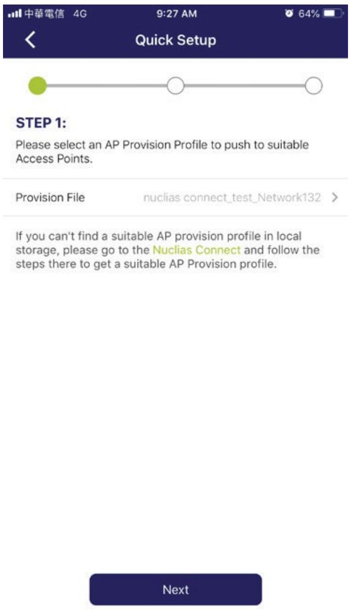
Provision File nuclias connect_test_Network132 >

If you can't find a suitable AP provision profile in local storage, please go to the Nuclias Connect and follow the steps there to get a suitable AP Provision profile.



The Provision file was not found on this device.

4. Once connected to a Hub, you will see profiles listed next to **Provision File**. Tap **Provision File** to select an AP provision profile.



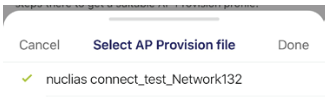
STEP 1:

Please select an AP Provision Profile to push to suitable Access Points.

Provision File nuclias connect_test_Network132 >

If you can't find a suitable AP provision profile in local storage, please go to the Nuclias Connect and follow the steps there to get a suitable AP Provision profile.

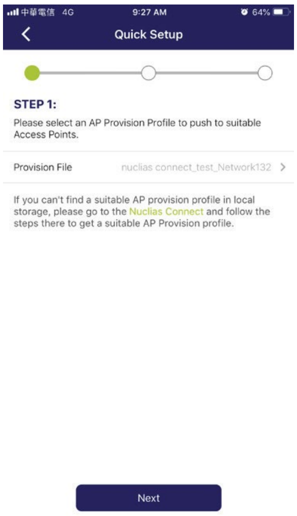
5. Select an available provision file. Tap **Done** to continue.



Cancel **Select AP Provision file** Done

✓ nuclias connect_test_Network132

6. Tap **Next** to continue when the Quick Setup screen appears.



中華電信 4G 9:27 AM 64%

Quick Setup

STEP 1:

Please select an AP Provision Profile to push to suitable Access Points.

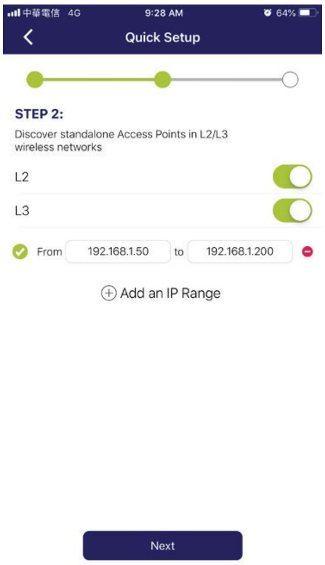
Provision File nuclias connect_test_Network132 >

If you can't find a suitable AP provision profile in local storage, please go to the Nuclias Connect and follow the steps there to get a suitable AP Provision profile.

Next

7. Tap the L2 or L3 button to enable discovery of APs on the L2 or L3 network respectively. For L3 network, enter a range of IP addresses. Tap add **+** to create a new IP range. Tap remove **-** to delete a defined range.

   Tap **Next** to initiate the discovery.



中華電信 4G 9:28 AM 64%

Quick Setup

STEP 2:

Discover standalone Access Points in L2/L3 wireless networks

L2 ●

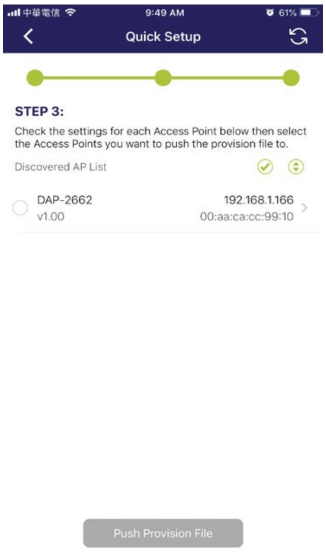
L3 ●

✓ From 192.168.1.50 to 192.168.1.200

⊕ Add an IP Range

Next

8. The detected access points are listed. Tap the radio button next to the AP to select it. The provision file that you selected will be pushed to the selected AP.



9:49 AM

Quick Setup

STEP 3:

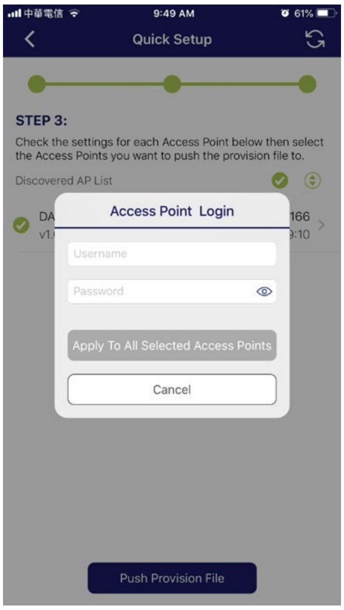
Check the settings for each Access Point below then select the Access Points you want to push the provision file to.

Discovered AP List

DAP-2662 v1.00	192.168.1.166 00:aa:ca:cc:99:10

Tap **Push Provision File** to continue.

9. The AP login pop-up window appears. Enter the username and password to access the selected AP.



9:49 AM

Quick Setup

STEP 3:

Check the settings for each Access Point below then select the Access Points you want to push the provision file to.

Discovered AP List

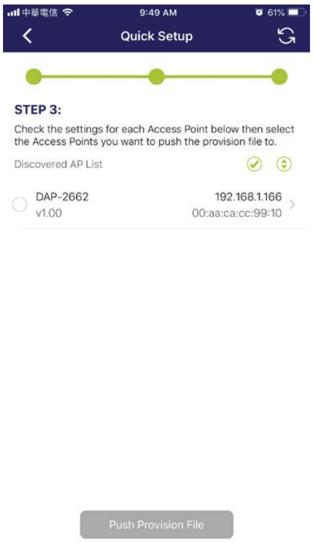
Access Point Login

10. Tap **Apply** to continue the login process. The Modify IP Information page appears. The entries can be modified.

Cancel	Discard any changes and continue.
Done	Accept any changes and continue the process.
Model Name	Displays the model name of the listed AP.
MAC	Displays the MAC address of the listed AP.
DHCP Mode	Enable or disable the DHCP mode function. When enabled, the AP establishes dynamic IP addressing with authorized clients.
IP Address	Enter the IP address of the AP.

Subnet Mask	Enter the subnet mask.
Default Gateway	Enter the IP address of the default gateway.
DNS	Enter the IP address of the DNS (Domain Name Server) server.

11. Tap **Done** or **Cancel** to continue the process. The provision file will be pushed to the selected APs. Tap **Finish** to complete the process. The screen displays the status of the push operation. For failed operation, tap **Push Provision File** to redo the operation again.



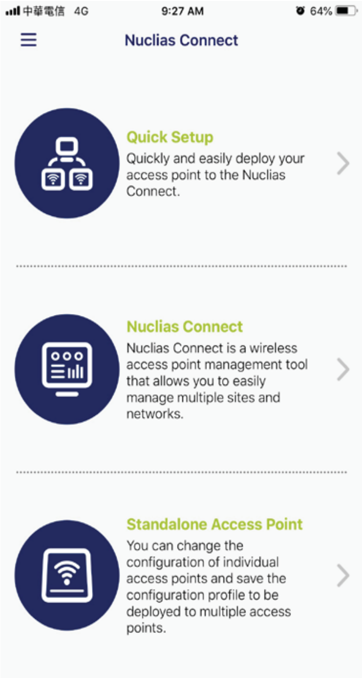
STEP 3:

Check the settings for each Access Point below then select the Access Points you want to push the provision file to.

Nuclias Connect

Nuclias Connect is a wireless access point management tool that allows you to manage your sites and networks.

1. Tap **Nuclias Connect** to connect to a Nuclias Connect Hub.

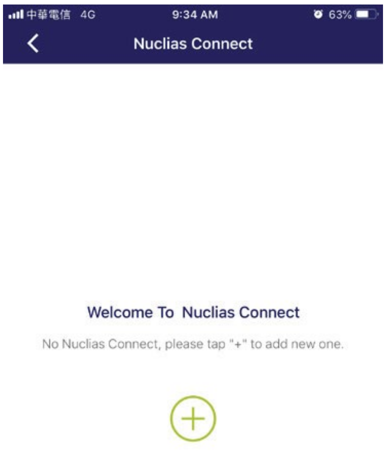


Quick Setup
Quickly and easily deploy your access point to the Nuclias Connect.

Nuclias Connect
Nuclias Connect is a wireless access point management tool that allows you to easily manage multiple sites and networks.

Standalone Access Point
You can change the configuration of individual access points and save the configuration profile to be deployed to multiple access points.

2. If no previous Nuclias Connect Hub has been paired, it will ask you to create a new Nuclias Connect pairing. Tap Add **+** to start the process.

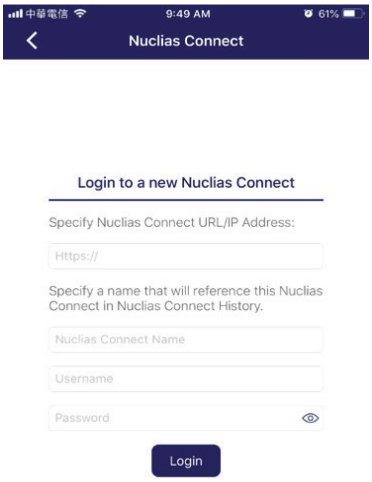


Welcome To Nuclias Connect

No Nuclias Connect, please tap "+" to add new one.

3. The following page lists the information required to log in to a designated Nuclias Connect Hub. Enter the required information in each field.

Specify Nuclias Connect URL/IP Address	Enter the secure URL/IP address of the Nuclias Connect Hub to pair with the app.
Nuclias Connect Name	Enter a descriptive name to easily identify the paired Hub.
Username	Enter the username to access the Hub.
Password	Enter the password for the user.
Login	Initiate the login process.



Specify Nuclias Connect URL/IP Address:

Https://

Specify a name that will reference this Nuclias Connect in Nuclias Connect History.

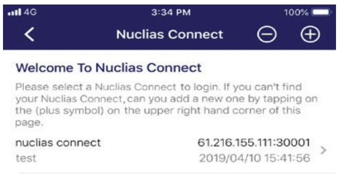
Nuclias Connect Name

Username

Password

Tap **Login** to initiate the login process.

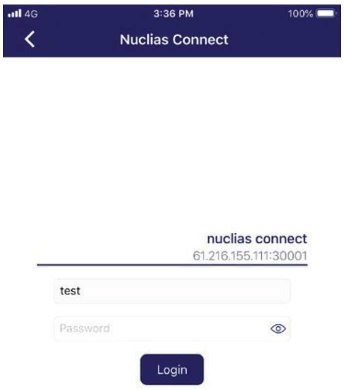
4. After a successful login, the pairing result will be added to the list and will be available for future login selection.



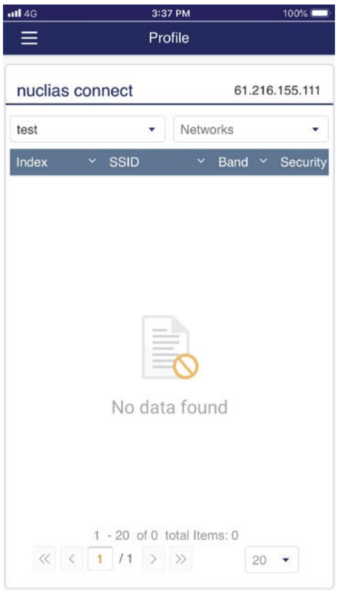
Please select a Nuclias Connect to login. If you can't find your Nuclias Connect, can you add a new one by tapping on the (plus symbol) on the upper right hand corner of this page.

nuclias connect 61.216.155.111:30001
test 2019/04/10 15:41:56

5. Tap on a **Nuclias Connect** Hub from the list. And enter the username and password to access the selected Nuclias Connect Hub. Then Tap **Login**.



6. The dashboard appears. The Nuclias Connect dashboard will list the currently defined sites, networks, access points, and clients.



The Nuclias Connect app is now paired with the Nuclias Connect Hub. With the app, profiles can be downloaded to the local device, then it can be pushed to supported access points.

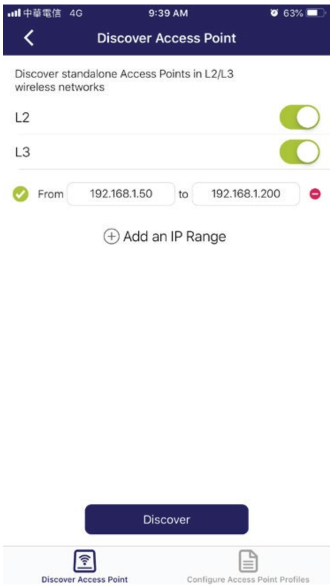
Standalone Access Point

Discover Access Point

This function allows you to discover access points in a L2/L3 wireless network.

1. Tap the L2 or L3 button to enable discovery of APs on the L2 or L3 network respectively.

For L3 network, enter a range of IP addresses. Tap add **+** to create a new IP range. Tap remove **-** to delete a defined range.



Discover standalone Access Points in L2/L3 wireless networks

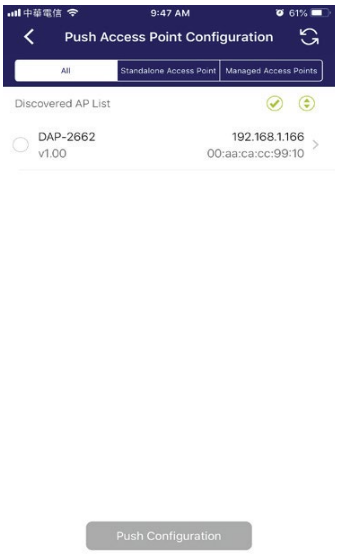
L2

L3

From 192.168.1.50 to 192.168.1.200

2. Tap **Next** to initiate the discovery process. Alternatively, tap **Configure Access Point Profiles** at the bottom of the page to add or delete any local profiles.

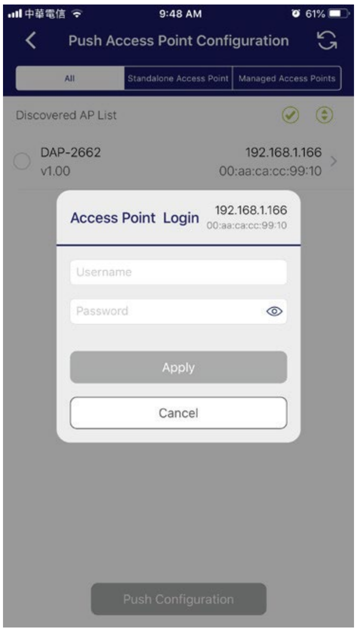
Upon completing the scan, a list of detected APs will be displayed. Tap the radio button next to an AP to select it. The selected local provision file will be pushed to the selected APs. Tap **Push Provision File** to continue.



Discovered AP List

○	DAP-2662 v1.00	192.168.1.166 00:aa:ca:cc:99:10

3. The AP login window appears. The IP and MAC address are shown at the top of the window. Confirm the selection and enter the username and password to access the selected AP. Tap **Apply** to continue.



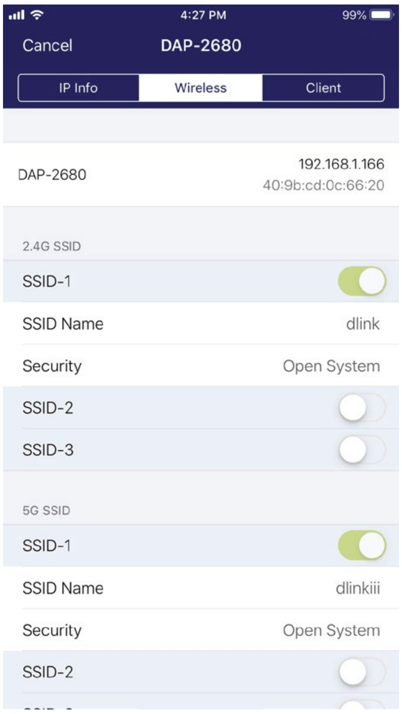
Once a successful login is established, the AP information will be displayed. The IP information, Wireless, and Client menus can be accessed as shown below.

Parameter	Description
Cancel	Discard any changes and continue.
Model Name	Displays the model name of the listed AP.
MAC	Displays the MAC address of the listed AP.
DHCP Mode	Enable or disable the DHCP mode function. When enabled, the AP establishes dynamic IP addressing with authorized clients.
IP Address	Enter the IP address of the AP.
Subnet Mask	Enter the subnet mask.
Default Gateway	Enter the IP address of the default gateway.
DNS	Enter the IP address of the DNS server.

The Wireless settings menu displays the following information:

Parameter	Description
Cancel	Discard any changes and continue the process.
DAP	Displays the model name and IP address of the AP.
2.4G SSID	
SSID-#	Enable or disable the SSID. The # character indicates the index of the SSID.
SSID Name	Change the current name of the SSID.
Security	Select wireless security mode: Open System (default), WPA Personal, or WPA-Enterprise.
5G SSID	

SSID-#	Enable or disable the SSID. The # character indicates the index of the SSID.
SSID Name	Change the current name of the SSID.
Security	Select wireless security mode: Open System (default), WPA Personal, or WPA-Enterprise.
Wireless Information	
Radio Band	Select a specific radio band: Off, 2.4G, 5G, or 2.4G / 5G.
Radio 2.4G Mode	Select a specific 2.4G radio mode: Mixed 802.11n, 80211g and 802.11b; Mixed 802.11g, 802.11b; 802.11n Only.
Radio 5G Mode	Select a specific 5G radio mode: Mixed 802.11n, 80211a; 802.11a Only; 802.11n; Mixed 802.11ac.
Country Code	Displays the assigned country for the AP.
Copy & Save Configuration	
Apply Configuration	Select an alternative AP in the discovered list to push the current configuration.
Save Configuration	Save the current configuration profile and enter a name for it.



DAP-2680

DAP-2680 192.168.1.166 40:9b:cd:0c:66:20

2.4G SSID

SSID-1

SSID Name dlink

Security Open System

SSID-2

SSID-3

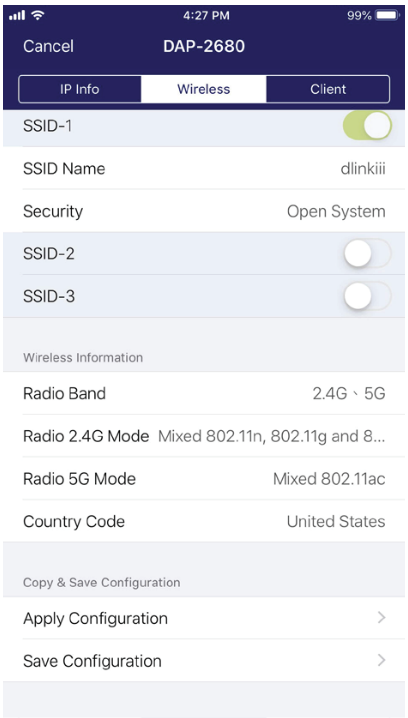
5G SSID

SSID-1

SSID Name dlinkiii

Security Open System

SSID-2



DAP-2680

SSID-1

SSID Name dlinkiii

Security Open System

SSID-2

SSID-3

Wireless Information

Radio Band 2.4G、5G

Radio 2.4G Mode Mixed 802.11n, 802.11g and 8...

Radio 5G Mode Mixed 802.11ac

Country Code United States

Copy & Save Configuration

Apply Configuration

Save Configuration

Nuclias Protect App

With the Nuclias Protect app, users can monitor dozens of network cameras effortlessly while accessing live video feeds from your mobile devices.

Discover and Configure Cameras Using the Nuclias Protect App

The Nuclias Protect app is a smart and convenient tool that is designed for easy management of network cameras that are connected through the Nuclias Connect Hub Plus (may be referred to as the Hub*)*. With the Nuclias Protect app, you can perform essential surveillance functions as well as monitor the system health of the DNH-200 remotely.

Notes:

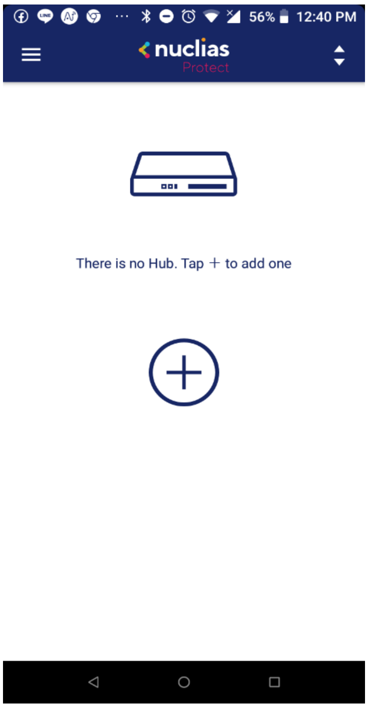
1. You could select "Access Local" to have local management. Or you will need a Nuclias SSO (single sign-on) account to use this app remotely. If you do not already have an account, you can click **Create New Account** where a browser window will open to a link where you can create one. Refer to Single Sign-On for more information.
2. The Nuclias Protect app is available for both iOS and Android smart devices.

Please use your mobile device to scan the QR code below to download the Nuclias Protect app:

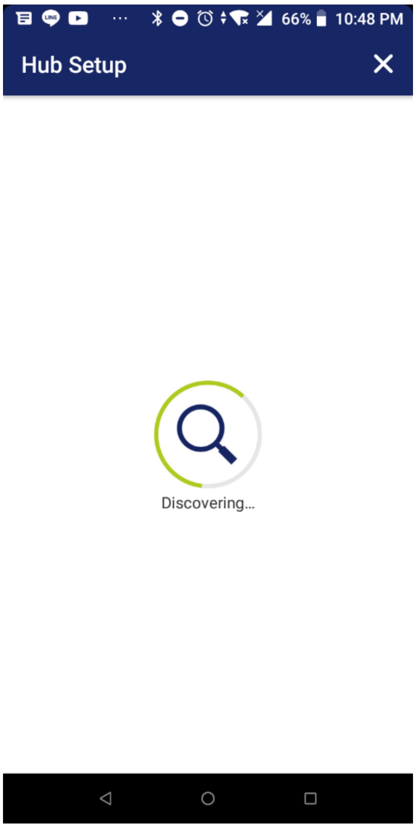
After logging in to the Nuclias Protect app, the following screen appears.

To add a new device, use the following procedure:

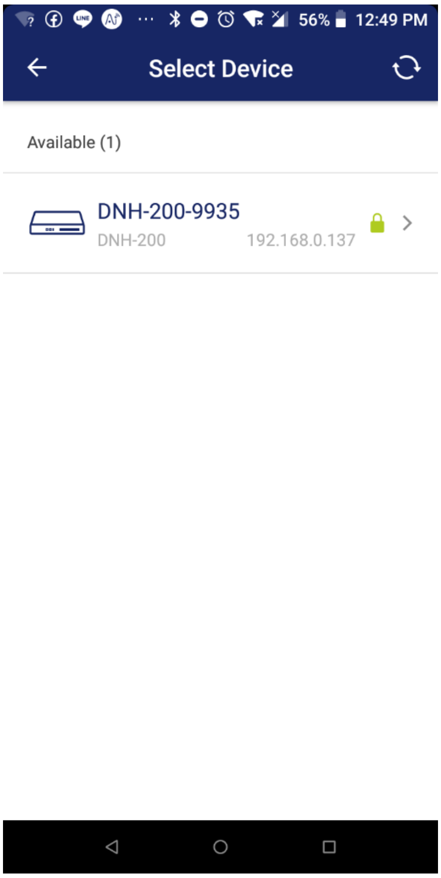
1. Tap **+** to add a new Hub device:



2. The automatic discovery starts to find hubs and lists available devices.



3. Tap the desired device to be connected.

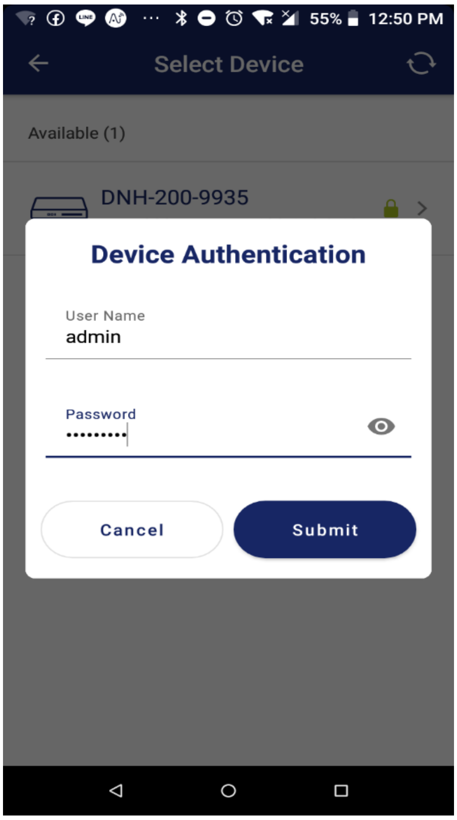


Select Device

Available (1)

DNH-200-9935
DNH-200 192.168.0.137

4. Enter device authentication information to add the device.



Select Device

Available (1)

DNH-200-9935

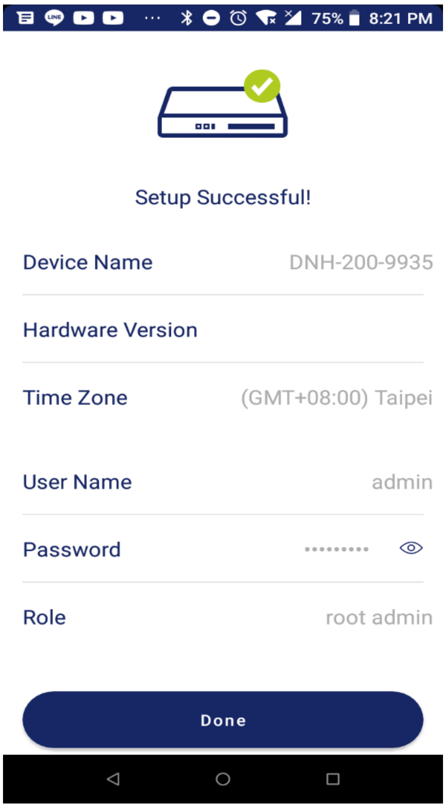
Device Authentication

User Name
admin

Password
•••••••••

5. If the device has been successfully added, the following Setup Successful! Screen will be

displayed.



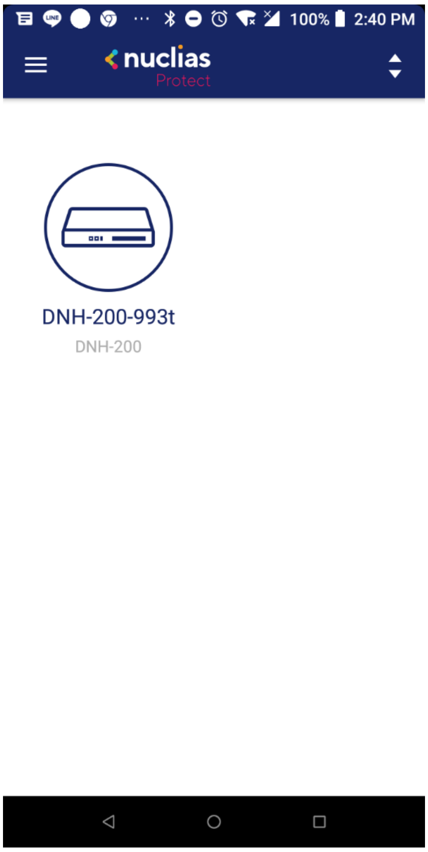
Setup Successful!

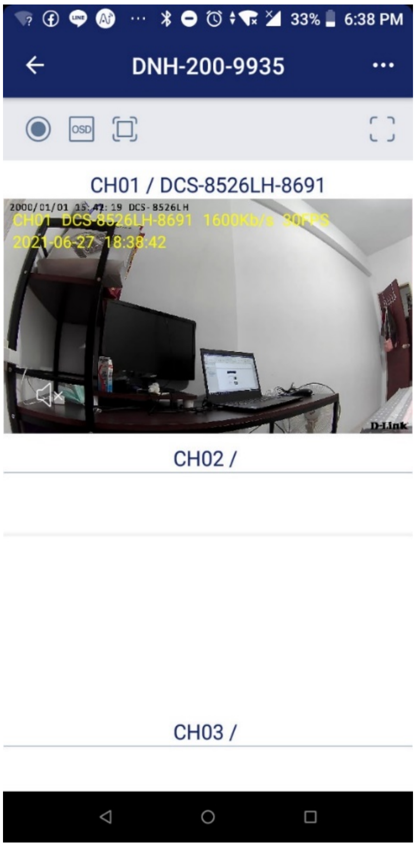
Device Name	DNH-200-9935
Hardware Version	
Time Zone	(GMT+08:00) Taipei
User Name	admin
Password	•••••••••
Role	root admin

Tap **Done** to go to the device list.

Access Camera List

Tap the DNH-200 device icon to go to the camera list.

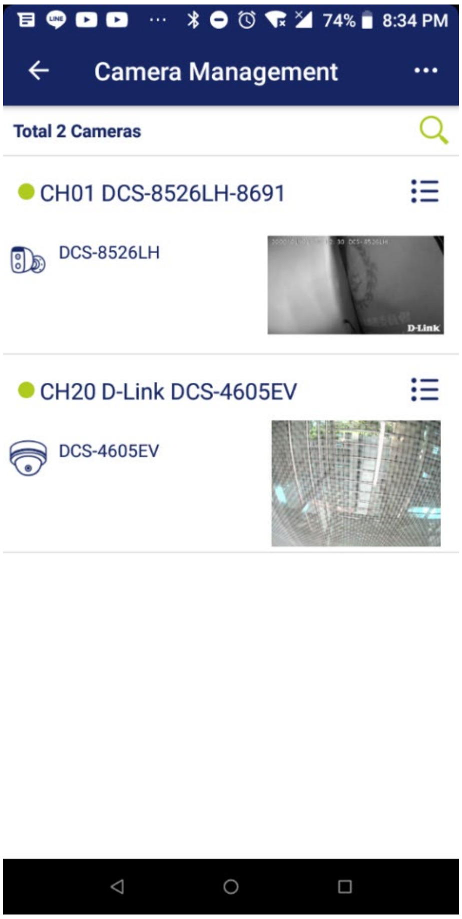




For advanced management options, click ••• . Then select one of the following options: **Camera Management, Hub Dashboard,** and **Hub Settings**.

Camera Management

Tap this option to see a list of connected cameras. Tap ••• to add cameras to the list or sort the list.

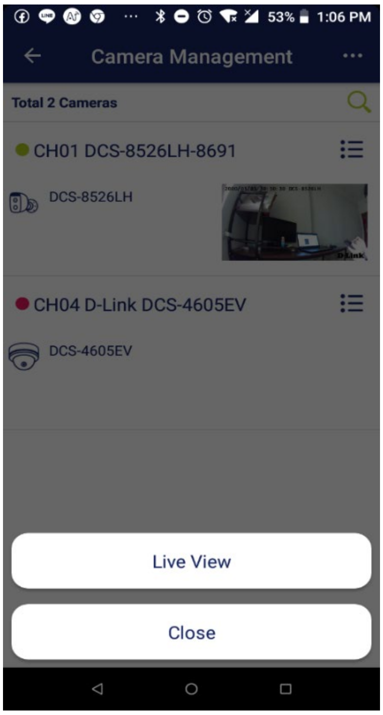


Tap the camera name to go to the respective **Camera Settings** page.

To change its name, tap the name field. Tap **Device Info** to obtain detailed camera information. The following table explains the information:

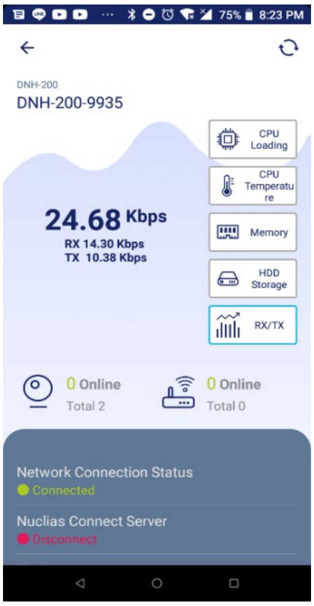
Name	The displayed name of the network camera.
Password	The password for the username with the authority to access the network camera.
Model	The model number of the network camera.
Channel	The channel number assigned to the network camera.
Camera Status	The operating status of the camera: online, offline, or authentication failed.
IPv4	The IP address of the network camera in IPv4 addressing scheme.
IPv6	The IP address of the network camera in IPv6 addressing scheme.
MAC Address	The MAC address of the network camera.
FW Version	The firmware version of the network camera.
HW Version	The hardware version of the network camera.
Update Time	The last time the device information was updated.
E-map association	The e-map name associated with this camera.

Tap ☰ to access Live View.



Hub Dashboard

This page displays system health information such as CPU loading and temperature. It allows you to monitor system operation and proactively prevent failures. You can update the information instantly by tapping the refresh icon in the upper-right corner.



Tap each icon for the respective type of information as described in the following table:

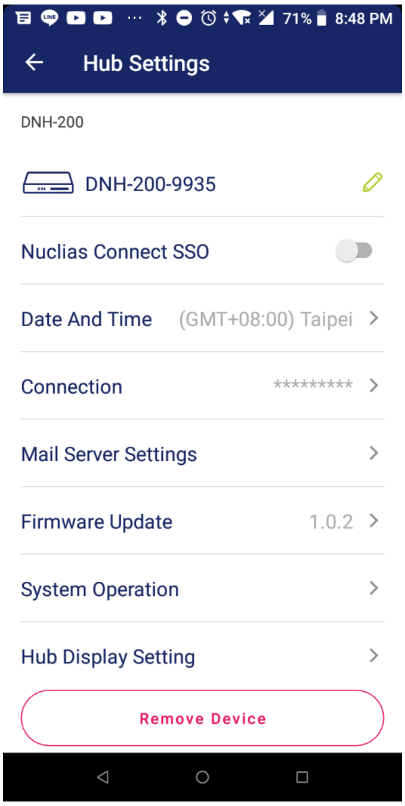
CPU Loading	The CPU’s workload in percentage.
CPU Temperature	The current CPU temperature under load.
Memory	The RAM usage in actual number and percentage.
HDD Storage	The HDD storage usage in actual number and in percentage.
RX/TX	The data transmission statistics for the Ethernet port.

Swipe up from the bottom to reveal more information about the Hub.

Network Connection Status	Shows whether the Hub is connected or disconnected.
Nuclias Connect Server	Shows whether the Hub is connected with a Nuclias Connect Server.
IPv4	The IP address of the Hub in IPv4 addressing scheme.
IPv6	The IP address of the Hub in IPv6 addressing scheme.
MAC Address	The MAC address of the Hub.
Uptime	The amount of time that the Hub has been up and running.
HDD Model	The model name of the HDD.
Firmware Version	The firmware version of the Hub.
Camera Surveillance Version	The version of the camera surveillance module.
AP Network Version	The version of the AP network module.
DDPv5 Client Version	The DDPv5 (D-Link Discovery Protocol) client version.

Hub Settings

This page displays the Hub information and allows you to configure it.



Hub Settings

DNH-200

DNH-200-9935

Nuclias Connect SSO

Date And Time (GMT+08:00) Taipei

Connection *********

Mail Server Settings

Firmware Update 1.0.2

System Operation

Hub Display Setting

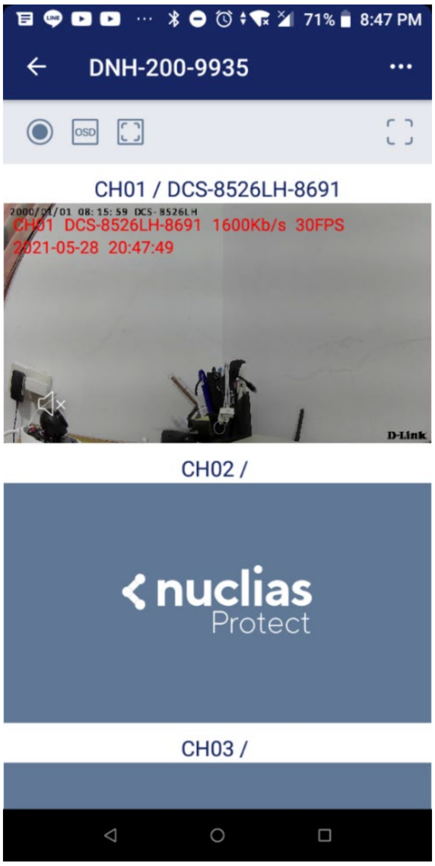
Remove Device

Tap one of these fields to change or configure its value:

Device Name	Click on the field to modify the device name.
Nuclias Connect SSO	Enable or disable Single Sign-On (SSO).
Date and Time	Select the time zone for the device. You will also be able to enable Daylight Saving and configure NTP.
Connection	Configure the IP assignment and web access port of the Hub. The IP assignment can be either DHCP or static IP address. The default is 443 for secure HTTP.
Mail Server Settings	Set an SMTP server (including the server address and port number as well as security mechanism and encoding type for communication) and the sender’s email account in order to reset your password in the event that you’ve forgotten your current password.
System Operation	Perform power-on, power-off or factory reset. When restoring the device, you can choose to preserve IP address and web access port of the Hub. You can also

	format the HDD installed on the Hub.
Hub Display Setting	Configure the background of the live video for all channels. You can also select the camera information (i.e., Channel, Camera Name, Date, Time, Bitrate, and Frame Rate) and the color it should be displayed on the screen in OSD settings. Note the configuration will overwrite the OSD settings on the Hub. Refer to **Camera Surveillance > System > Display Settings > OSD Settings**.
Remove Device	Tap this button to remove the Hub from the device list.

From the Home screen, tap the Hub and a list of channels with live videos from connected cameras appears.

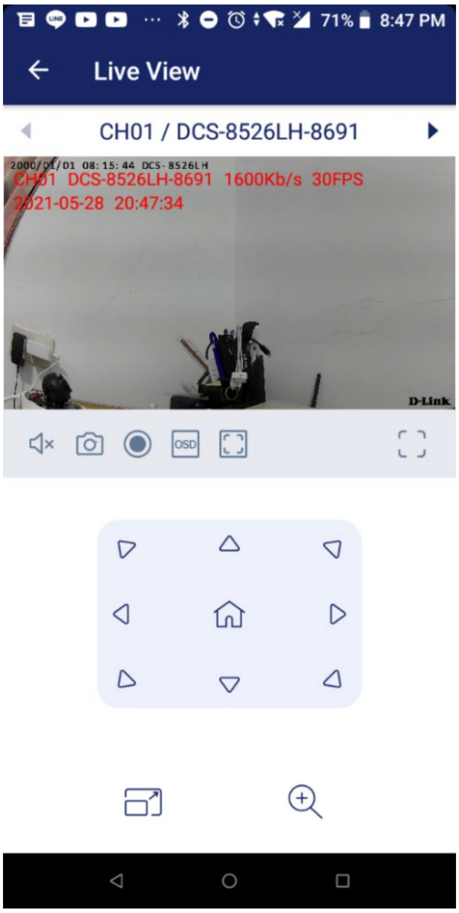


You can perform the following functions on all channels:

● **Manual Recording**	Start or stop recording the live video.
OSD **Show/Hide OSD**	Show or hide the on-screen display of camera information.

Standard/ Actual Size	Switch the display in standard or actual size.

To control each channel, tap a channel.



The following table shows the controls you can perform on each channel:

Sound	Enable or disable output audio with the camera's microphone support.
Manual Recording	Start recording or stop recording the live video.
Standard/Actual Size	Display the live view in standard or actual size.
Show/Hide OSD	Show or hide the on-screen display of camera information.
Snapshot	Take a snapshot of the live view image and store in your mobile device.
Zoom in/out	Zoom in or out with the camera's PTZ support. You can also control the camera len's movement with the arrows of the control pad.

Video Quality	Switch between low and high video quality. Please refer to the video profiles settings for exact video quality parameters. Go to **Camera Surveillance** module of the Hub, select **Camera** in the left pane and click a network camera to display its settings page, then select the **Image** tab.

To browse the main menu, swipe right on the Home screen. The main menu allows you to manage the devices or obtain more information on the app:

Add Device	Add a device to the list. Note that only users with the **Root Admin** or **System Admin** role can access the camera list on the device. The app will scan for available devices in the network.
Sort Device	Drag the device and place it in the desired order of the list
Security	Enable fingerprint to access Nuclias Protect without entering your username and password for security purposes.
About	Shows the information of the app including its version, date of release, privacy policy and terms of use.

Troubleshooting

The Troubleshooting section provides methods for overcoming problems and fundamental operation information.

The Live View is not working if it is accessed from the Safari browser on macOS using IPv6.

Here are some tips to help you solve disconnected Live View.

Use IPv4 addressing method

This problem occurs only with cameras using IPv6 address scheme. Connect to a camera using an IPv4 address instead.

Enable "NSURLSession Websocket"

To enable NSURLSession WebSocket:

1. Make sure that your Safari version is 14.0 and above. (Go to **Safari > About Safari**.)
2. Open the Safari® browser. Choose **Safari > Preferences**, click **Advanced**, then select **Show Develop menu in menu bar**.
3. Choose **Safari > Develop** in the menu bar, then select **Experimental Features** and click **NSURLSession WebSocket** to enable it.

What is the storage requirement for DNH-200?

The DNH-200 supports the installation of one 2.5-inch solid-state drive (SSD) or Hard disk drive (HDD) with at least 128GB capacity.
Suggest to use Conventional Magnetic Recording (CMR) hard disk or Solid State Disk (SSD) for video recording.