

NUCLIAS CONNECT

User Manual

V 1.10

Table of Contents

Product Overview	3
Recommended System Requirements	3
Software Installation.....	4
Downloading Nuclias Connect Package	4
Nuclias Connect for Windows	5
Nuclias Connect for Linux.....	5
Windows Installation.....	7
Nuclias Connect Server Installation	7
Linux OS Installation.....	18
Launching Nuclias Connect	26
Nuclias Connect App.....	28
Nuclias Connect Configuration.....	40
Dashboard.....	41
Monitor.....	42
Access Point	42
Switch.....	46
Topology.....	62
Topology.....	63
Floor Plan.....	65
Configuration.....	66
Create Profile	66
Profile Settings.....	69
Firmware Upgrade.....	97
SSL Certificate	98
Payment Gateway.....	99
Report	100
Access Point	100
Switch.....	104
Log	107
Device Syslog	107
System Event Log.....	108
Device Log.....	109
Audit Log	110
Alerts	111
System	112
Device Management	112
User Management.....	113
Settings	115
Resources.....	124
About	125

Product Overview

D-Link Nuclias Connect is a versatile, convenient software solution for administrators to manage wireless devices throughout the network from a central point.

Recommended System Requirements

Scale Size	Larger Scale	Smaller Scale
Maximum Managed Devices	1500 devices	100 devices
Recommended CPU	8th Generation Intel® Core™, i7 Processors	Intel® Core™ i5 Processors, 3.2 GHz
Recommended RAM	24G DDR3	8G DDR3
Recommended Storage	4TB	2TB
Ethernet NIC¹	Gigabit Ethernet Card	Gigabit Ethernet Card
Monitor Resolution	1080P	1080P
Platform (Windows)	Windows 10 Server 2019 (64-bit)	Windows 10 Professional (64-bit)
Platform (Linux²)	Ubuntu CentOS 7	Ubuntu CentOS 7
Browser for Nuclias Connect Management	Edge, Chrome, Safari	Edge, Chrome, Safari
Recommended Uplink Bandwidth	20 Mbps for larger scale	10 Mbps for smaller scale

¹ Recommended uplink bandwidth: 20 Mbps for larger scale, 10 Mbps for smaller scale.

² Docker and Docker Compose toolsets are required for the installation in a Linux platform.

Software Installation

In the following section, we'll discuss the software that needs to be installed to successfully run the Nuclias Connect application.

The following software applications must be installed in the following order:

- The **Nuclias Connect Server** application. This is the main application that will be responsible for the day-to-day wireless network management and maintenance tasks. For more information, refer to "Nuclias Connect Server Installation" on page 7 and "Nuclias Connect Configuration" on page 40.
- The **Nuclias Connect App**. This App is a wireless access point management tool that allows for easy configuration and deployment of standalone AP devices and the management of multiple sites and networks. For more information, refer to "Nuclias Connect App" on page 28.

Downloading Nuclias Connect Package

Access to the Nuclias Connect packages for Windows and Linux is available at <https://download.nuclias.com>.

Through this page, you can generate the command for installing through Docker Hub for Linux OS or download the compressed installation file for both Linux and Windows OS. See "Recommended System Requirements" on page 3 for system requirements and details. The Download Nuclias website will appear as per the following figure.



Download Nuclias Connect for Windows

Windows10 / Windows server 2016 (64 bit)

Download file

Download Nuclias Connect for Linux

- Ubuntu Cosmic 18.10 / Bionic 18.04 (LTS) / Xenial 16.04 (LTS)
- CentOS 7

Docker Hub Installation

You may enter your preferred MongoDB username and password to generate the specific command for setup.

Username :	<input type="text"/>	Password :	<input type="password"/>	<input type="button" value="Generate command"/>
Command :	<input type="text" value="curl -L https://raw.githubusercontent.com/nuclias-connect/connect/dev/install.sh sudo sh -s username password"/>			<input type="button" value="Copy command"/>

Tarball Installation

Direct URL :	<input type="text" value="https://gitlab.com/Nuclias/connect/raw/master/packages/Linux/nuclias_connect_1.0.0.tar.gz"/>	<input type="button" value="Copy URL"/>
		<input type="button" value="Download file"/>

Software Installation

Nuclias Connect for Windows

Go to <https://download.nuclias.com> to download the installation package for Windows OS.

From the menu, locate the section labeled **Download Nuclias Connect for Windows**.

Click **Download file** to begin downloading the installation package.



Download Nuclias Connect for Windows

Windows10 / Windows server 2016 (64 bit)

Download file

Save the file to a local directory. Take note of the location for installation.

Once the download is complete, you can begin the installation. See "Windows Installation" on page 7 for more details.

Nuclias Connect for Linux

Nuclias Connect is available for Linux and can be installed using Docker Hub or Tarball. See below on how to obtain the correct command that can be used in Linux for either Docker Hub or Tarball.

Go to <https://download.nuclias.com> to obtain the Linux command.

From the menu, locate the section labeled **Download Nuclias Connect for Linux**.

Docker Hub Installation

A specific command line can be downloaded from the Nuclias Connect download website.

From the menu, locate the section labeled Docker Hub Installation.

In the **Username** and **Password** fields, specify the preferred variables to associate with MongoDB.

Click **Generate Command** to get the command line.

Download Nuclias Connect for Linux

- Ubuntu Cosmic 18.10 / Bionic 18.04 (LTS) / Xenial 16.04 (LTS)
- CentOS 7

Docker Hub Installation

You may enter your preferred MongoDB username and password to generate the specific command for setup.

Username :	<input type="text"/>	Password :	<input type="text"/>	<input type="button" value="Generate command"/>
Command :	<pre>curl -L https://raw.githubusercontent.com/nuclias-connect/connect/dev/install.sh sudo sh -s username password</pre>			<input type="button" value="Copy command"/>

Tarball Installation

Direct URL :	<input type="text" value="https://gitlab.com/Nuclias/connect/raw/master/packages/Linux/nuclias_connect_1.0.0.tar.gz"/>	<input type="button" value="Copy URL"/>
		<input type="button" value="Download file"/>

Click on the **Copy command**.

Username :	<input type="text"/>	Password :	<input type="text"/>	<input type="button" value="Generate command"/>
Command :	<pre>curl -L https://raw.githubusercontent.com/nuclias-connect/connect/dev/install.sh sudo sh -s username password</pre>			<input type="button" value="Copy command"/>

The command is now copied to the clipboard and can be used during the Linux Docker Hub installation.

Software Installation

Tarball File Installation

Nuclias Connect is also available for Linux through a compressed tarball file. Use the following information to obtain the correct Nuclias Connect package.

Go to <https://download.nuclias.com>.

From the menu, locate the section labeled **Tarball Installation**.

In the Direct URL field, the latest tarball package will be listed.

Click **Copy URL** to copy the link to the clipboard or **Download file** to begin downloading the compressed tarball file.

Tarball Installation

Direct URL :

Copy URL

Download file

Save file to a local directory. Take note of the location for installation.

Once the download is complete, you can begin the installation.

Software Installation

Nuclias Connect Server Installation

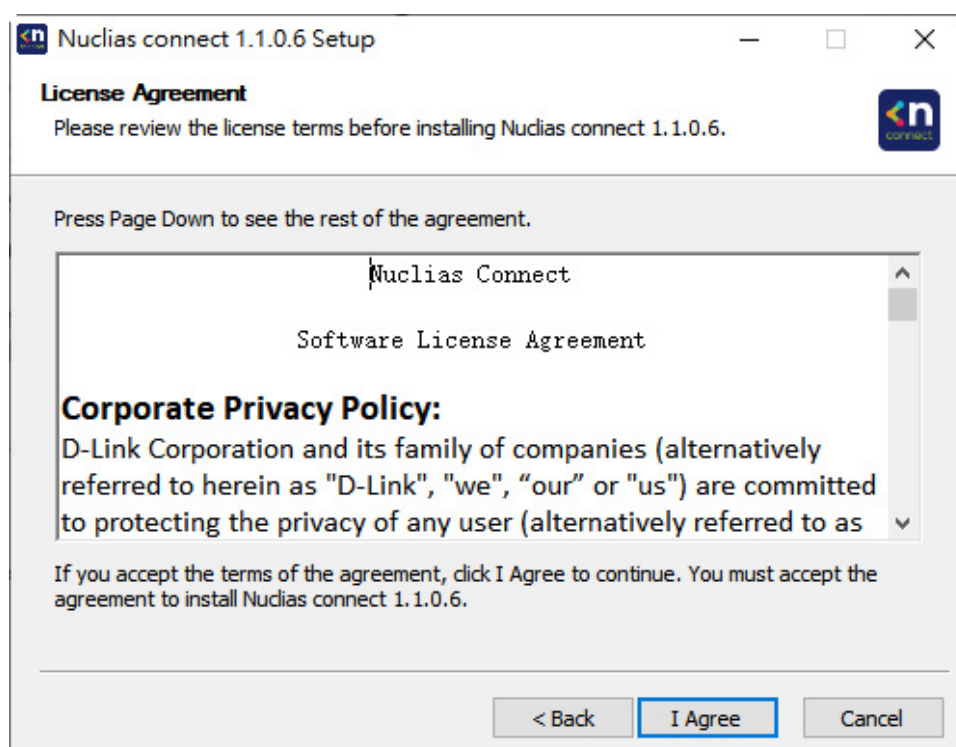
Windows Installation

Before you begin this procedure, download the latest Nuclias Connect package. See the following for further information. Locate the Nuclias Connect package and run the file to start the installation process. A Welcome window will appear.

Click the **Next >** button to continue. Click the **Cancel** button to stop and exit the installation.



The License Agreement window will appear. Before installing, review the license terms. Once accepted, click the **I Agree** button to continue.

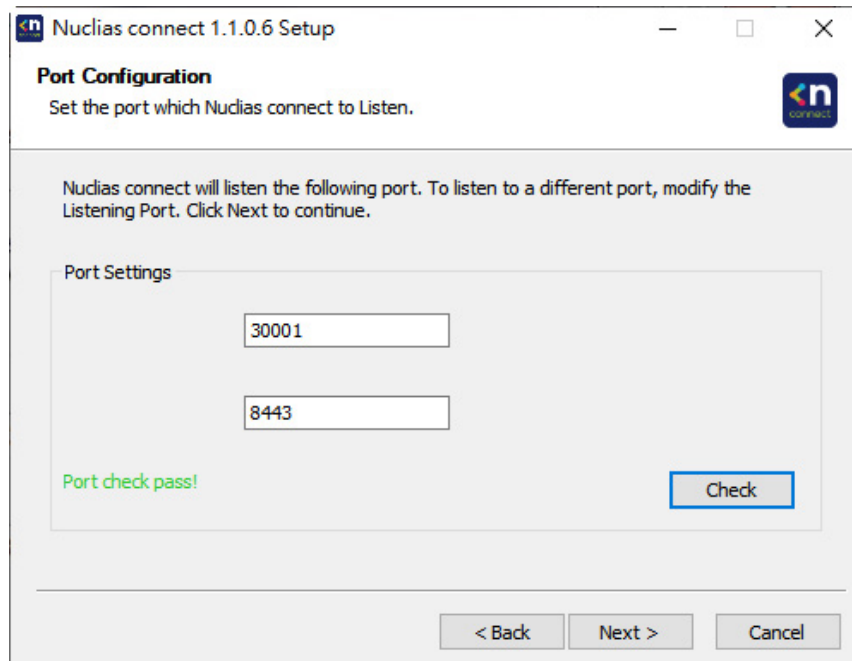


Software Installation Linux OS Installation

Nuclias Connect Server Installation

In this window, enter the **Web Port** (default: 30001) and **CoreServer Port** (default: 8443) settings as required. These ports are used for multiple access point connections and must be specified in this window. Use the default settings if the ports are accessible.

Click the **< Back** button to return to the previous step. Click the **Next >** button to continue to the next step. Click the **Cancel** button to stop and exit the installation.

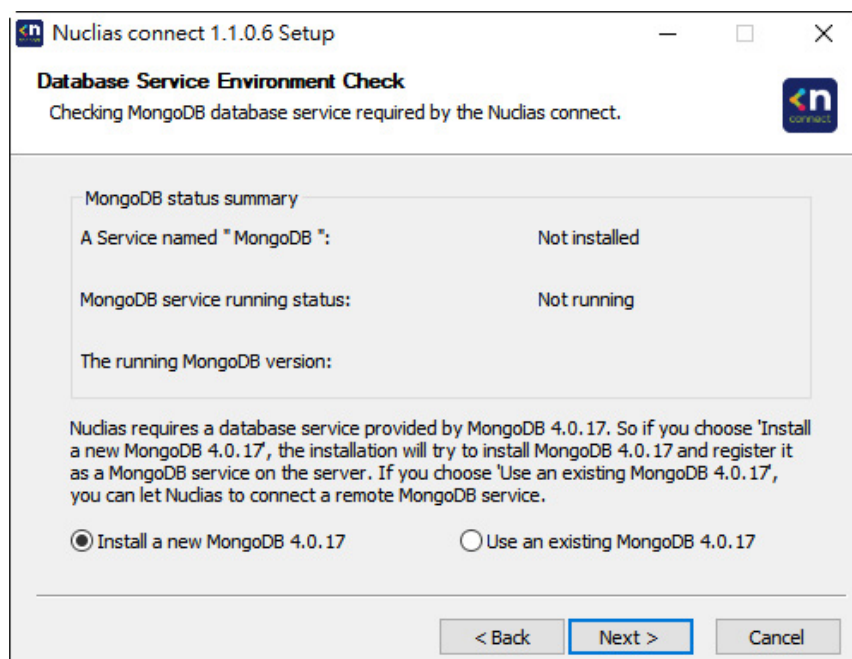


The screenshot shows the 'Port Configuration' window of the Nuclias connect 1.1.0.6 Setup. The window title is 'Nuclias connect 1.1.0.6 Setup'. The subtitle is 'Port Configuration'. The main text says 'Set the port which Nuclias connect to Listen.' Below this, it states 'Nuclias connect will listen the following port. To listen to a different port, modify the Listening Port. Click Next to continue.' There are two input fields: the first contains '30001' and the second contains '8443'. Below the fields, it says 'Port check pass!' in green. A 'Check' button is on the right. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

The **Database Service Environment Check** window is displayed. Click **Check** to perform a systems check for the required MongoDB database services. A report is visible in the MongoDB status summary field displaying the MongoDB version and status.

Nuclias Connect requires a database service to function properly. Support for existing MongoDB on the server or remotely is available by selecting the related radio button, see the following image. By selecting a new install instance, mongoDB is registered as a service on the server.

Click the **< Back** button to return to the previous step. Click the **Next >** button to continue to the next step. Click the **Cancel** button to stop and exit the installation.



The screenshot shows the 'Database Service Environment Check' window of the Nuclias connect 1.1.0.6 Setup. The window title is 'Nuclias connect 1.1.0.6 Setup'. The subtitle is 'Database Service Environment Check'. The main text says 'Checking MongoDB database service required by the Nuclias connect.' Below this, there is a 'MongoDB status summary' section with the following information: 'A Service named "MongoDB ": Not installed', 'MongoDB service running status: Not running', and 'The running MongoDB version:'. Below this, there is a text block: 'Nuclias requires a database service provided by MongoDB 4.0.17. So if you choose 'Install a new MongoDB 4.0.17', the installation will try to install MongoDB 4.0.17 and register it as a MongoDB service on the server. If you choose 'Use an existing MongoDB 4.0.17', you can let Nuclias to connect a remote MongoDB service.' At the bottom, there are two radio buttons: 'Install a new MongoDB 4.0.17' (selected) and 'Use an existing MongoDB 4.0.17'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

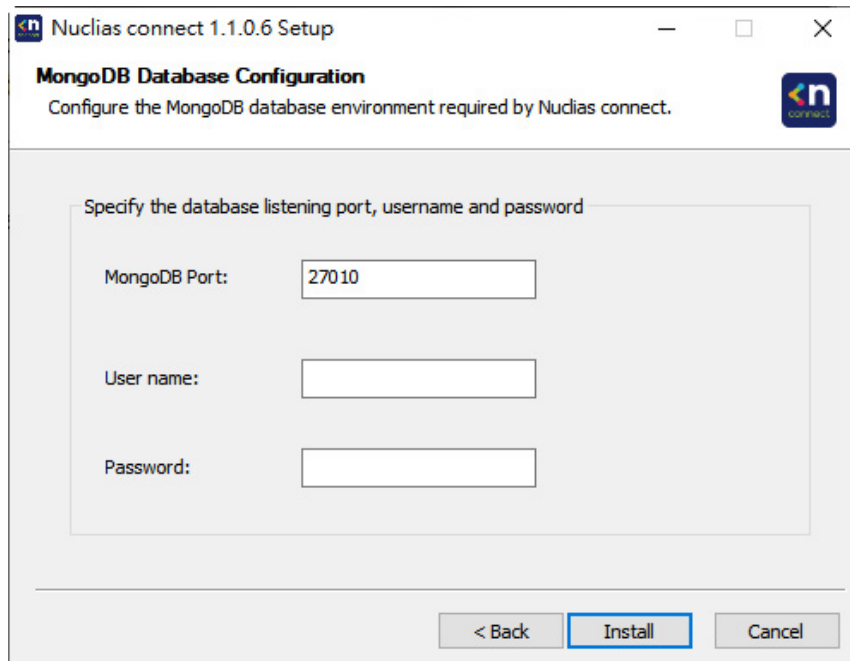
Software Installation

Windows Installation

Nuclias Connect Server Installation

The **MongoDB Database Configuration** window will appear. In this window, specify the MongoDB listening port (default: 27010), the user name and password for the **Postgres** database associated with this application.

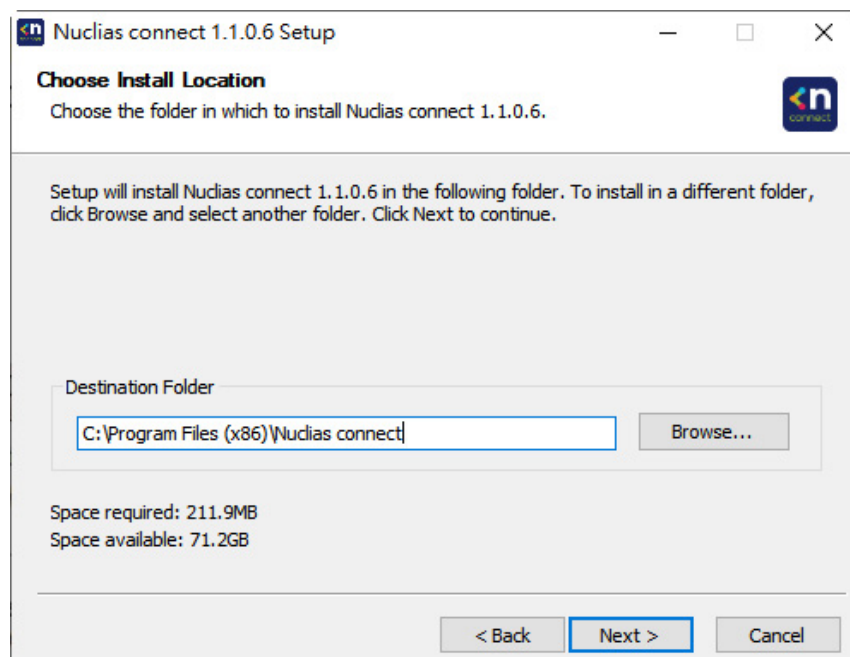
Click the **< Back** button to return to the previous step. Click the **Next >** button to continue to the next step. Click the **Cancel** button to stop and exit the installation.



The firewall on the computer might block the Apache HTTP Server application. If the server uses Windows Firewall, a security alert message will appear. Click the **Allow Access** button to allow this application to communicate with the network.

The **Choose Destination Location** window will appear. To install Nuclias Connect in a different folder or on a different drive, click the **Browse...** button and specify a target folder.

Click the **< Back** button to return to the previous step. Click the **Next >** button to continue to the next step. Click the **Cancel** button to stop and exit the installation.

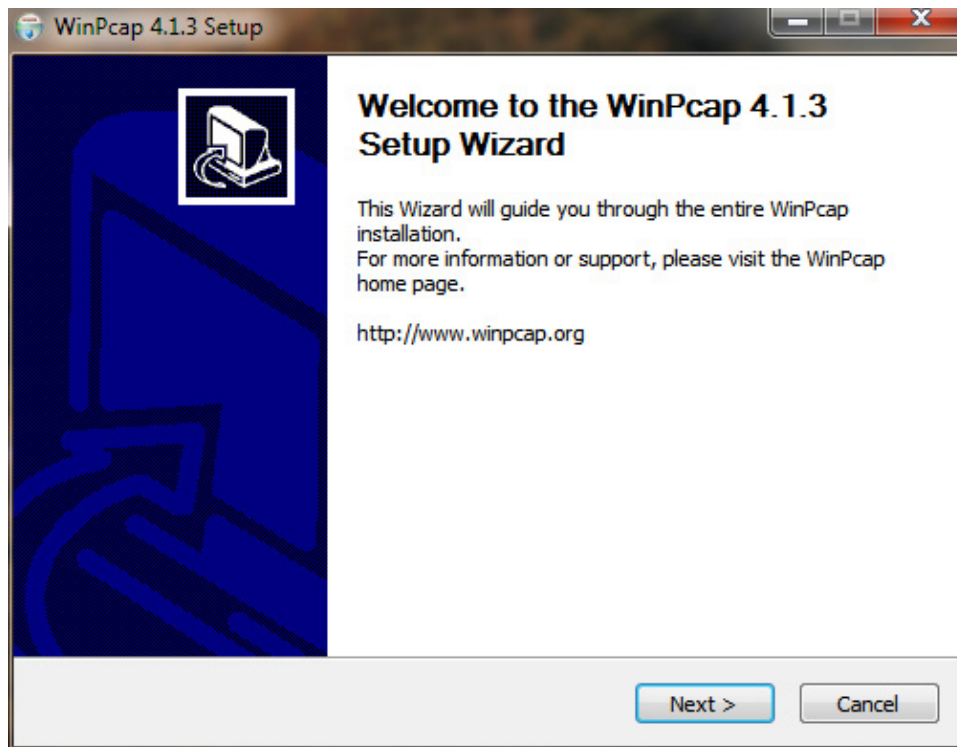


Software Installation Windows Installation

Nuclias Connect Server Installation

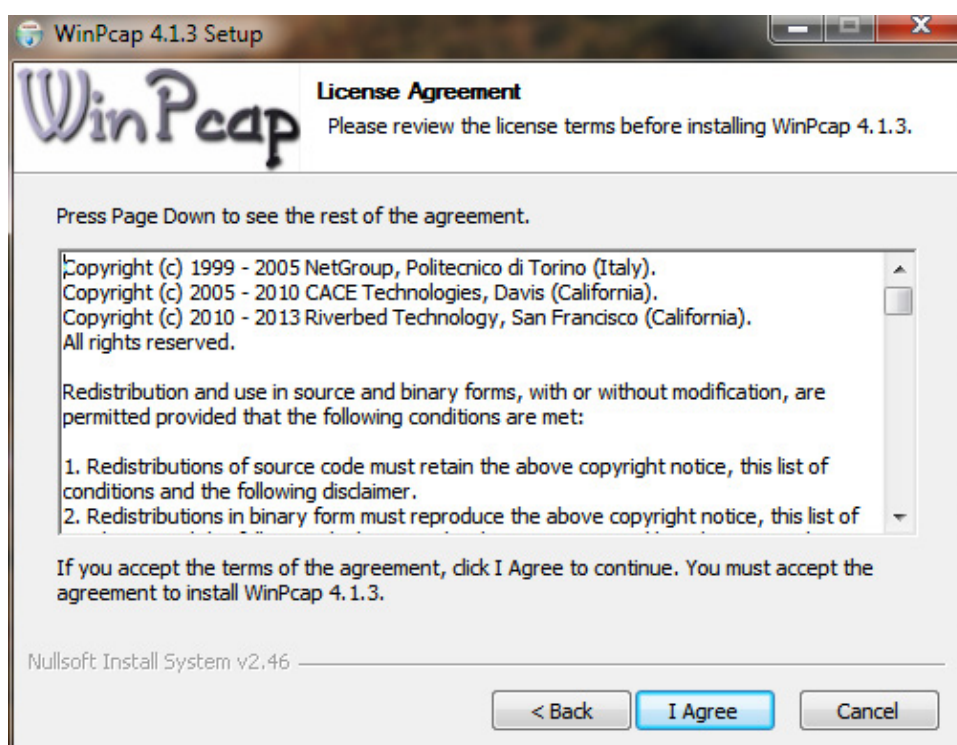
The **WinPcap Setup Wizard** window will appear. The WinPcap installation allows link-layer network access in Windows environments, allowing applications to capture and transmit network packets bypassing the protocol stack, this includes kernel-level packet filtering, a network statistics engine and support for remote packet capture.

Click the **Next >** button to initiate the Setup Wizard. Click the **Cancel** button to stop and exit the installation.



The **License Agreement** window will appear. Review the license terms before installing WinPcap. Once the agreement is accepted, click **I Agree** to continue.

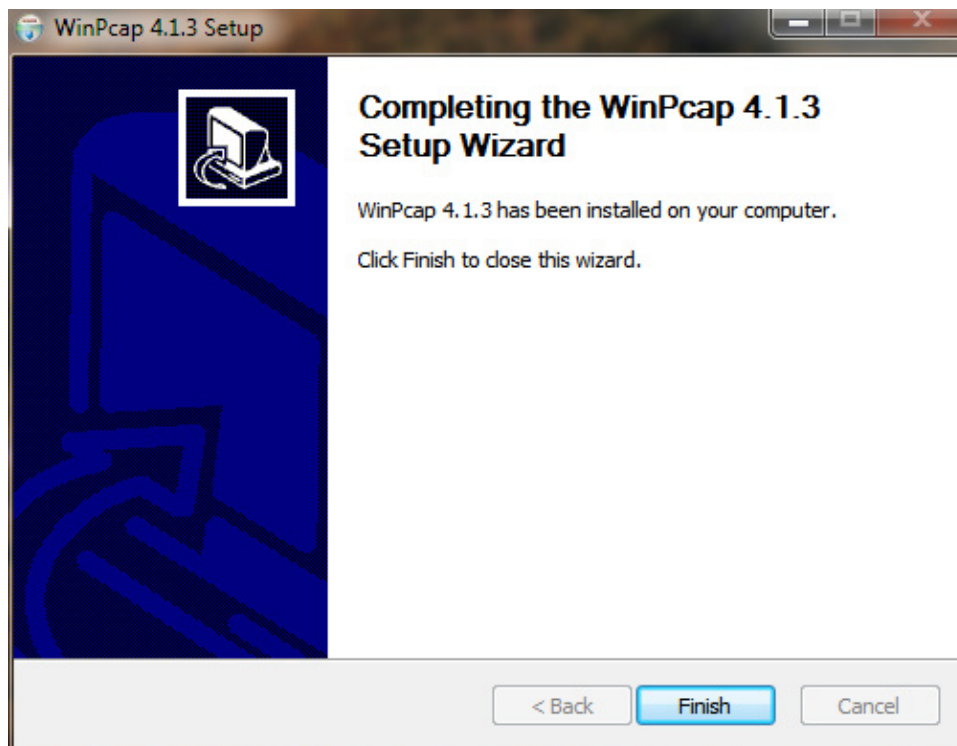
Click the **< Back** button to return to the previous step. Click the **Cancel** button to stop and exit the installation.



Software Installation Windows Installation

Nuclias Connect Server Installation

The **Completing ... Setup Wizard** window will appear. Click the **Finish** button to complete and exit the installation wizard.



Once the WinPcap tool has been installed, the Nuclias Connect setup wizard will continue with the installation.

A Windows Security Alert may display a warning that certain features are blocked from installation, such as Server-side JavaScript. If the pop-up window appears, select network settings—in the following figure, select **Private networks** (best suited to access the firewall) and click **Allow access**. Otherwise, click **Cancel** to stop the installation process. See the following figure for further information.



Software Installation

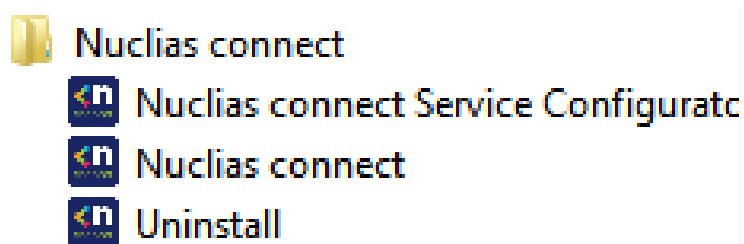
Windows Installation

Nuclias Connect Server Installation

The **Completing the D-Link Nuclias Connect Setup** window will appear. Click the **Finish** button to complete and exit the installation wizard.



After the installation, the **Nuclias Connect Service Configurator**, **Nuclias Connect**, and **Uninstall** shortcuts will appear in the programs list as follows:



Software Installation

Windows Installation

Nuclias Connect Server Installation

Running the Nuclias Connect Server

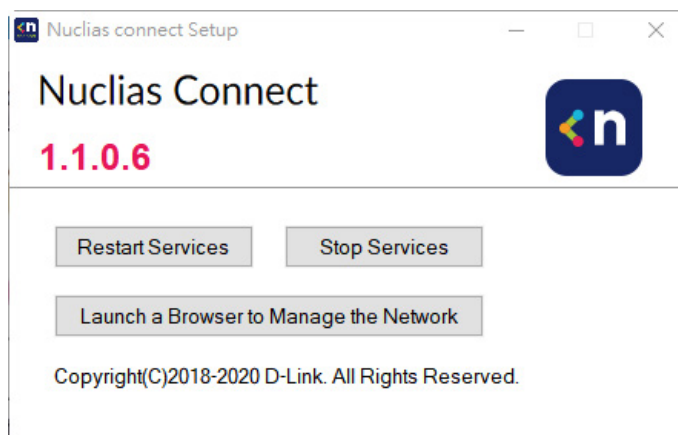
This section describes how to run the Nuclias Connect Server application. After the installation is completed, the following applications will appear on the Programs listing.

NOTE: The following instructions were written under the Windows 7 operating system, screenshots and wording may vary depending on your operating system.

From the desktop, navigate to **Start > All Programs > Nuclias Connect** and click  Nuclias connect Service Configurator  Nuclias connect to open the Nuclias Connect setup. The Configuration window will appear as follows.

The **Menu** contains the **Start/Stop Services** and **Launch** access buttons. Before you can manage Nuclias Connect, its Services must first be enabled. Use the **Restart Services** button to enable Nuclias server or **Stop** to disable the server services.

The Nuclias Connect configuration interface is accessible through a browser window. Click **Launch a Browser to Manage the Network** to open a default browser window.



Logging in for the First Time

Nuclias Connect Online Registration

Nuclias Connect provides a 30-days Free Trial. You may continue the use by registering a Nuclias account at **register.nuclias.com** or redirected from the Settings on Nuclias Connect. The Nuclias account can also login to D-Link's Nuclias Cloud Platform if you have Cloud-managed devices. If there is no registered account, click **No Account? Register now** to create valid credentials.

Software Installation Windows Installation

Nuclias Connect Server Installation

Once the registration process is initialized, a new browser window will be opened. The server registration page will appear. There are three steps in the registration process. The first step is as follows.

Step 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.

The screenshot shows the first step of the registration process. At the top, there is a progress bar with three circles; the first circle is filled green, indicating the current step. Below the progress bar, the text reads "STEP 1" and "Select server region and country:". The main form area has the Nuclias logo at the top, followed by a message: "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." Below this message are two dropdown menus labeled "Server region" and "Country". At the bottom of the form is a "Next" button and a link that says "Already have an account? Log in".

NOTE: If you already have an account, you may login directly.

Once the region and country are entered, you will see the user, organization, and site page. Enter the required information and agree to the Terms of Use and Privacy agreement to enable the account creation button.

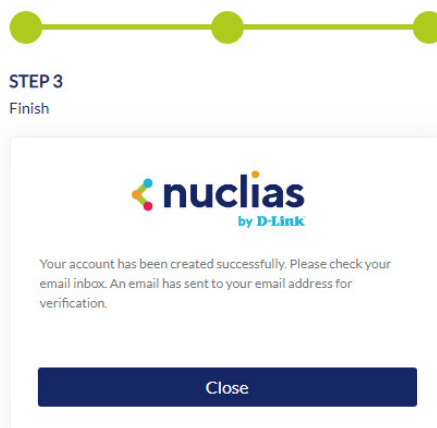
Click **Create Account** to continue.

The screenshot shows the second step of the registration process. At the top, the progress bar has the second circle filled green. Below it, the text reads "STEP 2" and "Create your user, organization and site:". The form contains several input fields: an email field (pre-filled with "novascriptor@gmail.com"), a "D-Link:" field, two password fields (each with a strength indicator and an eye icon to toggle visibility), a "D-Link Test" field, a "Taiwan" dropdown menu, an "Asia/Taipei(UTC+08:00, DST)" dropdown menu, and a "No.1 Street Name, City Name, State, Country, ZIP" field. At the bottom, there is a checkbox labeled "I have read and agree to the Terms of use and Privacy" and a dark blue "Create account" button.

Software Installation Windows Installation

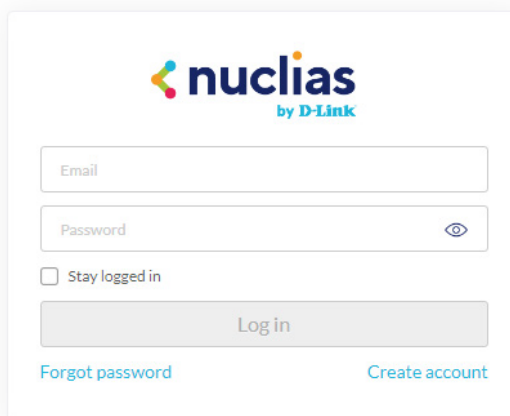
Nuclias Connect Server Installation

If the registration is successful, the Finish page will appear. 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.



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

You will be redirected to the Login page. You may skip this step if you do not have Nuclias Cloud-enabled devices.

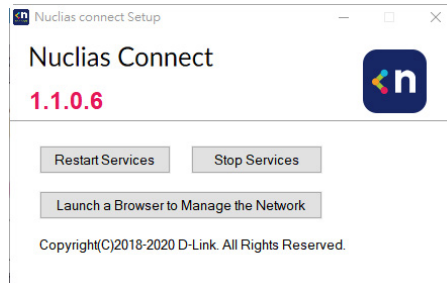


Software Installation Windows Installation

Nuclias Connect Server Installation

Launch Nuclias Connect

Nuclias Connect features multiple login options from using the Nuclias Connect installed software on a local computer to a browser on a remote computer (Edge or Chrome is recommended). Open the browser and enter the **IP address** or **Domain Name** of the host computer running the Nuclias server (for example, <https://192.168.10.1:30001> or <https://domain-name.com>).



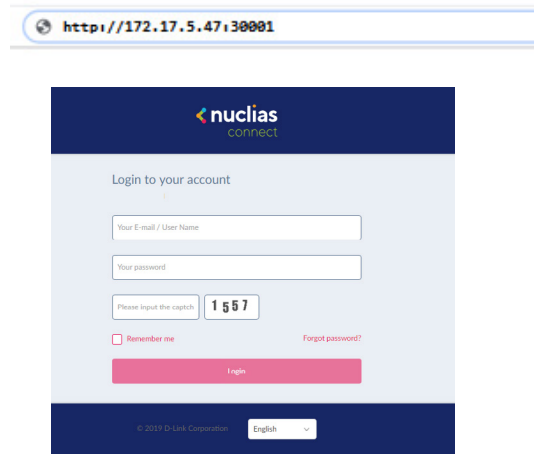
On the locally installed software, use the Nuclias Service Configurator or the Nuclias Connect shortcuts to open the interface in a browser.

From the desktop, navigate to **Start > All Programs > Nuclias Connect** and click on  **Nuclias connect Service Configurator** to open the Nuclias Connect Configuration window.

From the Nuclias Connect window, click **Launch a Browser to Manage the Network**. The default browser will be launched to show the Nuclias Connect interface.

Alternatively, the interface is also accessible through the following:

From the desktop, navigate to **Start > All Programs > Nuclias Connect** and click on  **Nuclias connect** to open the default Web browser.

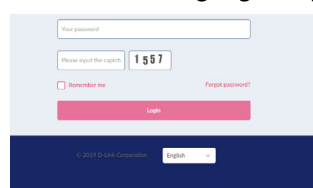


Enter the modified username and password in the respective fields.

Enter the Captcha code as shown on screen.

NOTE:

- The Remember me function saves the password entry for future use.
- The Forgot password function allows you to reset your password in the event that the current password is lost.
- The interface supports Multi-language options. Click the language drop-down menu to select a different language.

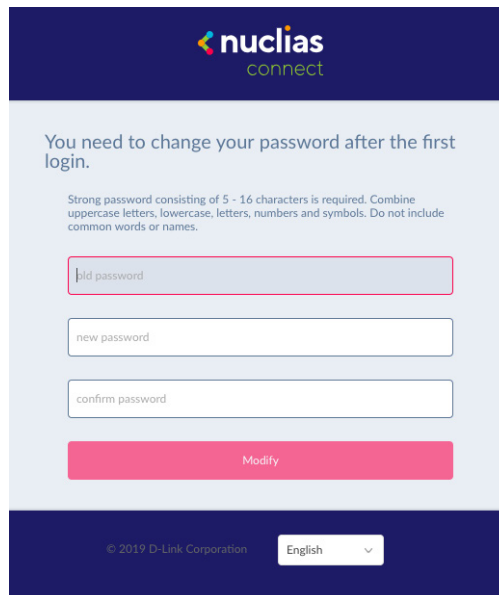


Software Installation Windows Installation

Nuclias Connect Server Installation

After the web browser opens and connects successfully to the server, a change-password dialog will appear. A change in the default password is required after the first login.

When assigning a password, it is recommended to use a strong password. The new password is required to be 5 - 16 characters in length. Mixing uppercase and lowercase characters along with numbers and symbols can help ensure stronger security.

The screenshot shows a web interface for changing a password. At the top is the 'nuclias connect' logo. Below it, a message states: 'You need to change your password after the first login.' This is followed by a note: 'Strong password consisting of 5 - 16 characters is required. Combine uppercase letters, lowercase, letters, numbers and symbols. Do not include common words or names.' There are three input fields: 'old password', 'new password', and 'confirm password'. Below these fields is a pink 'Modify' button. At the bottom of the page, there is a copyright notice '© 2019 D-Link Corporation' and a language dropdown menu set to 'English'.

NOTE: Do not include common words or names.

Enter the previous password in the **Old Password** field.

In the **New Password** field enter the new password.

Enter the same password in the **Confirm Password** field to verify the entry.

Click **Modify** to complete the process.

Upon logging in, the System Settings page will appear. In the event that the device access address or port have been changed, the Nuclias Connect Core server must be restarted. Complete the following settings page before continuing.

Software Installation

Nuclias Connect Server Installation

Linux OS Installation

There are two ways to install Nuclias Connect on Linux:

1. Docker Hub
2. Tarball – See “Tarball Installation (Option 2)” on page 22.

Docker Hub Installation

Preparing the Software Environment

Before installing the Nuclias Connect, we must first set up the environment. The steps outlined in the following information are provided as a guide to complete the installation task. Please follow the guide for installing Nuclias Connect with Docker Hub in the following order before continuing on to the next item on the list.

- Install Docker
- Install Docker Compose
- Install Nuclias Connect via the terminal

Install Docker

Docker is available in two editions: Community Edition (CE) and Enterprise Edition (EE). In this section, Docker CE is used. For more information about Docker CE, see Docker Enterprise Edition.

To install Docker, you will need a 64-bit OS and a kernel at 3.10 or newer. Kernels older than 3.10 do not have the necessary features required to run containers; data loss and kernel panics occur frequently under certain conditions.

Check your current Linux version by using the `uname -r` command.

Prerequisites

To install Docker CE, you need the 64-bit version of one of these Ubuntu versions, or CentOS 7:

- Cosmic 18.10
- Bionic 18.04 (LTS)
- Xenial 16.04 (LTS)
- User name with sudo privileges

Docker CE is supported on x86_64 (or amd64), armhf, arm64, s390x (IBM Z), and ppc64le (IBM Power) architectures.

Uninstalling Previous Versions of Docker

It is recommended to uninstall any previous versions of the Docker software before proceeding. Use the following command to uninstall.

```
$ sudo apt-get remove docker docker-engine docker.io docker-ce
```

Once the previous version is removed, the latest version of the Docker software can be installed.

Software Installation

Linux OS Installation

Nuclias Connect Server Installation

Installing Docker

Installing Docker is performed through the terminal window by using the following command:

```
$ sudo apt-get install docker.io
```

Once the command is initiated, the following results are displayed.

```
[sudo] password for dlink:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  bridge-utils cgroupfs-mount containerd docker.io pigz runc Ubuntu-fan
0 upgraded, 7 newly installed, 0 to remove and 63 not upgraded.
Need to get 0 B/52.2 MB of archives.
After this operation, 257 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

To finalize the installation, enter Y.

```
Do you want to continue? [Y/n] Y
```

The following results are displayed.

```
Preconfiguring packages ...
Selecting previously unselected package pigz.
(Reading database ... 175976 files and directories currently installed.)
Preparing to unpack .../0-pigz_2.4-1_amd64.deb ...
Unpacking pigz (2.4-1) ...
Selecting previously unselected package bridge-utils.
Preparing to unpack .../1-bridge-utils_1.6-2ubuntu1_amd64.deb ...
Unpacking bridge-utils (1.6-2ubuntu1) ...
Selecting previously unselected package cgroupfs-mount.
Preparing to unpack .../2-cgroupfs-mount_1.4_all.deb ...
Unpacking cgroupfs-mount (1.4) ...
Selecting previously unselected package runc.
Preparing to unpack .../3-runc_1.0.0~rc7+git20190403.029124da-0ubuntu1_adm64.deb ...
Unpacking runc (1.0.0~rc7+git20190403.029124da-0ubuntu1) ...
Selecting previously unselected package containerd.
Preparing to unpack .../4-containerd_1.2.6-0ubuntu1_amd64.deb ...
Unpacking containerd (1.2.6-0ubuntu1) ...
```

Software Installation

Linux OS Installation

Nuclias Connect Server Installation

```
Selecting
Preparing to unpack .../5-docker.io_18.09.5-0ubuntu1_amd64.deb ...
Unpacking docker.io (18.09.5-0ubuntu1) ...
Selecting previously unselected package Ubuntu-fan.
Preparing to unpack .../6-ubuntu-fan_0.12.12_all.deb ...
Unpacking Ubuntu-fan (0.12.12) ...
Setting up runc (1.0.0~rc7+git20190403.029124da-0ubuntu1) ...
Setting up pigz (2.4-1) ...
Setting up cgroupfs-mount (1.4) ...
Setting up containerd (1.2.6-0ubuntu1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/containerd.service/lib/systemd/system /
conatinerd.service.
Setting up Ubuntu-fan (0.12.12) ...
Created symlink /etc/systemd/system/multi-user.target.wants/Ubuntu-fan.service/lib/systemd/system /
Ubuntu-fan.service.
Setting up docker.io (18.09.4-0ubuntu1) ...
Adding group 'docker' (GID 130)
Done.
Created Symlink /etc/systemd/system/sockets.target.wants/docker.socket → /lib/systemd/system/docker.
socket.
Processing triggers for systemd (240-6ubuntu5) ...
Processing triggers for man-db (2.8.5-2) ...
```

After installing Docker, you need to configure Docker to start at boot so when the server is rebooted, Docker service will start automatically.

```
$ sudo systemctl enable docker
$ sudo systemctl start docker
```


Software Installation

Linux OS Installation

Nuclias Connect Server Installation

Install Docker Compose

Compose is available for the Windows or 64-bit Linux operating systems.

Prerequisites

Docker Engine must be installed prior to the installation of Compose.

- On Windows OS, Docker Compose is included in the desktop installation.
- On Linux OS, the Docker software for your specific OS must first be installed. Once installed, continue with the Compose installation process.

Installing Compose on Linux

On Linux, the Docker Compose binary can be downloaded from the Compose repository release page found on GitHub. See the following instructions.

Check the latest Docker Compose from Github at <https://github.com/docker/compose>.

```
$ sudo curl -L https://github.com/docker/compose/releases/download/1.23.1/docker-compose-`uname -s`-`uname -m` -o /usr/local/bin/docker-compose
```

NOTE: To install a different version of Compose, substitute the variable 1.23.1 with the preferred version of Compose.

Apply executable permissions to the aforementioned binary. See the following command:

```
$ sudo chmod +x /usr/local/bin/docker-compose
```

Once the installation is complete, verify it by checking its version number. See the following command to verify the version of the Compose binary.

```
$ sudo docker-compose -version
docker-compose version 1.23.1, build b02f1306
```

Docker Hub Installation (Option 1)

To generate the command for setting up Nuclias Connect through Docker Hub, go to <http://download.nuclias.com>. See "Nuclias Connect for Linux" on page 5. Below you can see an example of the command:

```
$ sudo curl -L https://raw.githubusercontent.com/nuclias-connect/connect/dev/install.sh |
sudo sh -s [mongo-username] [mongo-password]
```

This completes the Docker Hub installation of Nuclias Connect.

Software Installation

Linux OS Installation

Nuclias Connect Server Installation

Tarball Installation (Option 2)

Download Nuclias Connect for Linux to your system. You'll find the necessary information through the following link:

<https://download.nuclias.com>

Once the package is downloaded, make a note of its location for later use. In this example, the tar package (nuclias-connect.tar.gz) is downloaded in an archived form (GZ) to the desktop.

To extract the Nuclias Connect package:

From the desktop, press **Ctrl + Alt + T** to launch a terminal window.

From the terminal window, navigate to the location where the tar package is downloaded. In this example, the package is located on the desktop.

Enter the command to change directories.

```
$ cd Desktop
```

Once in the correct directory, use the **ls** command to view a list of available files in the directory.

To extract the package, type in the following command and the respective password for the user.

```
:~/Desktop$ sudo tar xvzf nuclias-connect.tar.gz
```

The command will extract the contents of the package. The following results will appear.

```
Nuclias_connect/  
Nuclias_connect/docker-compose.yml  
Nuclias_connect/config/  
Nuclias_connect/config/key/  
Nuclias_connect/config/key/ca-cert.pem  
Nuclias_connect/config/key/openssl.cnf  
Nuclias_connect/appconfig.json  
Nuclias_connect/images  
Nuclias_connect/images/mongo.tar  
Nuclias_connect/images/core.tar  
Nuclias_connect/images/web.tar  
Nuclias_connect/entrypoint-initdb.sh
```

The Nuclias Connect package is now extracted and ready for installation.

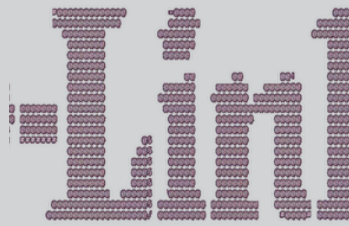
Navigate to the directory containing the init.sh shell file and type in the following command to initialize the Nuclias Connect package.

```
$ cd Desktop  
~/Desktop$ cd nuclias_connect  
~/Desktop/nuclias_connect$ sudo ./init.sh
```

Software Installation Linux OS Installation

Nuclias Connect Server Installation

The binary is executed and the following results will appear.



```
##### Welcome to Nuclias Connect #####
```

```
--  
--  
--
```

```
-e (1/11)---- check your system type ----
```

```
SYSTEM: Linux Ubuntu
```

```
-e check system finished
```

```
-e (2/11)---- check docker ----
```

```
Docker version 18.09.6, build 481bc77
```

```
-e docker installed
```

```
-e (3/11)---- check docker-compose ----
```

```
docker-compose version 1.23.1, build b02f1306
```

```
-e docker-compose installed
```

```
-e (4/11)---- check docker status ----
```

```
message: 2
```

```
-e docker service is running
```

```
-e (5/11)---- check core image ----
```

```
message: 2
```

```
-e core image is existed
```

```
-e (6/11)---- check web image ----
```

```
message: 2
```

```
-e web image is existed
```

```
-e (7/11)---- check mongo image ----
```

```
message: 2
```

```
-e mongo image is existed
```

```
-e (8/11)---- check web_port ----
```

```
message: 0
```

```
-e web_port is free
```

```
-e (9/11)---- check core_port ----
```

```
message: 0
```

Software Installation

Linux OS Installation

Nuclias Connect Server Installation

```
-e core_port is free
-e (11/11)---- check file and directory ----
-e check file finished
-e all check_job finished
-e Now initial set the database administrator account for Nuclias Connect, please confirm is
the first time set administrator account? [y/n]
```

As the initialization of the Nuclias Connect software takes place, a prompt will appear requesting to setup the database administrator account. If this is the first time using the database, you need to set a database administrator for the account. Otherwise, skip this step and go to Verifying the Installed Software.

Setup Database Profile

For first time users, you must first set the database administrator.. The following command describes the process.

In the Nuclias Connect initialization stage, the following prompt will appear.

```
-e Now initial set the database administrator account for Nuclias Connect, please confirm is
the first time set administrator account? [y/n]
```

Enter Y (Yes) to set the administrator account and password.

At the prompt, enter the administrator user name and the related password. In the following example, the variable admin is used for both instances.

```
User Name: admin
Password: admin
Confirm Password: admin
Creating volume "nuclias_connect_MONGO-DATA" with default driver
Creating mongo ... done
Creating nuclias_connect_core ... done
Creating nuclias_connect_web ... done
-e Nuclias services are running...
-- commands list -----
|                               |
-e | start: docker-compose up -d |
-e | stop:: docker-compose down  |
|                               |
-----
:~/Desktop/nuclias_connect$
```

With the Mongo DB, core, and web containers setup complete, the Nuclias Connect can now be launched using a web browser.

Software Installation

Linux OS Installation

Nuclias Connect Server Installation

Find Your Server IP Address

To connect to Nuclias Connect, follow the below informaton:

From the desktop, press **Ctrl + Alt + T** to launch a terminal window.

In the console, navigate to the directory containing the Nuclias Connect package. In the following example, the folder `nuclias_connect` is used to describe the location of the software.

```
$ cd Desktop
~/Desktop$ cd nuclias_connect
```

Enter the following command to obtain the defined IP address of the Nuclias Connect instance.

```
~/Desktop/nuclias_connect$ ip addr
```

The results will appear as follows. The IP address to use in a web browser is found below. In this instance, the address is 172.17.5.47, but yours may differ.

```
1: lo: <LOOPBACK, UP, LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group t glen 1000
   Link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
   Inet 127.0.0.1/8 scope host lo
       Valid_lft forever preferred_lft forever
   Inet6 ::1/128 scope host
       Valid_lft forever preferred_lft forever
2: enp3s0f2: <BROADCAST, MULTICAST, UP, LOWER_UP> mtu 1500 qdisc fq_code1 state up group
default qlen 1000
   link/ether 30:65:ec:25:be:3b brd ff:ff:ff:ff:ff:ff
   inet 172.17.5.47/24 brd 172.17.5.255 scope global dynamic noprefixroute ip3 sof2
       valid_lft 22085sec preferred_lft 22085sec
   inet6 fe80::c3a8:bcdb:6cda:4dc3/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: wlp2s0: <NO-CARRIER, BROADCAST, MULTICAST, UP> mtu 1500 qdisc noqueue state DOWN group
default qlen 1000
   link/ether a4:db:30:cb:36:0e brd ff:ff:ff:ff:ff:ff
4: docker0: <NO-CARRIER, BROADCAST, MULTICAST, UP> mtu 1500 qdisc noqueue state DOWN group
default qlen 1000
   link/ether 02:42:11:ff:39:9f brd ff:ff:ff:ff:ff:ff
   inet 172.18.0.1/16 brd 172.18.255.255 scope global docker0
       valid_lft forever preferred_lft forever
```

In the above interface session, the IP address (172.17.5.47) of the Nuclias Connect is identified. This is the IP address to use through a web browser to access the Nuclias Connect interface.

The Docker Hub installation process is now complete. The core containers necessary to access Nuclias Connect through a web browser are now in place. To access the Nuclias Connect interface, see "Launching Nuclias Connect" on page 26 for further details.

Software Installation

Launching Nuclias Connect

With the core containers setup and the MongoDB profiles configured, the Nuclias Connect can be accessed through a web browser.

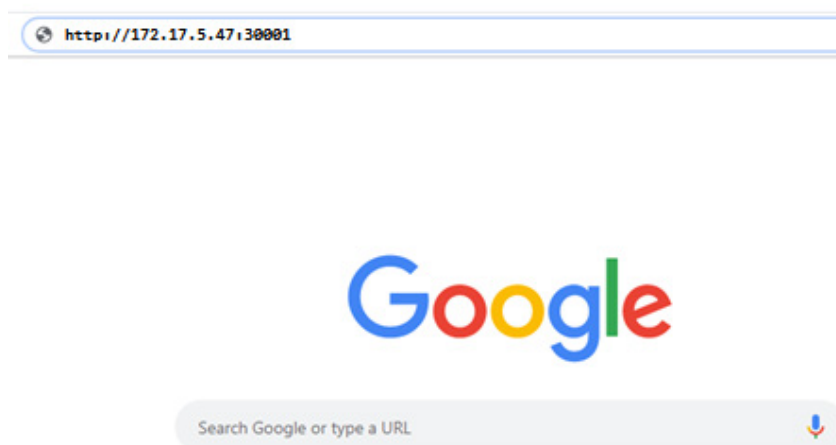
To obtain the defined IP address to access the Nuclias Connect through a web browser, see "" on page 245.

The default settings for the Nuclias Connect are as follows:

- Web port: 30001

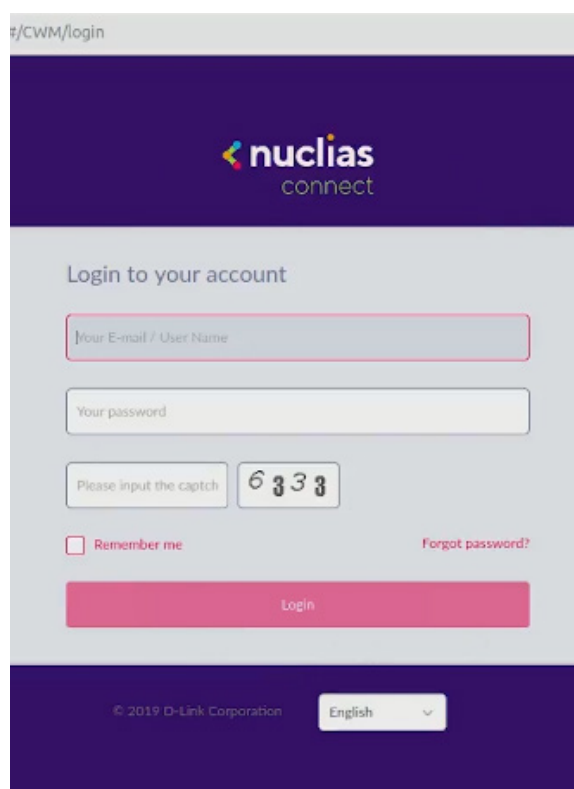
From the desktop, open a web browser.

In the address field, enter the aforementioned address to Nuclias Connect. In this instance, the IP address is 172.17.5.47:30001.



A privacy error message may appear when establishing a connection to the Nuclias Connect server. In this instance, click Proceed to 172.17.5.47 (unsafe) to open the Nuclias Connect portal.

The Nuclias Connect main login screen will appear as seen in the following figure.



Software Installation

Launching Nuclias Connect

The default username and password is admin. You will be required to change your password after the initial login. Enter the current password, then enter your new password and its confirmation in the appropriate fields.

Click **Modify** to continue.

After a successful password change, you will be required to provide installation information to continue the activation. Complete the requested information and click **Apply** to continue.

Parameter	Description
How are you using Nuclias Connect?	Personal Use or Customer
How many people in your department?	Options: <10, 10-50, 50-100, >100
How many APs do you plan to manage?	Options: <20, 20-50, 50-100, 100-500, >500
How many sites do you plan to manage?	Enter the number of sites to manage
Apply	Click to continue the activation process.

The activation process is now complete. Click **OK** to finalize the process.


Software Installation

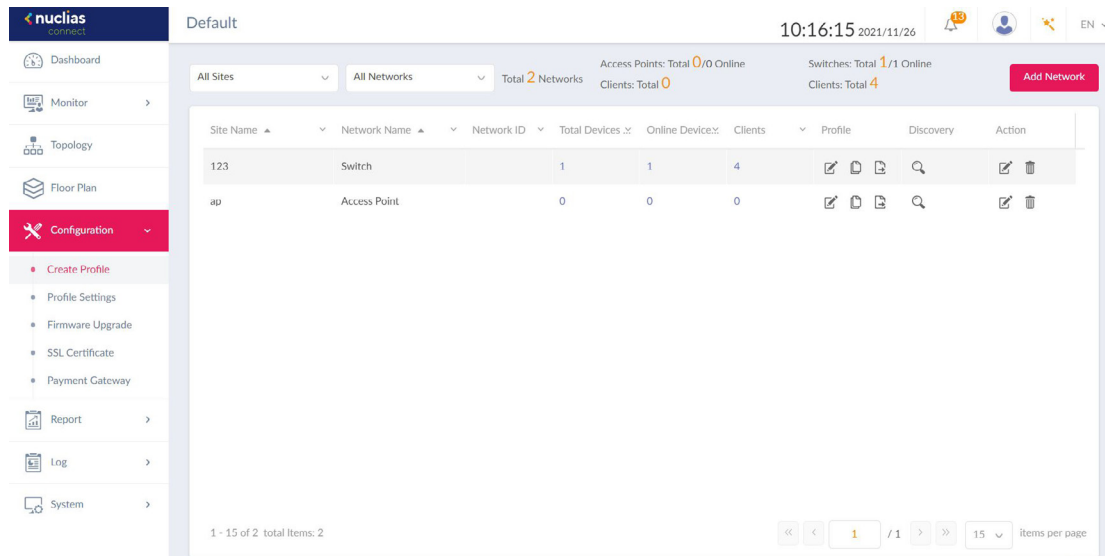
Nuclias Connect App

Through the use of 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 Nuclias server for managing connected APs. Additional information explaining the functionality of the Nuclias Connect App is also included.

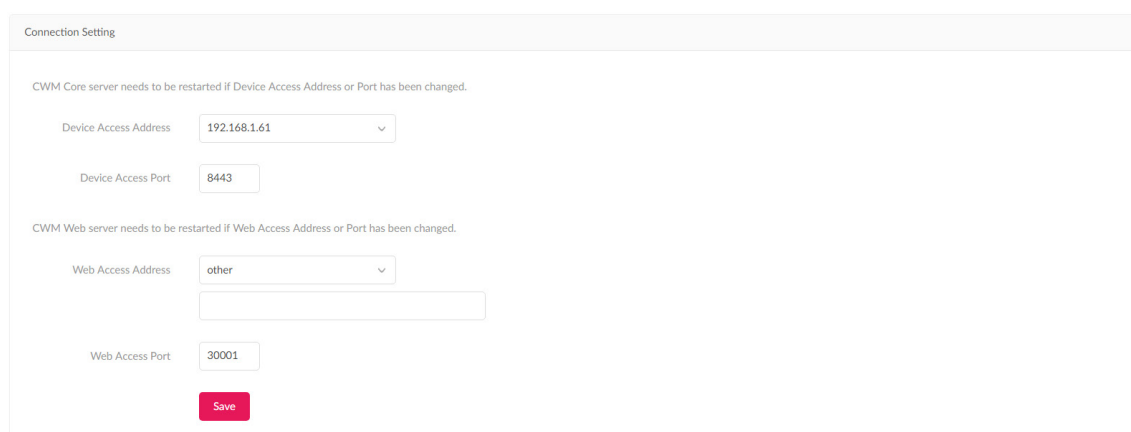
Export Network Profiles

To add new access points to Nuclias Connect, you must first export the required network profile from Nuclias. The network profile contains the authentication key and the IP address of the controller. Navigate to **Configuration > Create Profile** and click  to export the network profile to your computer.



Site Name	Network Name	Network ID	Total Devices	Online Devices	Clients	Profile	Discovery	Action
123	Switch	1	1	1	4			
ap	Access Point	0	0	0	0			

When switches or access points are located on a public network and you are accessing Nuclias Connect remotely, you must ensure that Nuclias Connect uses a public IP address or domain name. To verify Nuclias Connect's IP address, go to **System > Settings > Connection** and check the **Device Access Address** field.



Connection Setting

CWM Core server needs to be restarted if Device Access Address or Port has been changed.

Device Access Address: 192.168.1.61

Device Access Port: 8443

CWM Web server needs to be restarted if Web Access Address or Port has been changed.

Web Access Address: other

Web Access Port: 30001

Save

Software Installation

Nuclias Connect App

Discover and Configure APs Using the Nuclias Connect App

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

NOTE:

- The Nuclias Connect App cannot discover switches or access points located on Layer 3 networks.
- Before attempting to import a network profile, ensure that you have access to the Nuclias Connect controller.

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 Nuclias Connect controller.
- **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 (iOS). Tap on Quick Setup to start the setup process.

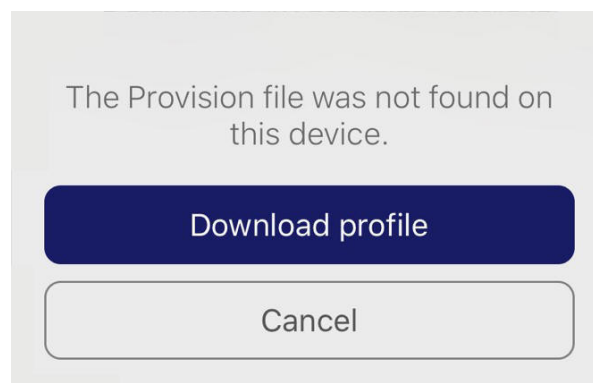
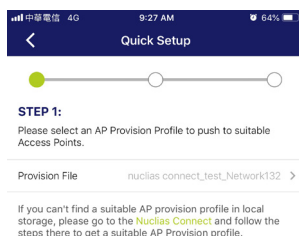


The next step is to select an AP provision profile. The profile is used to push the selected APs. Tap **Quick Setup** to begin the deployment of a standalone AP to the Nuclias Connect server.

The **Step 1** screen will appear. In the below figure, the Provision File entry is **None**.

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 to download a profile.

Tap **Download profile** to specify a connection to the Nuclias Connect controller.

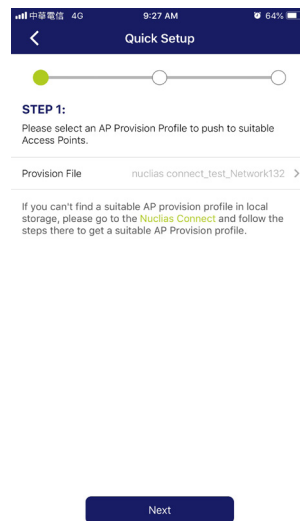


Software Installation

Nuclias Connect App

Once a Nuclias Connect controller connection is established, it'll be listed next to the field Provision File

Tap **Provision File** to select a local AP provision profile. In the following figure, the entry **Nuclias_test_Network1** is available.



A pop-up screen will appear. Select an available provision file from local storage and tap **Done** to continue.



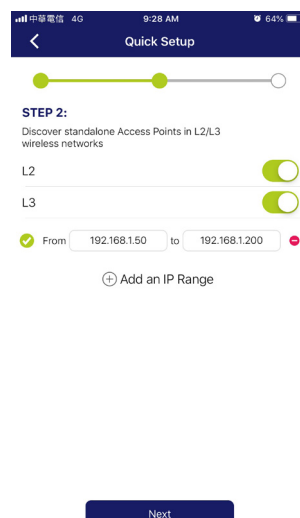
The process will continue and the app will return to the previous screen. From the Step 1 page, tap **Next** to continue.

Step 2 will appear. From this page, you can discover standalone APs connected to the L2/L3 wireless network.

Tap the button on the L2 field to enable discovery on the L2 network.

Tap the button on the L3 field to enable discovery on the L3 network. Then enter an IP range in the provided **From and To** fields. Tap add (+) to create a new IP range entry. Tap remove (-) to delete any defined range entries.

In the IP range fields, specify the starting and ending IP addresses.. Once the range is defined, tap **Next** to initiate the discovery process.



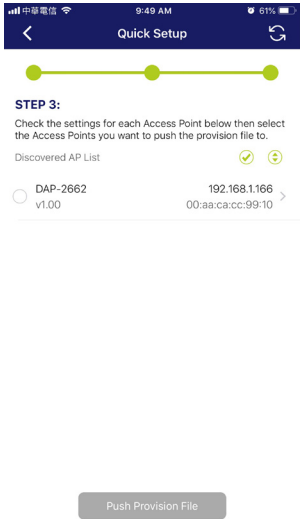
Software Installation

Nuclias Connect App

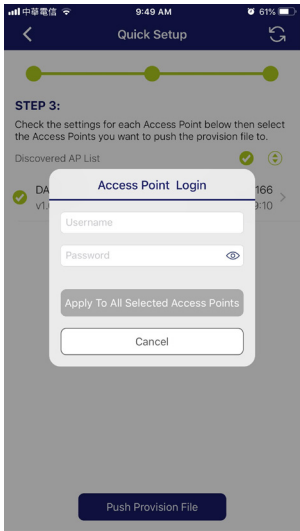
After scanning the network range, any detected access points will be listed here.

Tap the radio button next to the AP to select it. The local provision file that you previously selected will be pushed to the selected AP.

Tap **Push Provision File** to continue.



The AP login pop-up window is displayed. The listed IP and MAC address are shown at the top of the window. Confirm the selection and enter the user name and password with authorization to access the selected AP.



Tap **Apply** to continue the login process. The Modify IP Information page will appear. Any listed information can be modified; see the following figure for further information.

Parameter	Description
Cancel	Tap to discard any changes and continue the process.
Done	Tap to accept any changes and continue the process.
Model Name	Displays the model name for the listed AP device.
MAC	Displays the MAC address of the listed AP device.

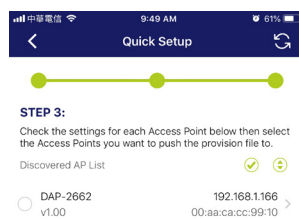
Software Installation

Nuclias Connect App

Parameter	Description
DHCP Mode	Tap to enable or disable the DHCP mode function. When enabled, the AP establishes dynamic IP address settings with any authorized client connections.
IP Address	Tap to designate an IP gateway setting.
Subnet Mask	Tap to designate a subnet mask.
Default Gateway	Tap to designate a default gateway setting.
DNS	Tap to designate a DNS setting.

Tap **Done** or **Cancel** to continue the process. The provision file will be pushed to the selected AP device (s). The App will return to the Step 3 page and will display the status of the Push function. The discovered APs lists the state of the push function with either a successful or failed state. See the following figure for further details.

Tap **Finish** to complete the process. In the event of a failed process, tap **Push Provision File** to attempt the function a second time.



Software Installation

Nuclias Connect App

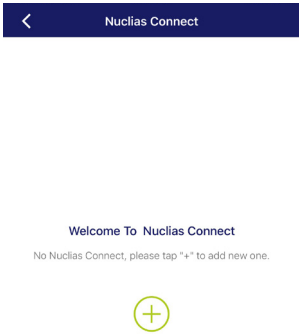
Nuclias Connect

Nuclias Connect is a wireless access point management tool capable of managing your sites and networks.

Tap **Nuclias Connect** to connect to a Nuclias Connect server.



The Welcome page will appear. If this is the first time pairing Nuclias Connect controller, you'll be asked to create a new Nuclias Connect pairing. Tap the add (+) button to start the process.



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

Parameter	Description
Specify NucliasConnect URL/IP Address	Enter the secure URL/IP address of the Nuclias Connect server to pair with the App.
Specify a reference name	Enter a specific name to identify the paired Nuclias Connect server.

Software Installation

Nuclias Connect App

Parameter	Description
User name	Enter a user name with the authority to access the Nuclias Connect controller.
Password	Enter the password for the referenced user name with the authority to access the Nuclias Connect server.
Login	Tap Login to initiate the login process.

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



Login to a new Nuclias Connect

Specify Nuclias Connect URL/IP Address:

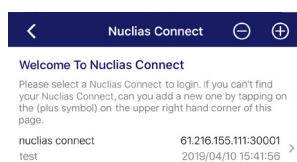
Specify a name that will reference this Nuclias Connect in Nuclias Connect History.

Username

Password

Login

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

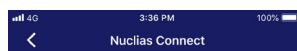


Tap on a Nuclias Connect server from the list.

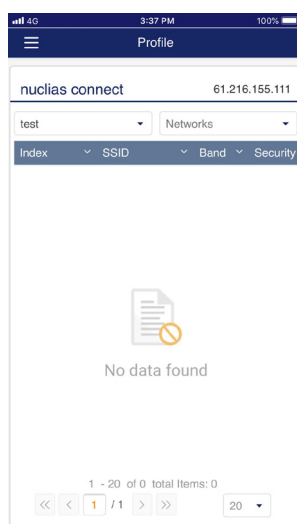
Software Installation

Nuclias Connect App

The user name page will appear. Enter the user name and password with authority to access the selected Nuclias Connect server. Tap **Login** to initiate the login process.



After the login process is authenticated, the dashboard will appear. The Nuclias Connect dashboard will list any currently defined sites, networks, access points, and clients.



The Nuclias Connect App is now paired with the Nuclias Connect server. Through the App interface, profiles can be downloaded to a local device, which can then be pushed to supported APs.

Software Installation

Nuclias Connect App

Standalone Access Point

Discover APs

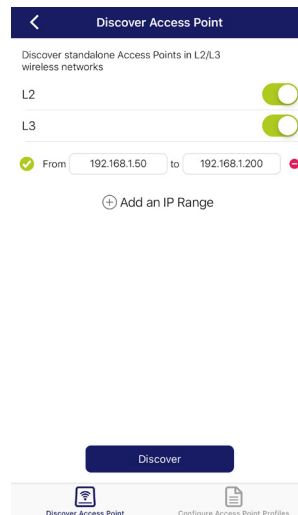
The Discover AP function allows you to discover any AP devices in a L2/L3 wireless network.

From this page, you can discover standalone APs connected to the L2/L3 wireless network.

Tap the button on the L2 field to enable discovery on the L2 network.

Tap the button on the L3 field to enable discovery on the L2 network. Then enter an IP range in the provided From and To fields.

Tap add (+) to create a new IP range entry. Tap remove (-) to delete any defined range entries.



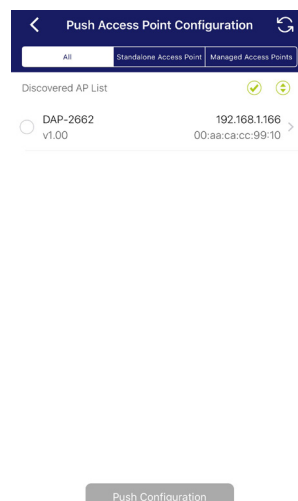
Once the range is defined, tap **Next** to initiate the discovery process.

Alternatively, tap Configure Access Point Profiles from the bottom of the page to add or delete any local profiles. See Configure Access Point Profiles.

After the scanning the network range, the Step 3 page will list any detected access points.

Tap the radio button next to the AP to select it. The selected local provision file will be pushed to the selected AP.

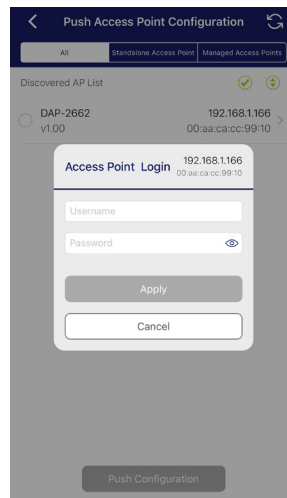
Tap **Push Provision File** to continue.



Software Installation

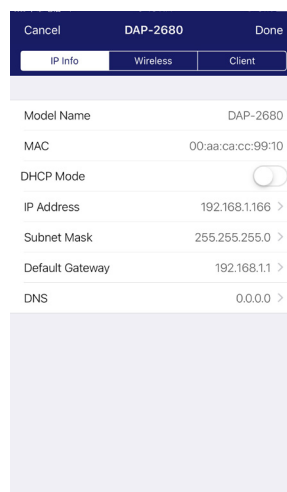
Nuclias Connect App

The AP login pop-up window will appear. The IP and MAC address are shown at the top of the window. Confirm the selection and enter the user name and password with authorization to access the selected AP. Tap **Apply** to continue.



Once a successful login is established, the AP interface menu will appear. The IP information, Wireless, and Client menu are listed as follows.

Parameter	Description
Cancel	Tap to discard any changes and continue the process.
Model Name	Displays the model name for the listed AP device.
MAC	Displays the MAC address of the listed AP device.
DHCP Mode	Tap to enable or disable the DHCP mode function. When enabled, the AP establishes dynamic IP address settings with any authorized client connections.
IP Address	Tap to designate an IP gateway setting.
Subnet Mask	Tap to designate a subnet mask.
Default Gateway	Tap to designate a default gateway setting.
DNS	Tap to designate a DNS setting.

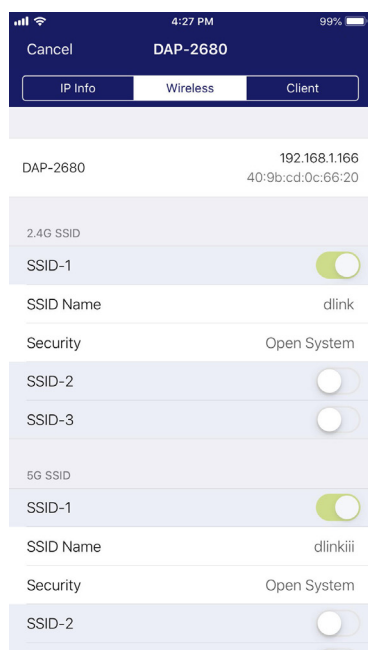


Software Installation

Nuclias Connect App

The Wireless settings menu is listed in the following figure.

Parameter	Description
Cancel	Tap to discard any changes and continue the process.
DAP-xxxx	Displays the model name and IP address of the AP device.
2.4G SSID	
SSID-#	Tap the slide button to enable or disable the SSID. The # character indicates the identifying number of the SSID.
SSID Name	Tap to change the current name of the SSID.
Security	Tap to select a specific security protocol: Open System (default), WPA-Personal, or WPA-Enterprise.
5G SSID	
SSID-#	Tap the slide button to enable or disable the SSID. The # character indicates the identifying number of the SSID.
SSID Name	Tap to change the current name of the SSID.
Security	Tap to select a specific security protocol: Open System (default), WPA-Personal, or WPA-Enterprise.
Wireless Information	
Radio Band	Tap to select a specific radio band: Off, 2.4G, 5G, or 2.4G / 5G.
Radio 2.4G Mode	Tap to select a specific 2.4G radio mode: Mixed 802.11n, 802.11g and 802.11b; Mixed 802.11g, 802.11b; 802.11n Only.
Radio 5G Mode	Tap to select a specific 5G radio mode: Mixed 802.11n, 802.11a; 802.11a Only; 802.11n; Mixed 802.11ac.
Country Code	Displays the assigned country designation for the AP.
Copy & Save Configuration	
Apply Configuration	Tap to select an alternate discovered AP device to push the current configuration.
Save Configuration	Tap to name and archive the current configuration profile.



Software Installation

Nuclias Connect App

Verify Managed Devices

To verify the connections status of the switch and access point, go to **Monitor > Access Point/ Switch**. Click on the drop-down menu to select the Site and the available network. The available APs/switches are listed. The Status column will show the either the online (●) and offline (●) status.

The following information is also available: Number, Action, Local IP Address, MAC Address, Model Type and Network.

The screenshot shows the Nuclias Connect Monitor interface. The left sidebar contains navigation options: Dashboard, Monitor (selected), Access Point, Switch, Switch Client, Switch Port, Topology, Floor Plan, Configuration, Report, Log, and System. The main area displays a table of managed devices under the 'Switch' section. The table has columns: No., Status, Action, Local IP Address, MAC Address, Model Type, Name, Network, Network ID, and Clients. One device is listed: No. 1, Status online (green dot), Action icons, Local IP Address 10.90.90.90, MAC Address 00:ad:24:a2:d5:20, Model Type DCS 1210 52, Name Dlink, Network Switch, Network ID, and Clients 6. The bottom of the table shows pagination: 1 - 20 of 1 total items: 1.

Upload New or Updated Configuration

Through the Nuclias Connect interface, you can manage individual or multiple AP models as well as upgrading the firmware. Simply select the firmware file and apply it immediately or schedule the update time.

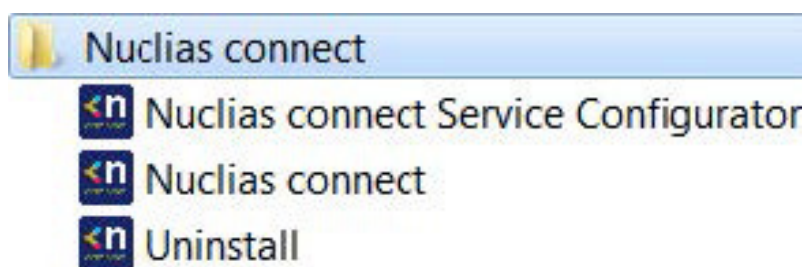
Navigate to **Configuration > Firmware Upgrade**, select the site and network to view the available AP models.

From the ensuing screen, select the firmware to upload by clicking the **Change** button. From the Time Start field, select Immediate and click **Apply** to immediately upgrade the firmware to the selected access points on the network. Alternatively, click the drop-down menu and use the Select Time option to define a set time for uploading the firmware.

The screenshot shows the Nuclias Connect Firmware Upgrade interface. The breadcrumb is 'Firmware Upgrade > cccccc > TEST1'. The main heading is 'Upload firmware files for each model'. There is a 'Check For Update' button. Below is a table with columns: Model Type / HW Version, Current FW Version (Device Quantity), New FW Version, and Firmware File. Two models are listed: DAP-2610/A1G with current FW v2.06r084 (1) and DAP-2680/2A1G with current FW v2.06r054 (1). Below the table is a 'Time Start' section with a 'Select Time' dropdown, a time picker showing 12:06 PM, and a date picker showing 2021.6.10. At the bottom are 'Apply' and 'Clear' buttons.

Nuclias Connect Configuration

After the software installation is complete, the following applications will be available.



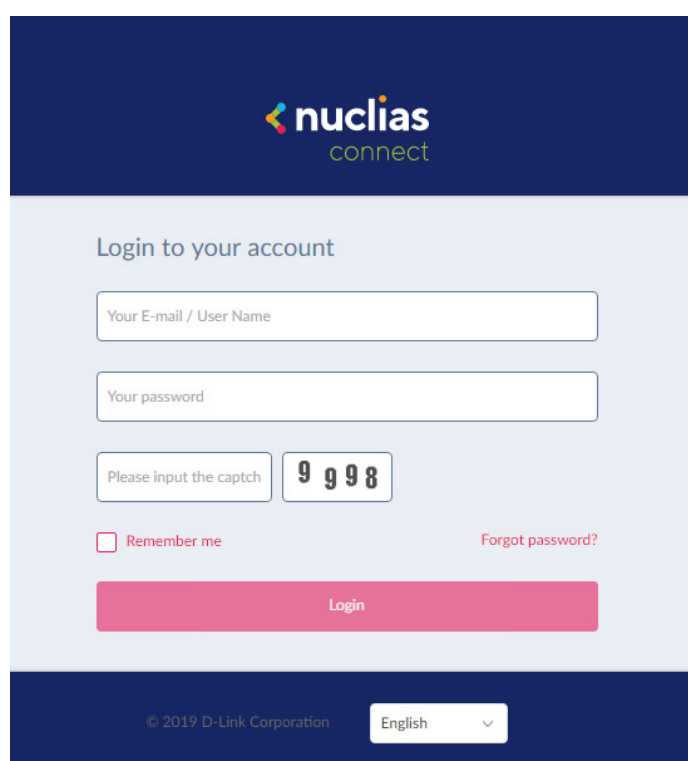
Click on **Nuclias Connect** to open the client application.

Nuclias Connect uses a secure HTTPS connection to connect to the Nuclias Connect Controller. By default, the application will open the default Web browser and connect to the localhost, which is the local means of connecting to the computer's own IP address.

Alternatively, from a remote computer, you can also connect to the Nuclias Connect Server by entering the IP address of the computer that has the controller application installed on the web browser. Open the web browser on the remote computer (Internet Explorer or Google Chrome are recommended) and enter the IP address or domain name of the host computer in the address bar of the Web browser and press **ENTER** to open the Nuclias Connect management interface.

The Nuclias login screen will appear once a connection to the server is established. Enter the login user name, password and captcha requirement, if applicable. Click **Login** to enter Nuclias Connect .

NOTE: By default, the user name and password are "**admin**". Supported languages include: English (default), Traditional Chinese, Simplified Chinese, Korean, Japanese, French, Spanish, German, Russian, Italian, and Turkish.

The image shows the Nuclias Connect login interface. At the top, there's a dark blue header with the 'nuclias connect' logo. Below the header, the text 'Login to your account' is centered. There are three input fields: 'Your E-mail / User Name', 'Your password', and a captcha field with the text 'Please input the captcha' and the digits '9 9 9 8'. Below the captcha field, there is a 'Remember me' checkbox and a 'Forgot password?' link. A large pink 'Login' button is positioned below these fields. At the bottom of the page, there is a dark blue footer containing the copyright notice '© 2019 D-Link Corporation' and a language dropdown menu currently set to 'English'.

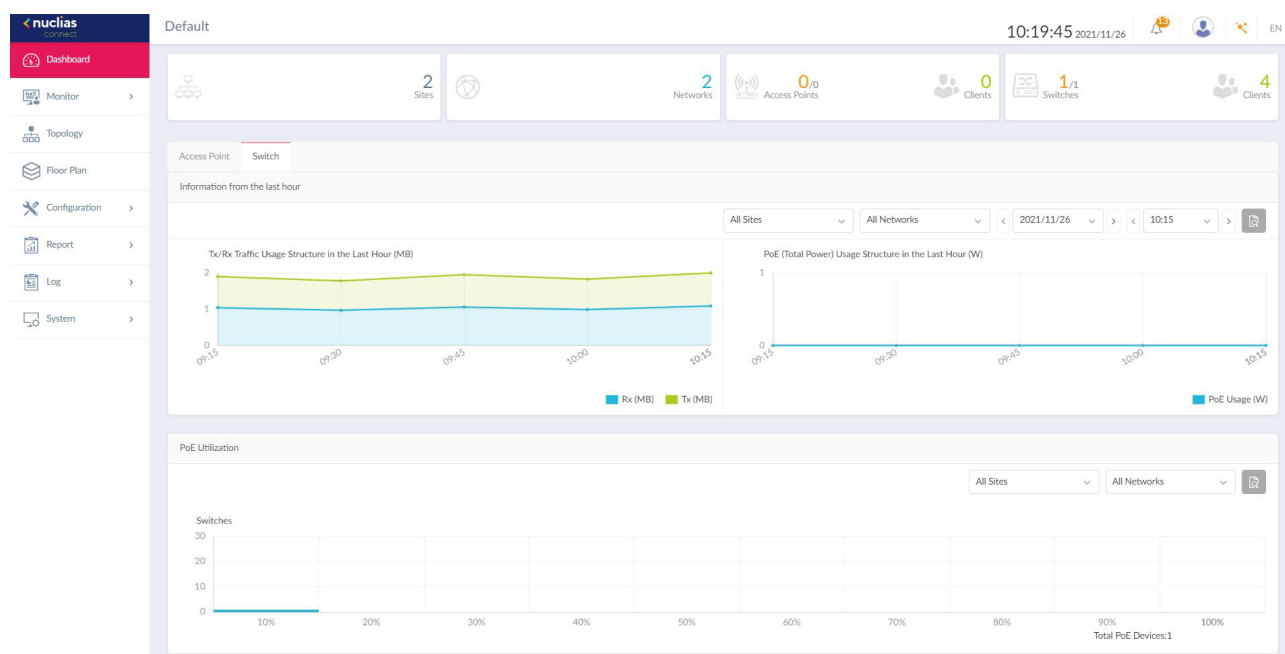
Nuclias Connect

Dashboard

After successfully logging into the server, the **Dashboard** page for Access Point and Switch is displayed. The dashboard provides an overview of total sites, created networks, available access points and its clients, and available switches and its clients

Access Point Field	Description
Information from the Last Hour	Displays the number of clients (Last hour vs Past 7 days), traffic (Last hour vs Past 7 days), last hour downlink/uplink traffic, and last hour traffic by SSID.
Channel Utilization	Displays the utilization rate for both 2.4 and 5 GHz bandwidth.
Latest Events	Displays a simplified log of the latest events across all or selected sites.

Switch Field	Description
Information from the Last Hour	Displays last hour Tx/Rx traffic usage and last hour PoE total power usage.
PoE Utilization	Displays the utilization rate of switches across different sites and networks.
Latest Events	Displays a simplified log of the latest events across all or selected sites.

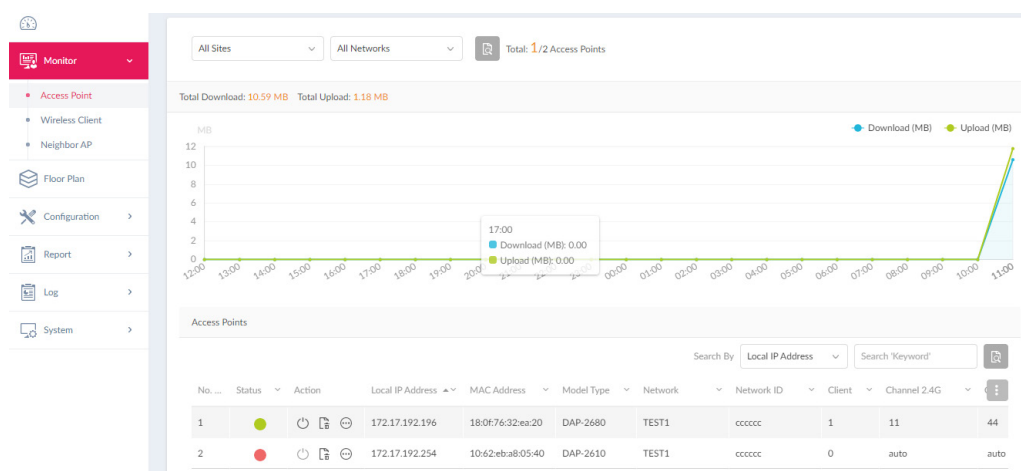


Nuclias Connect

Monitor

Access Point

Go to **Monitor** on the left panel to view data usage and total number of access points. On this page, you can view a summary of the data usage of all or selected number of wireless clients and networks managed by the application.



In the **Search By** drop-down field, select an attribute (**Local IP Address, Local IPv6 Address, NAT IP Address, MAC Address, Model Type, FW Version, Name, Location, Channel 2.4G, Channel 5G 1, Channel 5G 2 (Tri-Band), Power 2.4G, Power 5g 1, Power 5g 2 (Tri-Band)**) to specify the search field or enter a keyword related to the target device in the Search field. Click to start the process. Any relevant devices meeting the search criteria will be listed.-

Nuclias Connect

Monitor


Access Point

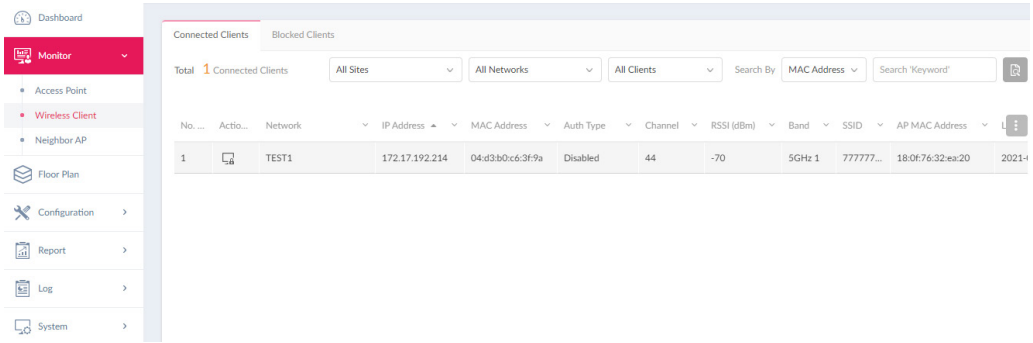
Wireless Client

Connected Clients

Navigate to **Monitor > Access Point > Wireless Client** on the left panel, the **Connected Clients** tab is displayed. You can view a summary of all connected clients managed by the application.

Three filters are displayed: **Site**, **Network**, and **Clients**.

The following figure shows a typical summary. Use the filters to select a specific Site, network and client. Additionally, you can enter a keyword related to the target device in the Search field and click  to start the process. Any relevant devices meeting the search criteria will be listed in the frame.



All wireless clients connected to the access points that are managed by this application are displayed. Information such as **Network**, **IP Address**, **IPv6 Address**, **MAC Address**, **Auth. Type**, **OS** (only available on captive portal clients), **Upload**, **Download**, **Channel**, **RSSI (dBm)**, **SNR (dB)**, **Band**, **SSID**, **AP MAC Address**, **Traffic Usage**, **Traffic Usage(%)**, **Last Seen**, and **Uptime** is displayed for each wireless client.


Nuclias Connect

Monitor

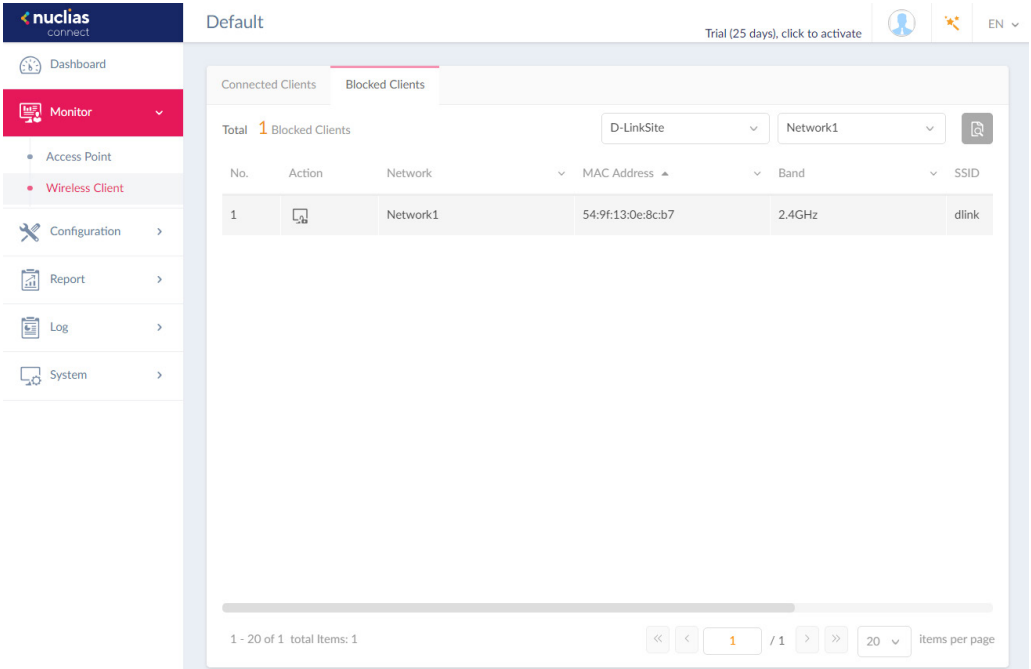
Access Point

Wireless Client

Blocked Clients

Navigate to **Monitor > Access Point > Wireless Client** on the left panel, then click the **Blocked Clients** tab. Use the **Sites** and **Networks** drop-down menu to select a Site and Network. Click  to start the search. Any relevant devices meeting the search criteria will be listed.

The page lists the following information: **Blocked client count**, **Action**, **Network**, **MAC Address**, **Band**, **SSID**, and **Auth. Type**.



Nuclias Connect Monitor Access Point Neighbor AP

Navigate to **Monitor > Access Point > Neighbor AP** on the left panel, the neighbor AP list is displayed. To enable this function, go to **Configuration > Profile Settings > Site>Network > Wireless Resource > Neighbor AP Detection** and click **Enabled**.

Search By Detected By Search 'Keyword'									
No.	BSSID	Detected By	Status	SSID	Security	RSSI (dBm)	BW(MHz)	Channel	Supported
1	33:00:00:00:01:00	00:11:22:33:45:00	unknown	Dlink-test_1	Open System ABC	-90	20	1	B,N
2	33:00:00:00:01:18	00:11:22:33:45:00	unknown	Dlink-test_2	Open System ABC	-90	20	1	B,N
3	33:00:00:00:01:30	00:11:22:33:45:00	unknown	Dlink-test_3	Open System ABC	-90	20	1	B,N
4	33:00:00:00:01:48	00:11:22:33:45:00	unknown	Dlink-test_4	Open System ABC	-90	20	1	B,N
5	33:00:00:00:01:60	00:11:22:33:45:00	unknown	Dlink-test_5	Open System ABC	-90	20	1	B,N
6	33:00:00:00:01:78	00:11:22:33:45:00	unknown	Dlink-test_6	Open System ABC	-90	20	1	B,N
7	33:00:00:00:01:90	00:11:22:33:45:00	unknown	Dlink-test_7	Open System ABC	-90	20	1	B,N
8	33:00:00:00:01:a8	00:11:22:33:45:00	unknown	Dlink-test_8	Open System ABC	-90	20	1	B,N
9	33:00:00:00:01:c0	00:11:22:33:45:00	unknown	Dlink-test_9	Open System ABC	-90	20	1	B,N
10	33:00:00:00:01:d8	00:11:22:33:45:00	unknown	Dlink-test_10	Open System ABC	-90	20	1	B,N
11	33:00:00:00:02:00	00:11:22:33:45:18	unknown	Dlink-test_11	Open System ABC	-90	20	1	B,N
12	33:00:00:00:02:18	00:11:22:33:45:18	unknown	Dlink-test_12	Open System ABC	-90	20	1	B,N

1 - 20 of 50 total items: 50

<< < 1 / 3 > >> 20 items per page


Field	Description
BSSID	Displays the MAC address of the AP's wireless interface.
Detected by	Displays the mac address of AP that the AP was scanning.
Status	Displays the status of AP (Unknown, Known, and Managed).
SSID	Displays the name of the wireless network.
Security	Displays the security status indicating whether encryption is used.
RSSI	Displays the RSSI that the AP was detecting.
BW(MHz)	Displays the channel width that the AP was using.
Channel	Displays the channel setting that the AP was detected on.
Supported Modes	Displays the list of modes that the AP was supported.

Nuclias Connect

Monitor

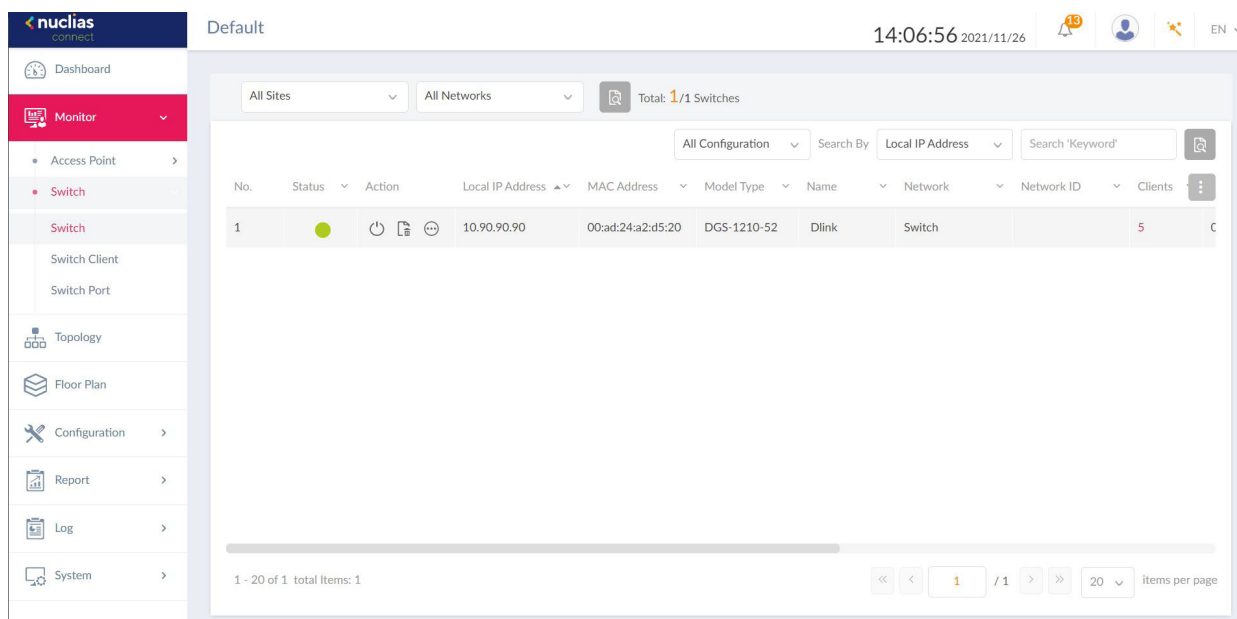
Switch

Go to **Monitor > Switch** and use the Site and Network filter to locate the device you'd like to monitor. On this page, you can view a summary of the devices managed by the application. The summary includes the following: **Status, Local IP Address, NAT IP Address, MAC Address, Model Type, FW Version, HW Version, Serial Number, Name, Location, Site, Network, Network ID, Clients, Power Budget, CPU Usage, Memory Usage, Ports, Use Configuration, Last Seen, Uptime** and **Power Delivered**.

Select a configuration type (**Profile, Standalone, All**) and attribute (**Local IP Address, MAC Address, Model Type, FW Version, Name, Ports**) to narrow down the search field or enter a keyword related to the target device in the Search field. Click  to start the process. Any relevant devices meeting the search criteria will be listed.

Under the Action panel, click  to restart your device. Click  to move the device to Unmanaged. Click  to enter the Device Detail Page.

Key Fields	Description
Name	Displays user-defined name of the switch. Empty if no name is given. Click the column to revise or create a name. The max length of the name is 63 characters.
Location	Displays the location of the switch. Click the column to revise or create a name for the location. The max length for the location name is 32 characters.
Clients	Displays the total number of clients connecting to the switch. Click on the Clients number to be directed to the Switch Client page.
Ports	Displays the total number of ports on the switch. Click on the ports to be directed to the Switch Port page.
Use Configuration	Displays the configuration mode (Profile/ Standalone). <ul style="list-style-type: none"> Profile: Devices under profile mode share the same configurations in the profile. Standalone: Devices have their own configurations, and does not get affected by profile.
Last Seen	Displays the last connected time of the switch.
Uptime	The activating time of the switch after reboot.

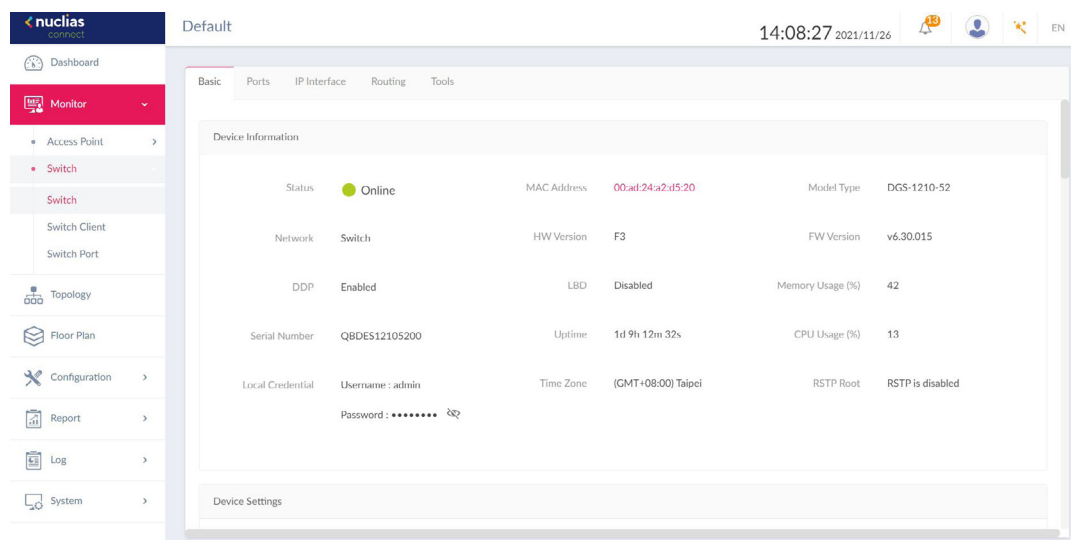


Nuclias Connect Monitor Switch Device Detail Page

Basic

The device detail page displays comprehensive information of your switches and allows users to configure the ports, IP interface, route settings, and many more. Navigate to **Monitor > Switch**, and click **Link to Device Detail Page** under Action.

On the **Basic** tab, you can configure your device and view a summary of Device Information. The following information is displayed under the **Device Information** section: **Online Status, Network, DDP, Serial Number, Local Credential, MAC Address, HW Version, LBD, Uptime, Time Zone, Model Type, FW Version, Memory Usage, CPU Usage, and RSTP Root.**



Key Fields	Description
DDP	Displays the DDP (D-Link Discovery Protocol) settings of the switch.
Local Credential	Displays the username and password for local GUI/console.
LBD	Displays the LBD (Loopback Detection) settings of the switch.
RSTP Root	Displays the root bridge and its priority of the spanning tree.

In the **Device Settings** section, select a use configuration (Profile or Standalone). If Profile is selected, the subsequent settings, such as VLAN and IGMP Snooping will be fixed. If Standalone is selected, the above-mentioned settings will be available for editing.

Under **VLAN Configuration**, you can set up a VLAN by entering a VLAN ID (2-4094) and a description for ease of identification. Click Add to create, or Clear to cancel. The created VLAN IDs will be displayed under the VLAN list. Enter a keyword in the search field and click to locate a VLAN ID. Click to edit the ID or click to delete it.

Nuclias Connect

Monitor

Switch

Device Detail Page

Basic

IGMP Snooping is disabled by default. When use configuration is set to **Standalone**, you can enable IGMP Snooping. Enter the VLAN to complete the process.

In the **Uncross Attributes** section, features that cannot be configured via profile will be listed here. Enter a name, location, and use the drop down menu to select a STP Bridge Priority. Click Apply to complete the settings.

IGMP Snooping Configuration

IGMP Snooping

☐ Enabled

☒ Disabled

VLAN

1-4094, c.g. 1-4,7,9 or All.

Uncross Attributes

Name

Location

STP Bridge Priority

▼

Apply

In the **IP Connect** section, you can deploy primary connections. Choose a type of IP (DHCP or Static IP), and enter a Local IP Address, VLAN (VLAN ID), Netmask, Gateway. If DHCP is selected, enter the DNS. If static IP is selected, enter a Primary DNS, Secondary DNS, Third DNS. Click **Apply** to complete the set up.

IP Connect

Type

☒ DHCP

☐ Static IP

Local IP Address*

VLAN*

▼

52 member ports belonging to this VLAN currently.

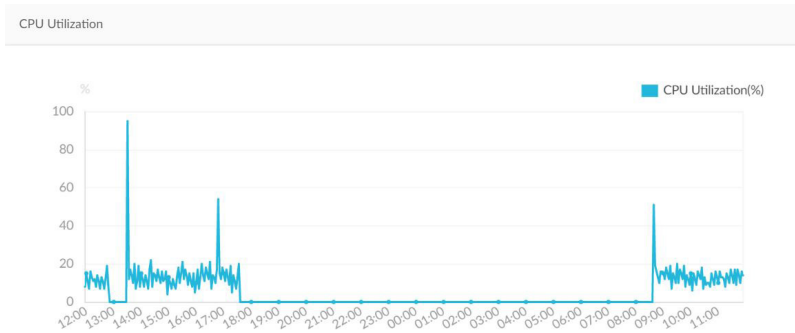
Netmask*

Gateway*

DNS

Apply

In the **CPU utilization** section, a CPU Utilization graph is displayed. On the Y axis shows the percentage of CPU utilization. On the X axis shows the time by hour.



Nuclias Connect

Monitor

Switch




Device Detail Page

Ports

Under the Ports tab, a port status overview is presented. The graph displays a range of colors and icons to inform users of the status of each individual port. Clicking on the port icons will direct users to the **Port Detail** page of the specified port.



Here's a summary of all the statuses and what they represent:

Status	Description
Green	Connected to Gigabit Ethernet
Orange	Connected to 10/100Mbps Ethernet
Dark Gray	Port disconnected
Light Gray	Port disabled
	Powered by PoE
	Port mirrored
Red	Error detected
	PoE+Mirror

In the **Port Traffic Usage** section, a graph indicating Rx and Tx usage based on time is presented.



In the **Port Information** section, you can view a summary of all active and inactive ports. The summary includes information such as **port number, Aggregate link status, Tx/Rx/Total bytes, used power, PoE, Port type, VLAN, Allowed VLANs, Port State, PoE Supply Schedule, RSTP, LBD, DDP, Port Shutdown Schedule, Mirror, Access Policies, LLDP, and Port Name.**

Use the **Search By** drop down menu to select between VLAN and Port, and select a **Port Type** (Access, Trunk, or all) to narrow down the search, or enter a keyword to locate a port.

Port Information

Search By

VLAN

Port Type

All Type

Search 'Keyword'

Port

Aggregate

Link

Tx Bytes

Rx Bytes

Total Bytes

Used Power ...

PoE

Port Type

VLAN

Allowed

1

-

Auto / Link down

0.00 (MB)

0.00 (MB)

0.00 (MB)

0.0 (W)

Enabled

Access

1

2

-

Auto / Link down

0.00 (MB)

0.00 (MB)

0.00 (MB)

0.0 (W)

Enabled

Access

1

3

-

Auto / Link down

0.00 (MB)

0.00 (MB)

0.00 (MB)

0.0 (W)

Enabled

Access

1

Key Fields	Description
Aggregate	Displays the port-channel ID and aggregate type (static/LACP).
VLAN	Displays the native VLAN ID of Trunk mode or the VLAN ID of Access mode. In addition, it also indicates the Voice VLAN ID when display.
Allowed VLANs	Displays the allowed VLAN ID when the Port Type belongs to Trunk.


Nuclias Connect

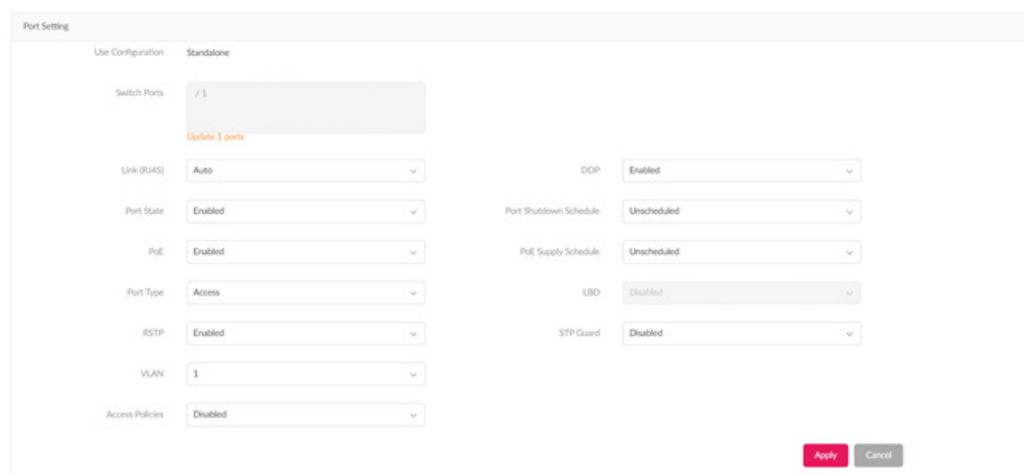
Monitor

Switch

Device Detail Page



Ports

To make changes to a port or port group on the switch, first make sure the User Configuration is set to Standalone in the Device Settings section. Next, check the boxes next to the port(s) you'd like to change. Click  to edit. Scroll down to access the Port Settings. Once the changes are made, click **Apply** to update the changes.



Field	Description
Port Shutdown Schedule	Apply a time profile to the port shutdown function. The time profile is created in the time profile page.
PoE Supply Schedule	Apply a time profile to the PoE supply function.
Port Type	<p>Type: Switch ports can be configured as one of the following two types.</p> <p>(1) Trunk: Trunk port allows the selected port to accept/pass 802.1Q tagged traffic.</p> <ul style="list-style-type: none"> Native VLAN: All untagged traffic will be placed on this VLAN. The range is 1-4094. Allowed VLANs: Only selected VLANs are able to traverse this link. The range is All/1-4094. <p>(2) Access: Access port places all traffic on its defined VLAN.</p> <ul style="list-style-type: none"> Access VLAN: All traffic is placed on this VLAN. The range is 1-4094. Access policy: Apply a restriction policy to this port. <p>* Disabled: All devices can access this port.</p> <p>* Static MAC Whitelist: Only the devices with MAC addresses specified in this list can access this port.</p> <p>* Port Security Delete-on-time Mode: All learned MAC addresses will be purged when an entry is aged out or when the user manually deletes these entries. Users can configure the number of dynamic learned entries via "Dynamic whitelist size limit". When the total number of "Dynamic Whitelisted MACs" exceeds the value of "Dynamic Whitelist Size Limit", all subsequent MAC address will be denied access to this port. A table displaying dynamically learned MAC address is available.</p> <p>* User defined access policy: Apply a policy name defined via Access Policy Page.</p>

In the **Aggregate Management** section, you can combine a minimum of 2 to 8 network connections into a link aggregation group. From the Port-channel ID drop-down menu, select between 1 to 8. Next, select an aggregate type, **LACP** or **Static**. From the Port list, select 2 to 8 ports to form a link aggregation group. Click **Add** to form, or **Clear** to cancel.

Under the Port-channel List, you'll see a summary list of link aggregation you have created. The summary shows the Port-channel ID, Aggregate Type and Port numbers. Beneath the Action field, click  to edit, or  to delete. Click Apply to save the changes.

Nuclias Connect

Monitor

Switch

Device Detail Page

Ports

Aggregate Management

Port-channel ID

3

Aggregate Type

LACP

Static

Port List

Unselected:

Port23

Port24

Port25

Port26

Port27

Port29

Port30

>>

<<

Selected:

Combine 2 to 8 ports to form a link aggregation group.

Add

Clear

Port-channel List

The max. number of Port-channel in the table is 8, 6 remain

Port-channel ID	Aggregate Type	Port	Action
1	Static	14, 16, 28	<div><div></div><div></div></div>
2	LACP	3, 5	<div><div></div><div></div></div>

In the **Mirror Management** section, you can mirror the network packet on one switch port to another. First select a Destination Port using the drop-down menu. Next, from the Souce Port list, select the ports you'd like to mirror. Once selected, from the drop-down menu, pick the type of traffic to mirror over(Rx, Tx, or Both). Click Add to create, or Clear to cancel.

Mirror Management

Destination Port

Port5

Source Port List

Unselected:

Port1

Port2

Port3

Port4

Port6

Port7

Port8

>>

<<

Selected:

Add

Clear

Under the **Port Mirror** list, you'll see a a summary of the ports you have mirrored. The summary displays the Destination Port, and Source Ports(Tx/Rx/Both). Beneath the Action field, click to edit, or to delete. Click Apply to save the changes.

Port Mirror List

The max. number of Port mirror in the table is 1, 0 remain

Destination Port	Source Ports (Tx)	Source Ports (Rx)	Source Ports (Both)	Action
5	4	6	1	<div><div></div><div></div></div>


Nuclias Connect

Monitor

Switch

Device Detail Page

Ports

In the **Client Information** section, a summary of client information is displayed. Use the **Search By** drop-down menu to select a criteria to filter the search result. Click  to start the search. The following information is displayed in the summary: **Number, Site, Network, Client MAC Address, Client IPv4 Address, Port, VLAN, LLDP, Manufacture, and Last Seen.**

Client Information

Search By Client MAC Ad v e.g. 3c:1e: 04:16:53:20



No.	Client Mac Address	Client IPv4 Address	Port	VLAN	LLDP	Manufacture	Last Seen	
1	8c:16:45:bf:1e:7d	-	3	1	8C-16-45-BF-1E-...	-	2021/11/12 13:31:01	
2	a8:63:7d:61:c2:62	-	5	1	-	-	2021/11/12 13:31:01	
3	a8:63:7d:61:c2:63	-	5	1	A8-63-7D-61-C2-...	-	2021/11/12 13:31:01	
4	b6:b7:d4:ac:46:c8	-	5	1	-	-	2021/11/12 13:31:01	

Key Fields	Description
Port	Displays the port number of the switch to which the client is connected to. Click the Port number to be directed to port detail page
LLDP	Displays the LLDP information of neighbors.
Manufacture	Displays the Manufacture name of the remote device via LLDP.
Last Seen	Displays the last time that the client was seen on the network.

Nuclias Connect

Monitor

Switch

Device Detail Page

IP Interface

Under the IP Interface tab, you can configure the IPv4 interface and view a summary of their statuses. To create an IPv4 interface, go to **IPv4 Interface**, select a **VLAN ID**, and choose to **Enable** or **Disable** the interface admin state. Enter an IPv4 **IP address** and **Netmask**. Click **Add** to apply the IP interface to a VLAN, or **Clear** to remove the entered values.

BasicPortsIP InterfaceRoutingTools

IPv4 Interface

VLAN ID1



StateDisabled

IP Address*

Netmask*

Add

Clear

In the IPv4 Interface Table, a summary containing VLAN ID, State, IP Address, and Link Status is displayed. Beneath the Action field, click  to edit, or  to delete. Click Apply to save the changes.

IPv4 Interface Table

The max. number of entries in the IPv4 Interface table is 4, 3 remain

VLAN ID	State	IP Address	Link Status	Action
1	Enabled	10.90.90.90 / 255.0.0.0	Up	

Apply

Nuclias Connect

Monitor

Switch

Device Detail Page

Routing

In the Routing tab, you can set up static routing for IPv4 formatted addressing. Under the IPv4 Static/Default Route Settings section, enter an **IP address or use the Default route, Netmask, Gateway, Cost, and Backup State(Primary/Backup)**. Click **Add** to add the route settings, or **Clear** to clear the values entered.

In the **Static Route Table**, a summary of Static Route containing **Number, IP Address/Netmask, Gateway, Cost, Protocol, Backup, and Status** is displayed. Beneath the Action field, click **Delete** to delete the static route. Click **Apply** to apply the settings to the switch.

BasicPortsIP InterfaceRoutingTools

IPv4 Static/ Default Route Settings

IP Address*0.0.0.0

☒ Default

Netmask*0

e.g. 255.255.255.254 or 0-32

Gateway*

e.g. 172.18.192.1


Cost (1-65535)*1

Backup State

Primary

Add

Clear

The IPv4 Route Table stores the routes information of the switch. Use the **Search By** drop-down menu to select a search criteria (**Network/IP Address**) to filter your search. Click  to start the search. The following information is presented in the table: **Number, IP Address, Netmask, Gateway, Interface Name, Cost, and Protocol**.

IPv4 Route Table

Search ByNetwork Addresse.g. 172.18.208.11/24

No. ...	IP Address	Netmask	Gateway	Interface Name	Cost	Protocol
1	10.0.0.0			System	0	
2	10.90.90.2			System	0	
3	10.90.90.90			System	0	
4	10.255.255.255			System	0	

Nuclias Connect

Monitor

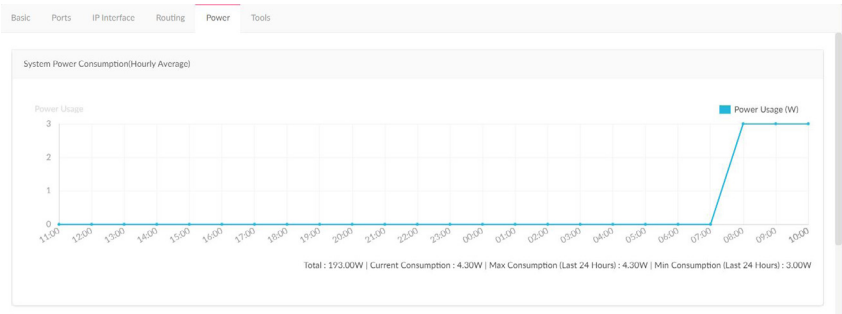
Switch

Device Detail Page

Power

Under the Power tab, the **System Power Consumption** chart and **PoE Port State** summary is displayed. Note that the Power tab will only be available if your switch supports PoE.

The System Power Consumption chart shows your switch's power usage in watt by the hour, as well as the total, current, minimum, and maximum power consumption.



The PoE Port State summary shows the IEEE classification and the power consumption of each port on the switch. The following table describes each of the field in the summary:

Field	Description
No.	Port number
State	PoE port status.
Class	The IEEE classification: N/A or a value from IEEE class 0 to 4.
Used(W)	The amount of power that is currently allocated to PoE ports in watts.

PoE Port State			
Port#	State	Class	Used (W)
1	no PD	N/A	0.00
2	no PD	N/A	0.00
3	no PD	N/A	0.00
4	no PD	N/A	0.00
5	no PD	N/A	0.00

Nuclias Connect

Monitor

Switch

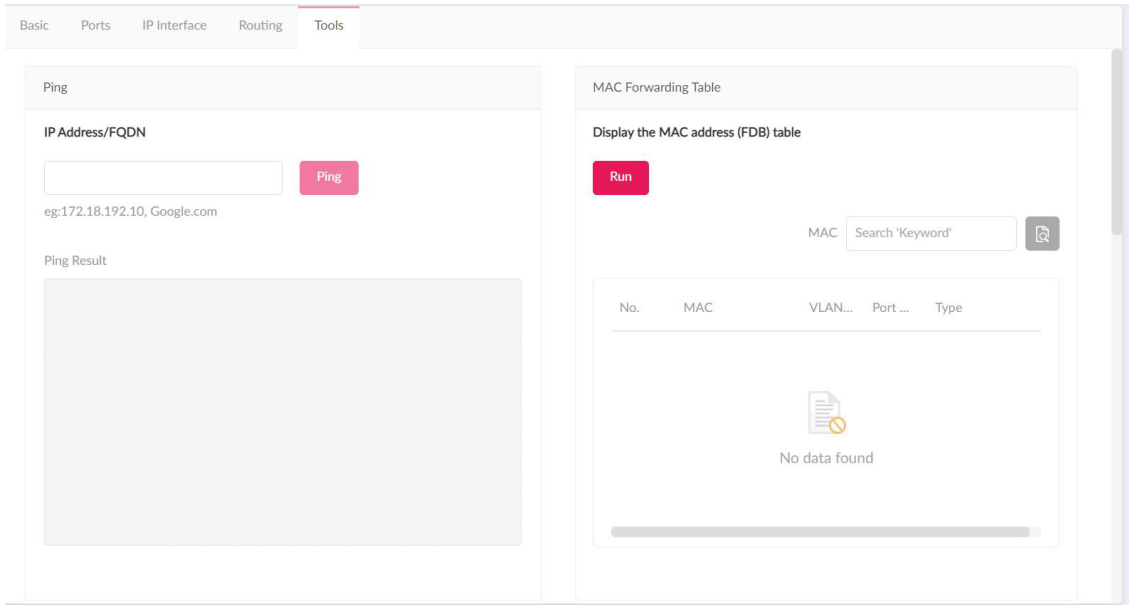
Device Detail Page

Tools

Under the Tools tab, you’re presented with the following tests to help troubleshooting: **Ping**, **Locate Device**, **Cable Test**, **Cycle PoE**, **MAC Forwarding Table**, and **Copy Configuration to Other Device**. Note that the tools are disabled when your devices are offline.

The **Ping Tool** can identify if a connection is working. Enter a host name or IP address and click **Ping** to perform the ping test. When the server received the ping signal, a summary of Ping Statistics including **Packet sent**, **received**, and **lost** is displayed. If no signal is received, the message “The device is unreachable” is displayed.

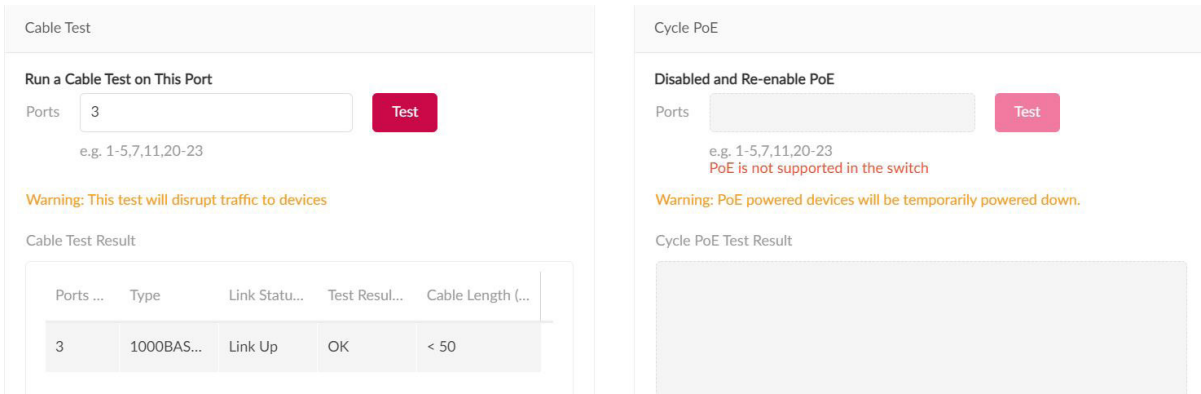
The **MAC Forwarding Table** shows a summary of **MAC addresses**, **VLAN**, **Port**, and **IP Address Type**. Press Run to begin the process. On the MAC search filed, enter a relevant keyword to help locate the MAC address.



The **Cable Test** allows you to test the connectivity of one or multiple ports. Enter a number of port(s) and click Test to begin the process. The following information will be displayed: **Port number**, **Type**, **Link Status**, **Test Result**, and **Cable Length**. Under the Test Result field, 5 statuses can be displayed: **OK**, **Open**, **Short**, **Test failed** and **-**.

Note: The cable test will disrupt traffic to devices.

The **Cycle PoE** tool allows you to disable or enable PoE on specific ports. This tool can only be executed when PoE is enabled. Note that if the switch does not support PoE, this section will be disabled.



Nuclias Connect

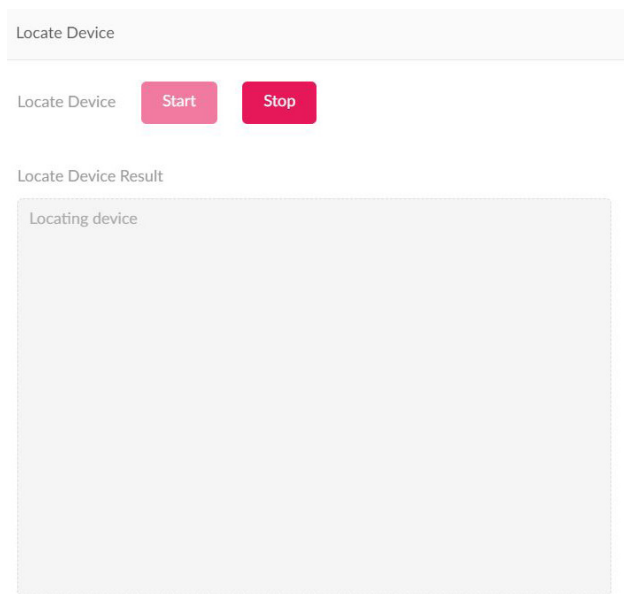
Monitor

Switch

Device Detail Page

Tools

The **Locate Device** function can help identify unlabeled switches by lighting up the LEDs on the switch. Click the Start button to light up the switch. All LEDs will light up in green for 5 minutes. Click the Stop button to stop the light immediately. If a device is located, a message "Locating device..." will be displayed under the Locate Device Result field. If no devices can be located, a message "The device is unreachable" will be displayed. If the server receives failure message sent by the switch, a message "Locate device failed" will be displayed.



Locate Device

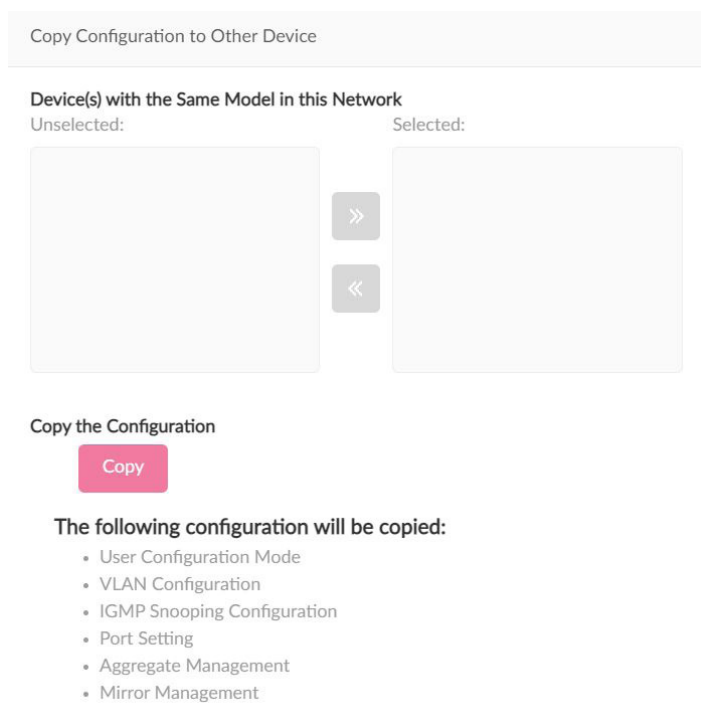
Locate Device Start Stop

Locate Device Result

Locating device

The **Copy Configuration** function allows you to copy **Configuration Mode, VLAN Configuration, IGMP Snooping, Port Settings, Aggregate Management, and Mirror Management** settings from your device to other device(s) in the network. (Note that the two device needs to be the same model.)

To copy the configuration, select the switch(es) in the network that will be copied. Click the **Copy** button to copy the configuration from your device to the selected device(s). A pop-up window will confirm once again. Click Copy to continue or Cancel to stop.



Copy Configuration to Other Device

Device(s) with the Same Model in this Network

Unselected: Selected:

Copy the Configuration

Copy

The following configuration will be copied:


- User Configuration Mode
- VLAN Configuration
- IGMP Snooping Configuration
- Port Setting
- Aggregate Management
- Mirror Management

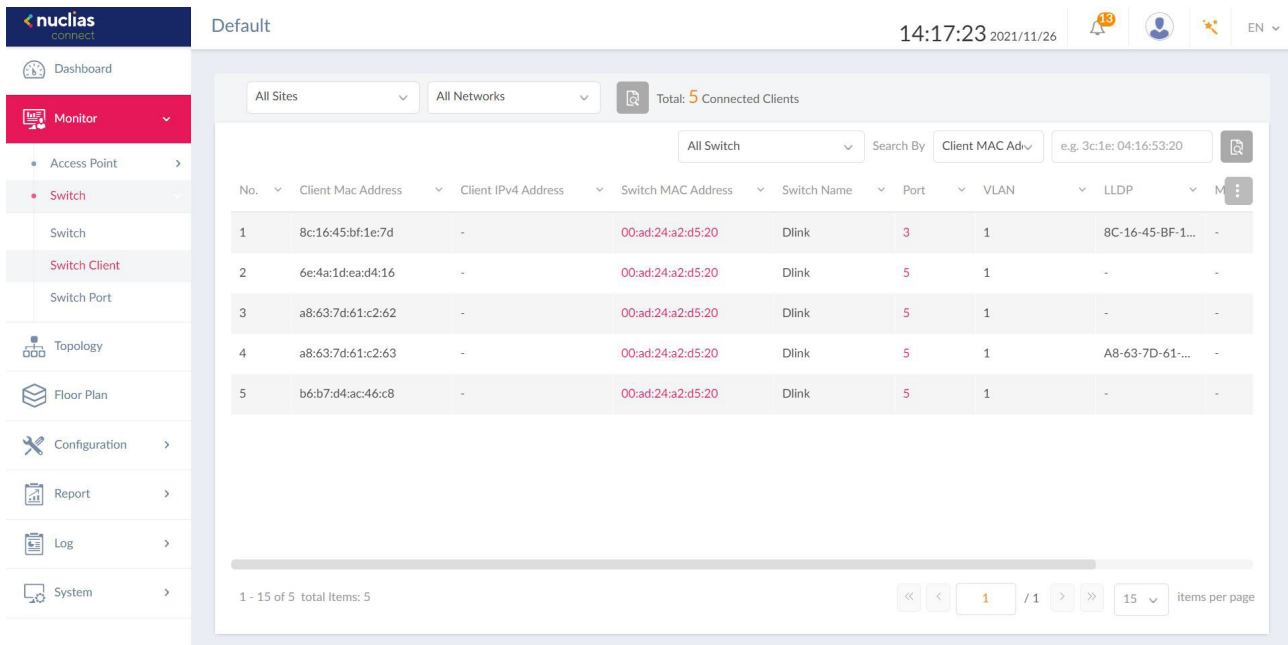
Nuclias Connect Monitor

Switch

Switch Client

The Switch Client page displays a cumulative list of all the active client devices that are connected to the switch network. The following information is displayed: **Number, Client MAC Address, Client IPv4 Address, Switch MAC Address, Switch Name, Port, VLAN, LLDP, Manufacturer, and Last Seen.**

Use the **Site and Network** drop-down menu to filter the information, and click  to start the search. Likewise, you can use the **Switch** and **Search By** drop-down menu to select a criteria (**Client MAC address, Client IPv4 Address, VLAN and Port**) and enter relevant keywords to narrow the search result.





No.	Client Mac Address	Client IPv4 Address	Switch MAC Address	Switch Name	Port	VLAN	LLDP	Manufacturer
1	8c:16:45:bf:1e:7d	-	00:ad:24:a2:d5:20	Dlink	3	1	8C-16-45-BF-1...	-
2	6e:4a:1d:ead4:16	-	00:ad:24:a2:d5:20	Dlink	5	1	-	-
3	a8:63:7d:61:c2:62	-	00:ad:24:a2:d5:20	Dlink	5	1	-	-
4	a8:63:7d:61:c2:63	-	00:ad:24:a2:d5:20	Dlink	5	1	A8-63-7D-61...	-
5	b6:b7:d4:ac:46:c8	-	00:ad:24:a2:d5:20	Dlink	5	1	-	-

Key Fields	Description
Switch MAC Address	Displays the MAC Address of the switch that the client is connected to. Click the MAC Address to be redirected to the switch detail page.
Port	Displays the port number of the D-Link switch that the client is connected to. Click the port number, it will be directed to per port page.

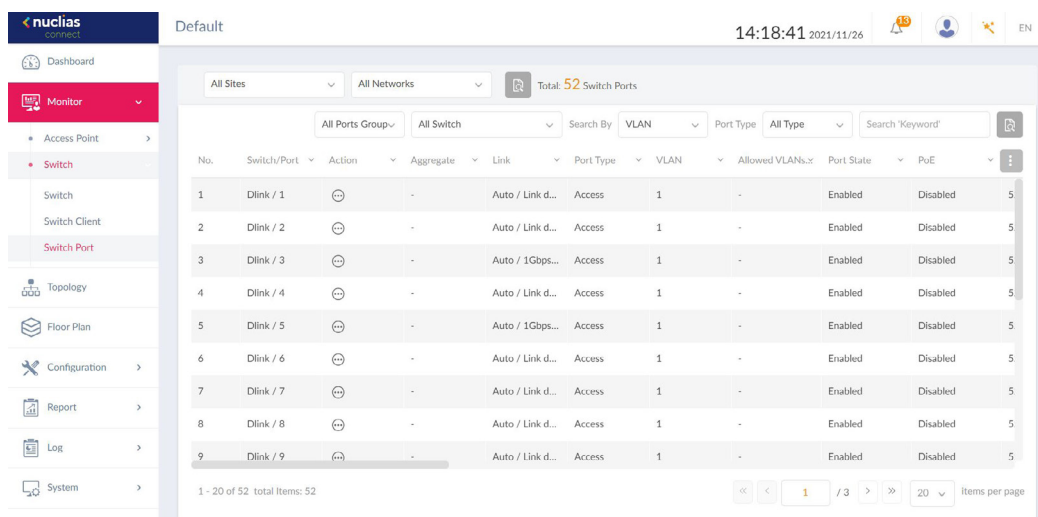
Nuclias Connect Monitor










Switch

Switch Port


Under the Switch Port section, you can view the statuses of all the switch ports from all sites and networks. Use the Sites and Networks drop-down menu to filter the search. Click  to start the search. Subsequently, use the Ports Group and Switch drop-down menu to filter the search, and select **VLAN/Port** and **Access/Trunk/All** from the **Search By** and **Port Type** drop-down menu respectively. Under the Search column, enter a relevant keyword to narrow the search. Click  to start the search.

The following information is displayed: **Number, Switch/Port, Aggregate, Link, Port Type, VLAN, Allowed VLANs, Port State, PoE, Ports, RSTP, LBD, DDP, Port Shutdown Schedule, PoE Supply Schedule, Access Policies, Mirror, LLDP, Port Name, Rx Broadcast Packets, Tx Broadcast Packets, Rx Multicast Packets, Tx Multicast Packets, Rx Bytes, Tx Bytes, Rx Packets, Tx Packets, and Total Bytes.**

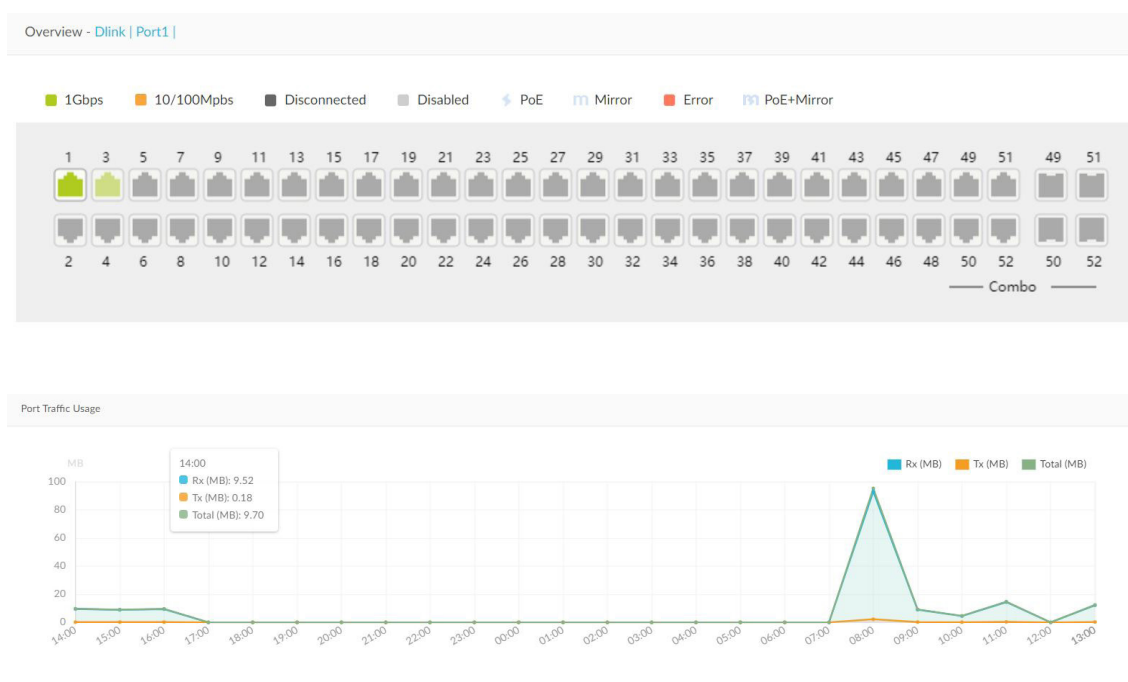


No.	Switch/Port	Action	Aggregate	Link	Port Type	VLAN	Allowed VLANs	Port State	PoE	Ports
1	Dlink / 1		-	Auto / Link d...	Access	1	-	Enabled	Disabled	5
2	Dlink / 2		-	Auto / Link d...	Access	1	-	Enabled	Disabled	5
3	Dlink / 3		-	Auto / 1Gbps...	Access	1	-	Enabled	Disabled	5
4	Dlink / 4		-	Auto / Link d...	Access	1	-	Enabled	Disabled	5
5	Dlink / 5		-	Auto / 1Gbps...	Access	1	-	Enabled	Disabled	5
6	Dlink / 6		-	Auto / Link d...	Access	1	-	Enabled	Disabled	5
7	Dlink / 7		-	Auto / Link d...	Access	1	-	Enabled	Disabled	5
8	Dlink / 8		-	Auto / Link d...	Access	1	-	Enabled	Disabled	5
9	Dlink / 9		-	Auto / Link d...	Access	1	-	Enabled	Disabled	5

Key Fields	Description
Switch/ Port	Displays the switch name and the port number.
Aggregate	Displays the link aggregation type (Static/LACP/-) of the port-channel group.
Link	Displays link configuration and link status of the port.

Under the **Action** field, click  to go to the Port Detail page. You'll be directed to detail page for the specific port of the switch you have selected.

In the **Port Detail** page, you get an overview on the **Switch Port Connection Status, Port Traffic Usage, Current Configuration, Port Status, Testing Tools including Cable Test and Cycle PoE, Packet Overview and Client Information.**



Current Configuration

Use Configuration

Profile

Cross Attributes

Switch Ports

Dlink / 1

Update 1 ports

Link (RJ45)

Auto

Port State

Enabled

Port Type

Access

RSTP

Enabled

VLAN

1

Access Policies

Disabled

DDP

Enabled

Port Shutdown Schedule

unscheduled

LBD

Disabled

STP Guard

Disabled

Uncross Attributes

Port Name

Link Aggregation Group

-

Mirror

-

Apply

Status

Port Utilization	0%	Port State	Connected
RSTP	-	PoE	Not PoE
LBD	Disabled	Link Negotiation	1Gbps Full Duplex
Link Aggregation Group	-		
Description	Access Port using Access VLAN 1		

Trouble Shooting

Cable Test

Run a Cable Test on This Port

Test

Warning: This test will disrupt traffic to devices

Cable Test Result

Ports ...	Type	Link Stat...	Test Resu...	Cable Length ...
<div><div></div>No data found</div>				

Cycle PoE

Disabled and Re-enable PoE

Test

PoE is not supported in the switch

Warning: PoE powered devices will be temporarily powered down.

Cycle PoE Test Result

Overview Packets

Time Frame Last 15 Minute



	Total	Rx	Tx	Rate (Rx,Tx)
Total Traffic	13769	13092	677	-
Broadcast	3392	3392	0	-
Multicast	9237	9237	0	-
CRC Error	0	0	-	-
Discard	438	438	0	-
Fragment	0	0	-	-
Collision	0	-	0	-
Error	0	0	0	-

Client Information

Search By

Client MAC Ad




e.g. 3c:1e: 04:16:53:20



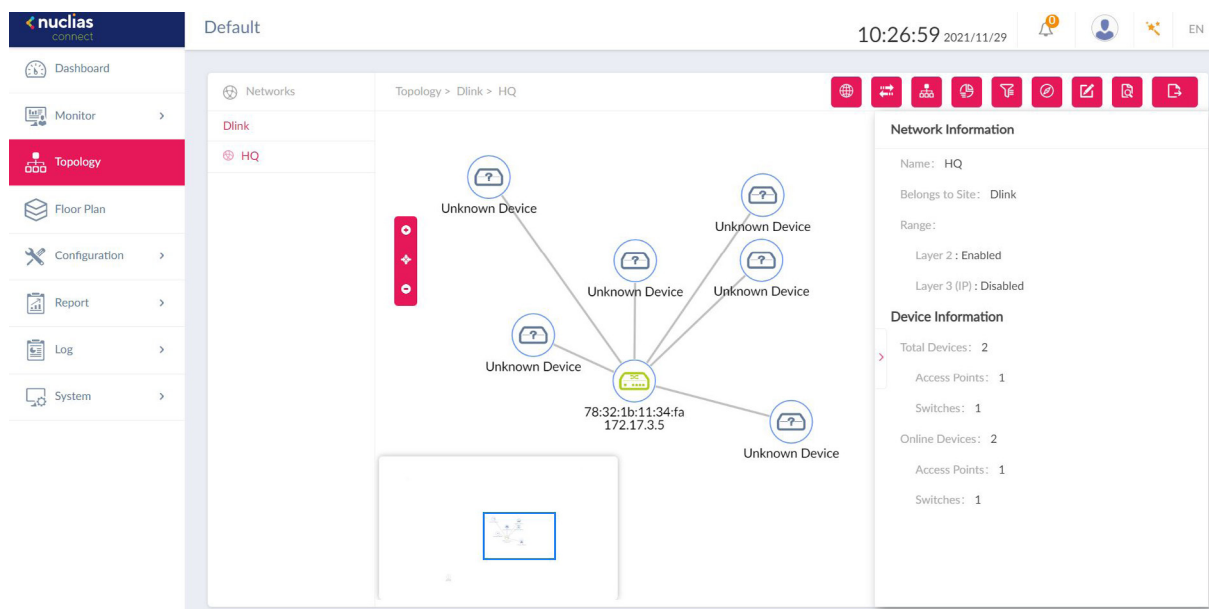
No.	Client Mac Address	Client IPv4 Address	Port	VLAN	LLDP	Manufacture	
1	00:0e:c6:f5:50:38	-	1	1	-	-	
2	00:1d:aa:3f:ea:a9	-	1	1	-	-	
3	00:1e:58:98:8f:5e	-	1	1	-	-	
4	00:1e:e3:12:34:56	-	1	1	-	-	
5	00:13:46:d4:e8:83	-	1	1	-	-	
6	00:23:7d:9e:b1:70	-	1	1	-	-	
7	00:24:b2:58:ee:ab	-	1	1	-	-	

Nuclias Connect

Topology

Under the Topology page, users can view the topological relations between switch devices and access points in a network. Press  to zoom in,  to zoom out, and  to reset the topology. A basic network and device summary is displayed. The following information is included: Network name, Belonging Site, Range, Total Device/Switch, Online Device/Switch.

Select an access point or switch from the site and network. The Device and Link information will be displayed on the right side. Clicking on the green device icon will reveal detailed device information. Clicking on the link will reveal the Link information.



AP Device Detail

Field	Description
Name	Displays the name to identify the switch on server. Click the name to be redirected to the device detail page. Note that the AP name must be unique to the Site.
Status	Displays the connection status of the AP: Online, Offline or Unmanaged. Green indicates online, red indicates offline.
Local IP Address	Displays the IP address.
MAC Address	Displays the system MAC address of the device.
Model Type	Displays the model type of the device.
Hardware Version	Displays the hardware version of the device.
FW version	Displays the Firmware version
CPU Usage (%)	Displays the CPU Usage of the device.
Memory Usage (%)	Displays the memory usage of the device.
Upload	Displays the upload traffic of the device.
Download	Displays the download traffic of the device.
Uptime	Display the activating time of the AP since after last start or reboot.
Location	Displays the location of the device.

Device Information


Name:	Dlink	⋮
Status:	●	
Local IP Address:	10.90.90.90	
MAC Address:	00:ad:24:a2:d5:20	
Model Type:	DGS-1210-52	
Serial Number:	QBDES12105200	
IGMP Snooping:	Disabled	
HW Version:	F3	
FW Version:	v6.30.015	
CPU Usage (%):	19	
Time Zone:	(GMT+08:00) Taipei	
RSTP Root:	RSTP is disabled	
LBD:	Disabled	
DDP:	Enabled	

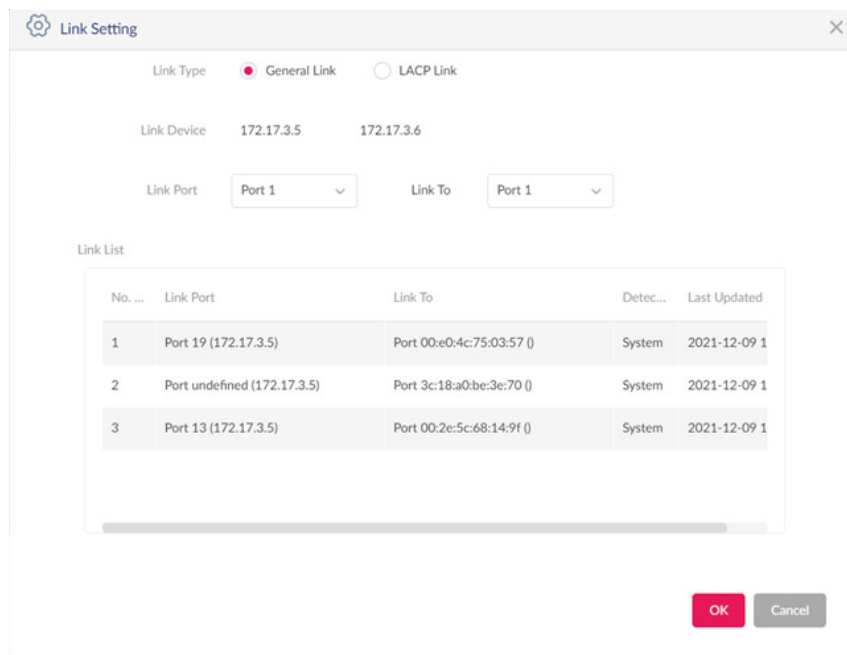
Nuclias Connect

Topology

Switch Device Detail

Field	Description
Name	Displays the switch name on the server. Click the name to be directed to the device detail page. Note that the switch name must be unique to the Site.
Status	Displays the connection status of the switch: Online or offline. Green indicates online, red indicates offline and is unreachable by the server.
IP Address	Displays the IPv4 address. Note: User configured IPv4 address is displayed when the device is unknown.
MAC Address	Displays the system MAC address of the switch.
Model Type	Displays the model type of the switch.
Serial Number	Displays the serial number of the switch.
IGMP Snooping	Displays the state of IGMP snooping.
RSTP Root	Displays the root bridge and its spanning tree priority. Display format. <ul style="list-style-type: none"> • "Root is X/ root bridge priority: Y" X represents device name (System name) of the root switch. Y represents bridge priority of root switch. • "RSTP is disabled" - When RSTP is not enabled on the switch - RSTP is enabled only on the switch, not the ports. • "-" When the switch is offline or doesn't relay the information.
DDP	Display the DDP setting of the switch.
LBD	Display the LBD setting of the switch.
IGMP Snooping	Displays the state of IGMP snooping.
Hardware Version	Displays the hardware version of the switch.
CPU Usage (%)	Displays the CPU Usage of the switch.
FW Version	Displays the Firmware version of the switch.
Time zone	Displays the time zone which the device belongs to.
Uptime	Display the activating time of the switch after the last start or reboot.
Location	Displays the location of the switch.

Users can also view relations between two devices by manually defining the link. Click  to begin edit. Click on one of the targeted device icon, then click another device icon to create a linkage. Once created, the Link Setting page is displayed. Below charts explain what each field entails.



The Link Setting dialog box is used to configure a link between two devices. It includes fields for Link Type, Link Device, Link Port, and Link To. Below these fields is a Link List table showing existing links.

Link Setting

Link Type: ☒ General Link ☐ LACP Link

Link Device: 172.17.3.5 172.17.3.6








Link Port: Port 1 Link To: Port 1

Link List

No. ...	Link Port	Link To	Detec...	Last Updated
1	Port 19 (172.17.3.5)	Port 00:e0:4c:75:03:57 ()	System	2021-12-09 1
2	Port undefined (172.17.3.5)	Port 3c:18:a0:be:3e:70 ()	System	2021-12-09 1
3	Port 13 (172.17.3.5)	Port 00:2e:5c:68:14:9f ()	System	2021-12-09 1

OK Cancel

On the upper right corner, there are options available to modify and check basic information of the switches and access points.

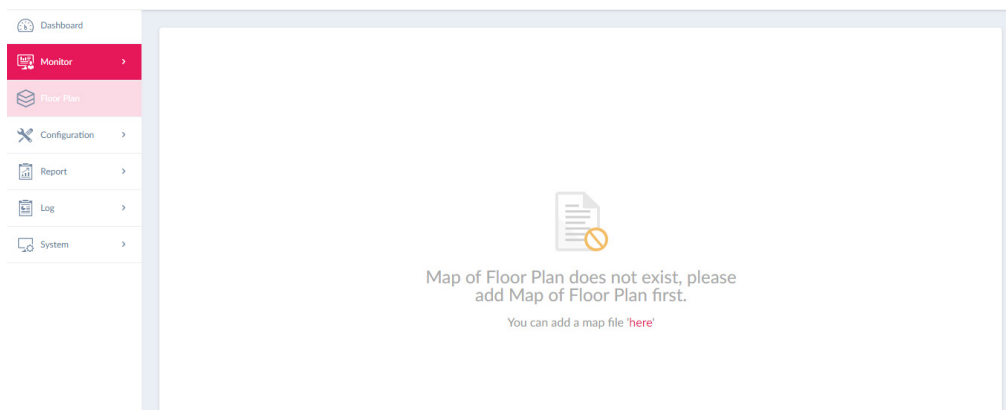
Click  to show Network and Device information. Click  to change the background image of the topology. Click  to configure the arrangement type (Star/Tree) and Central Device. Click  to view the Topological Legend, or the meaning of symbols and colors used on the topology. Click  to set the display content for node information (IP Address or Name). Click  to rediscovery the topology. Click  to search for matching devices in the network, and finally, click  to export the topology as a PDF file.

Nuclias Connect

Floor Plan

Floor plan is a drawing to scale, a bird's-eye view of the relationships between rooms, spaces, traffic patterns, and other physical features at one level of a structure.

Click "here" to add a new floor image, enter a name and select Site and Network.



Click "choose a picture" to upload the image, then click "Save".

Name*

Site*

Network*

Upload Image*

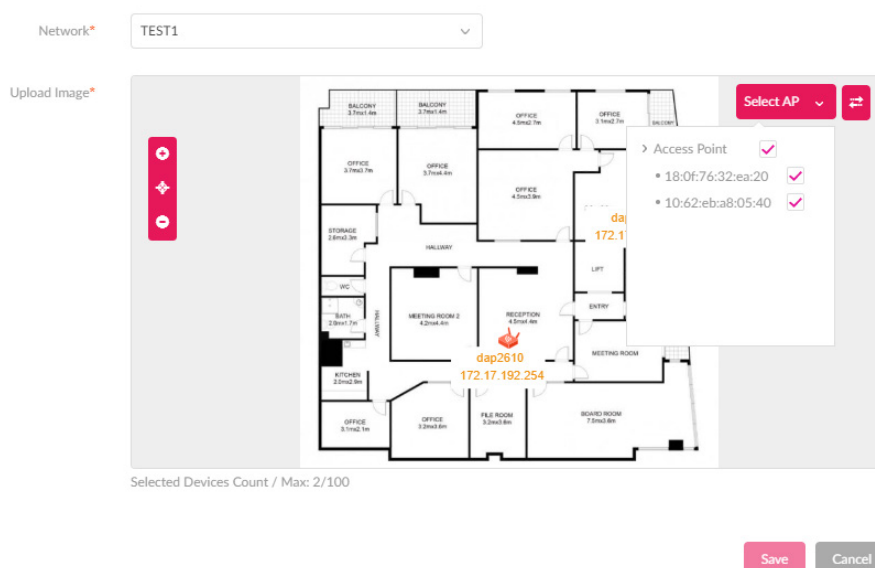
Drag & Drop

Your Picture Here (file format is ".png",".jpg", size is up to 10M)

or

Click to [choose a picture](#)

Click **Select AP** to choose devices, move devices to the correct position and save it.









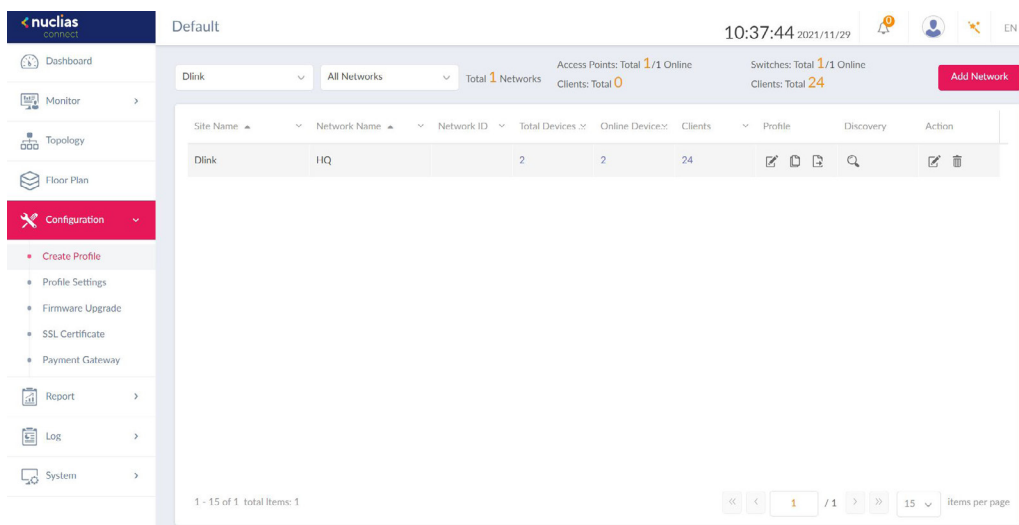
Nuclias Connect

Configuration

Create Profile

Navigate to **Configuration > Create Profile**, click **Add Network** to create a new site and network. All available sites and networks are listed in the Default page. See the following for further information.

Field	Description
Edit Profile 	Opens Profile Settings page of the selected site. The security, access control, user authentication settings , many more are available.
Copy Profile to this Network 	Copy existing profile to a designated site and network.
Export Network Profile 	Export selected profile to a file (*.dat) on a local directory.
Discovery 	Opens the Discovery Network Settings page. From this page, you can search for devices located on L2 protocol layer or specific IP addresses / Prefix subnet IPs. Once the criteria is defined, click Next . Click Start Discovery to find begin the search(Configurable and Managed devices).
Edit Network 	Opens the Edit Network page. From this page, you can edit network settings or migrate to a new or existing site.
Delete Network 	Delete the selected network configuration.



The screenshot displays the Nuclias Connect Configuration interface. The top navigation bar includes the Nuclias Connect logo, a 'Default' tab, and a clock showing 10:37:44 on 2021/11/29. The main content area shows a table of networks with columns for Site Name, Network Name, Network ID, Total Devices, Online Devices, Clients, Profile, Discovery, and Action. The table contains one entry for 'Dlink' with Network ID '11Q', 2 total devices, 2 online devices, and 24 clients. The sidebar on the left lists various configuration options under 'Configuration', including 'Create Profile', 'Profile Settings', 'Firmware Upgrade', 'SSL Certificate', and 'Payment Gateway'. The bottom of the page shows pagination information: '1 - 15 of 1 total items: 1' and a dropdown for '15 items per page'.

Nuclias Connect Configuration Create Profile Add Network

From the Create Profile link, click on **Add Network** to create a new network.

The Add Network page is displayed. From the Site drop-down menu, select an existing site or a new Site and enter the name of the site in the empty field.

In the Network Name field, enter the name to identify the new network. Click **Next** to continue or **Exit** to return to the previous screen.

The Network Configurations page will appear. Enter the wireless and device settings to define the network configuration. Click **Next** to continue. To return to the previous page, click **Back** or click **Exit** to discontinue the configuration process. The Network ID field is optional and is used for REST API function. Leave it as empty if you're not intended to use REST API.

Add Network

Site

newSite

Network Name

Network1

Network ID

The network ID will be used for REST API.

Next

Exit

Network Configurations

General Settings

Country

Taiwan

Time Zone

(GMT+08:00) Taipei

Device Type

☐ Access Point ☐ Switch

Please select the device type that will be managed in the network.

Access Point

Admin

Username

admin

Password

SSID Name

dlink

Security

WPA-Personal

SSID Password

SSID Setting

☐ Add Guest SSID (Optional)

Guest SSID Name

Switch

Series Supported

☐ DGS-1210

Username

admin

Password



Back

Next

Cancel

Nuclias Connect Configuration Create Profile Add Network

The Discover Network Settings page is displayed. Select the data link layer (layer 2 or layer 3) to define the type of network to run on. If Layer 3 is selected, click the drop-down menu to define either an IP or a prefix segmentation. Click **+** to add additional IP/prefix segments or **Next** to continue. Click **Exit** to discontinue the configuration process.

 Discover Network Settings 

☒ Layer 2

☒ Layer 3 (IP)

IP

192.168.1.150

-

192.168.1.200

—

Pick one...



-

+

Next

Exit

The Start Discovery Page is displayed. Click **Start Discovery** to search for all available unmanaged devices. If a device is found, select it and click **Apply** to import the network profile. Click on the Managed tab to select defined devices and add them to the network.

 Discovery AP 

Re-Discovery

Scan Finished (2019-01-03 15:14:34)

Configurable

Managed

☒

State

IP Address

MAC Address

Model Type

NMS URL

Network

☒


Unregistered

192.168.1.166

40:9b:cd:0c:66:20

DAP-2680

192.168.1.61:8443

Import Network Profile: * 

Apply

Back

Exit

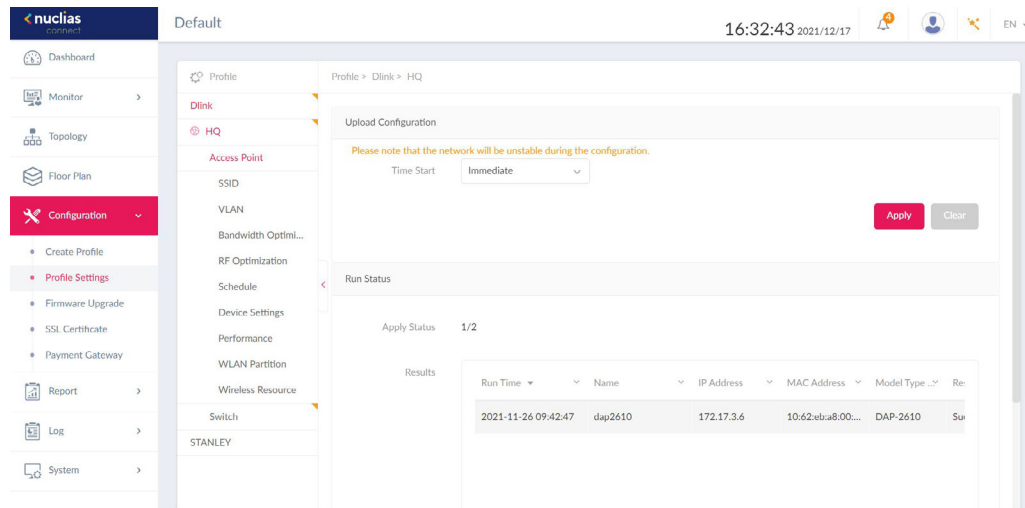
Nuclias Connect

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 a network to view all settings that are available for edit. For Access Points, the below options are displayed: **SSID, VLAN, Bandwidth Optimization, RF Optimization, Schedule, Device Setting, Performance, WLAN Partition, and Wireless Resources**. For Switches, the following options are displayed: Common settings (**RADIUS Server and Time Profile**) and **Switch series (Basic, IPv4 ACL, Access Policy, Port Setting, and SNMP)**.

Once a network is selected, the Upload Configuration and Run Status will become available for both switches and access points.



For the configuration to take effect, it must be uploaded to the access point/switch. Under the **Upload Configuration** tab, click the **Time Start** drop-down menu and select **Immediate** or **Select Time** to set the time for uploading the configuration.

If **Select Time** is selected, set the day and time to upload the configuration. Once the Time Start is defined, click **Apply** to initiate the process.

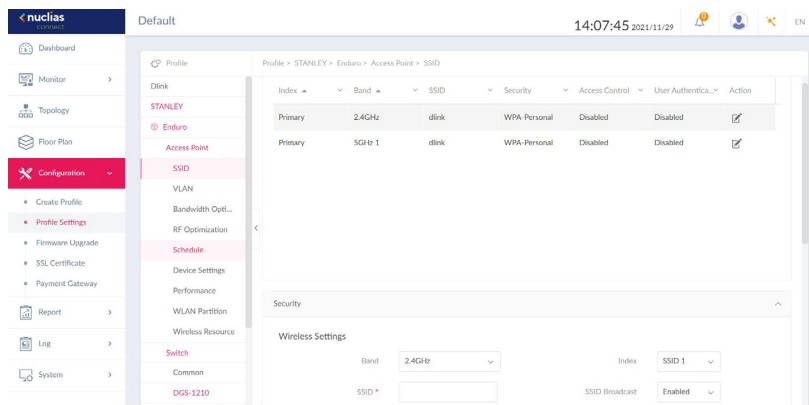
Under the **Run Status** window, the status of the upload configuration is reported. Once an update is complete, the results will be displayed in the **Results** window.

Nuclias Connect Configuration Profile Settings Access Point

SSID

If the device type of the profile chosen is an Access Point, the following options are displayed: **SSID, VLAN, Bandwidth Optimization, RF Optimization, Schedule, Device Settings, Performance, WLAN Partition, and Wireless Resource.**

The SSID page displays the configurable parameters of a network's wireless settings. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Access Point > SSID** to view existing settings.



In the **Security** section, the following parameters can be configured:

Field	Description
Band	Click the drop-down menu to select wireless frequency band.
Index	Click the drop-down menu to select SSID index (Parameters: Primary, SSID 1 to SSID 7). To create a new SSID, select the index parameter first.
SSID	Enter the wireless network name. The SSID must be the same across all frequencies. In addition, make sure the network name (SSID) on the selected access point is the same as the defined network name (SSID) on Nuclias Connect. For further information, go to Access Point Basic > Wireless Settings and Advanced Settings > DHCP Server > Dynamic Pool Settings, to ensure the Domain Name field reflects the defined network name (SSID) on Nuclias Connect.
Character Set	Click the drop-down menu to select the character set to be used in the SSID encoding: UTF-8 or GB2312.
SSID Broadcast	Click the drop-down menu to enable or disable the wireless SSID visibility.
WMM (Wi-Fi Multimedia)	Click the drop-down menu to enable or disable the Wi-Fi multimedia.
Security	Click the drop-down menu to select the wireless security protocol: Open System (no pre-shared key required), WPA-Personal, WPA Enterprise (Radius server required), WPA2-Personal, WPA2-Enterprise (Radius server required), WPA-Auto-Personal, WPA-Auto-Enterprise (Radius server required).
Fast Roaming	Select Enabled to enable Fast Roaming function on AP. (Applicable only to APs that support this function.)
Encryption	Click the drop-down menu to enable or disable WEP Open System encryption. The function is only available when Security is set to Open System .
Key Size	Click the drop-down menu to select the WEP key size.
Key Type	Click the drop-down menu to select the WEP key type.
Key Index	Click the drop-down menu to select the WEP key index.
Key Value	Enter the open system WEP encryption key.

Nuclias Connect Configuration Profile Settings Access Point SSID



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

Block	Description
Action	Click the drop-down menu to select the action that will applied to the clients.
MAC Address	Enter the MAC address of the clients that will be allowed or denied access and click Add .
Upload MAC Address List	Click Browser... to select a MAC address file located on the local computer. Click Upload to update the MAC address list. Click Download to download the current MAC address list.
Action	Click on the drop-down menu to enable or disable the IP filter function.
IP Address	Enter the IP address.
Subnet Mask	Enter the subnet mask.

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

Block	Description
Authentication Type	Click the drop-down menu to select the authentication type applied to the wireless client. (Web redirection only, User name/Password, Remote Radius, LDAP, POP3, Passcode, External Captive Portal, MAC address, Click through and Social Login)
Idle Timeout (2~1440)	Enter the session timeout value.
Session timeout	Define how long wireless client can use network without re-login.
Allow	Define how many times wireless client can re-login per day(The start time is 0:00)
Interval	Define how long wireless client can login after session timeout.
Enable White List	Check the box to enable the white list function. This function is only available when Authentication Type is Username/Password .
MAC Address	Enter the MAC address of the network device that will be whitelisted and click Add to add the address to the white list table. This function is only available when Authentication Type is set to Username/Password .
Upload Whitelist File	Click Browser... to select a white list file, located on the local computer. Click Upload to update the white list. Click Download to download the current white list. The function is only available when Authentication Type is set to Username/Password .
IPIF Status	Click the drop-down menu to enable or disable the use of the IP interface.
VLAN Group	Enter the VLAN group name.
Get IP Address From	Click the drop-down menu to select the IP address configuration setting.
IP Address	Enter the IP address of the IP interface.
Subnet Mask	Enter the subnet mask of the IP interface.
Gateway	Enter the gateway of the IP interface.
DNS	Enter the preferred DNS address of the IP interface.
Username	Enter the username. The function is only available when Authentication Type is set as Username/Password .

Block	Description
Password	Enter the password and click Add . Click Clear to clear the entered fields. This function is only available when Authentication Type is set to Username/Password .
RADIUS Server	Enter the RADIUS server's IP address. This function is only available when Authentication Type is set to Remote RADIUS or MAC Address .
RADIUS Port	Enter the RADIUS server's port number. This function is only available when Authentication Type is set to Remote RADIUS or MAC Address .
RADIUS Secret	Enter the RADIUS server's secret. This function is only available when Authentication Type is set to Remote RADIUS or MAC Address .
Remote RADIUS Type	Enter the RADIUS server's type. This function is only available when Authentication Type is set to Remote RADIUS or MAC Address .
Server	Enter the LDAP server's IP address. This function is only available when Authentication Type is set to LDAP .
Port	Enter the LDAP server's port number. This function is only available when Authentication Type is set to LDAP .
Authentication Mode	Click on the drop-down menu to select the authentication mode. This function is only available when Authentication Type is set to LDAP .
Username	Enter the administrator's username to access and search the LDAP database. This function is only available when Authentication Type is set to LDAP .
Password	Enter the administrator's password to access and search the LDAP database. This function is only available when Authentication Type is set to LDAP .
Base DN	Enter the base domain name of the LDAP database. This function is only available when Authentication Type is set to LDAP .
Account Attribute	Enter attribute for the account. This function is only available when Authentication Type is set to LDAP .
Identity	Enter the name of the administrator. This function is only available when Authentication Type is set to LDAP .
Server	Enter the POP3 server's IP address. This function is only available when Authentication Type is set to POP3 .
Port	Enter the POP3 server's port number. This function is only available when Authentication Type is POP3 .
Connection Type	Click the drop-down menu to select the connection type. This function is only available when Authentication Type is set to POP3 .
Passcode List	Display the configured front desk user accounts that have been assigned to this network and have generated a passcode from the Web login page.
Account Server Status	Click the drop-down menu to select HTTP or HTTPS. After selecting, enter the URL of the website. This function is only available when Authentication Type is set to External Captive Portal .
Web Redirection	Check the box to enable the website redirection function.
Website	Click the drop-down menu to select HTTP or HTTPS. After selecting, enter the URL of the website.

Block	Description
Choose Template	<p>Click the drop-down menu to select the used login style. This function is only not available when Authentication Type is set to Web Redirection Only.</p> <ul style="list-style-type: none">• Click Preview to preview the selected style.• Click Upload Login File to upload a new style.• Click  to delete the selected style.• Click  to download the style template.

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

Click **Reset** to reset all settings.

Click **Cancel** to restore default value.

Once the settings are updated, the configuration must be uploaded to the access points. See “Profile Settings” on page 69 for further information.

Nuclias Connect Configuration Profile Settings Access Point


VLAN


The VLAN page will show the configurable settings of a network's virtual LAN subnetwork settings. Navigate to **Configuration > Profile Settings > [Site] > [Network] > VLAN** to view existing settings.

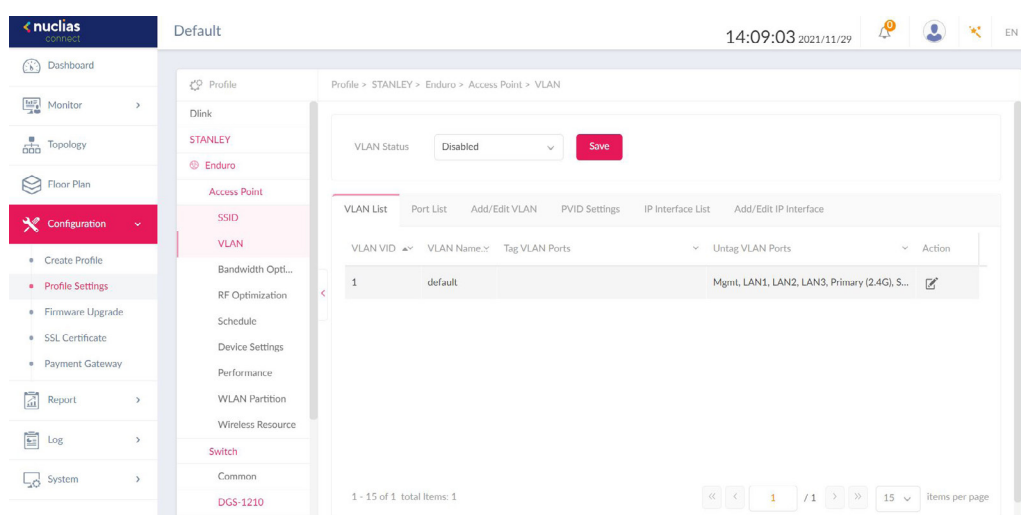
Block	Description
VLAN Status	Click the drop-down menu to enable or disable VLANs.

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

The **VLAN List** tab will show a list of all created VLANs.

Click  to modify an existing VLAN.

Click  to remove an existing VLAN.



In the **Port List** tab, a list of port assignments is displayed. The list shows the tagged and untagged ports available on the access points in the network.

In the columns next to the Port Name entries, the Tag/Untag ID columns indicate if the port is a tagged member (Tag VID) or an untagged member (Untag VID) of the VLAN. In the last column, the port VLAN ID shows the connected virtual LAN segment.

In the **Add/Edit VLAN** tab, you can create a new VLAN and assign untagged ports in that VLAN. Click the Modify icon in the VLAN List tab to modify an existing VLAN.

In the **PVID Setting** tab, you can view and configure the Port VLAN Identifier (PVID) settings for access points and wireless client in this network.

In the **IP Interface List** tab, you can view a summary of IP Interface. The following information is listed: VLAN VID, VLAN Name, Get IP Address From, and IP Address. Under the action field, click  to revise, or click  to delete.

In the **Add/Edit IP Interface** tab, you can add or edit IP interface. The following fields are presented: VLAN VID, Get IP Address From, IP Address, Subnet Mask, Gateway, and DNS. Click **Save** to save your changes.

Once the settings are updated, the configuration must be uploaded to the access points. See "Profile Settings" on page 69 for further information.

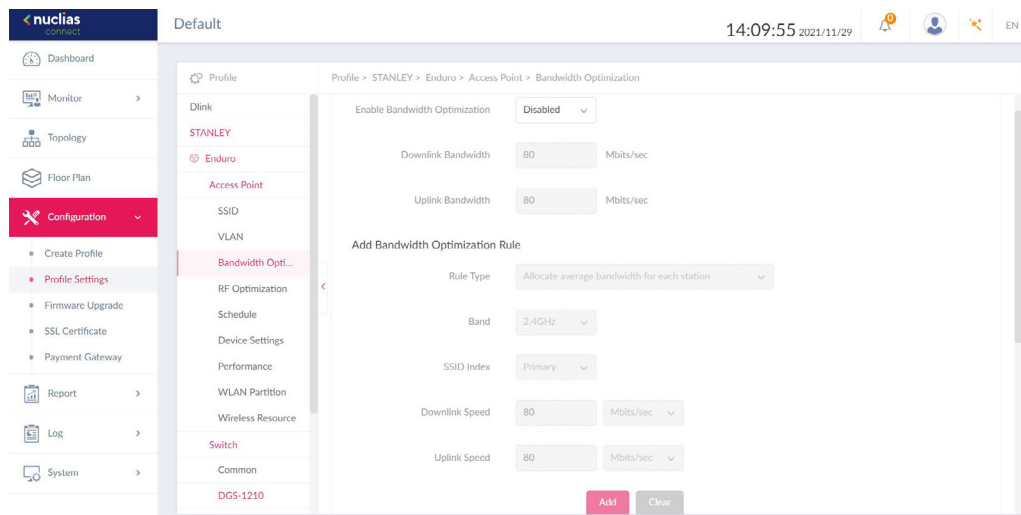
Nuclias Connect Configuration Profile Settings Access Point

Bandwidth Optimization

The Bandwidth Optimization page displays the configurable settings to optimize available bandwidth. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Bandwidth Optimization** to view existing settings.

Block	Description
Enable Bandwidth Optimization	Click the drop-down menu to enable or disable the bandwidth optimization function.
Downlink Bandwidth	Enter the total downlink bandwidth speed for the access points in the network.
Uplink Bandwidth	Enter the total uplink bandwidth speed for the access points in the network.
Rule Type	Click the drop-down menu to select the rule type. <ul style="list-style-type: none"> Allocate an average BW for each station: Optimize bandwidth by averaging the allocated bandwidth for each client. Allocate a maximum BW for each station: Specify the maximum bandwidth for each connected client, while reserving available bandwidth for additional clients. Allocate a different BW for 11a/b/g/n station: The weight of 802.11b/g/n and 802.11a/n clients are 10%/20%/70% and 20%/80%. The AP will distribute different bandwidth for 802.11a/b/g/n clients. Allocate a specific BW for SSID: All clients share the assigned bandwidth.
Band	Click the drop-down menu to select the wireless frequency band used in the rule.
SSID Index	Click the drop-down menu to select the SSID used in the rule.
Downlink Speed	Enter the downlink speed assigned to either each station or the specified SSID.
Uplink Speed	Enter the uplink speed assigned to either each station or the specified SSID.
Add	Click Add to add the rule 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” on page 69 for further information.

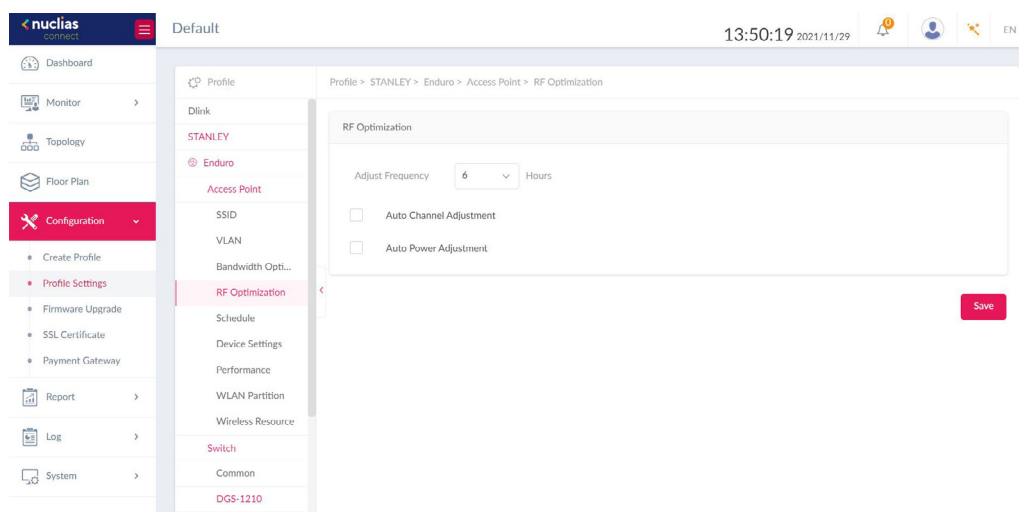
Nuclias Connect Configuration Profile Settings Access Point

RF Optimization

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

Block	Description
Adjust Frequency	Click the drop-down menu to set the rate in hours at which the RF frequency is adjusted.
Auto Channel Adjustment	Click the Auto RF Optimize radio button to 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. Click the radio button to 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” on page 69 for further information.

Nuclias Connect Configuration Profile Settings Access Point

Schedule

Under the Schedule page, you can configure a schedule to keep the SSID active within a specified time. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Schedule** to view settings.

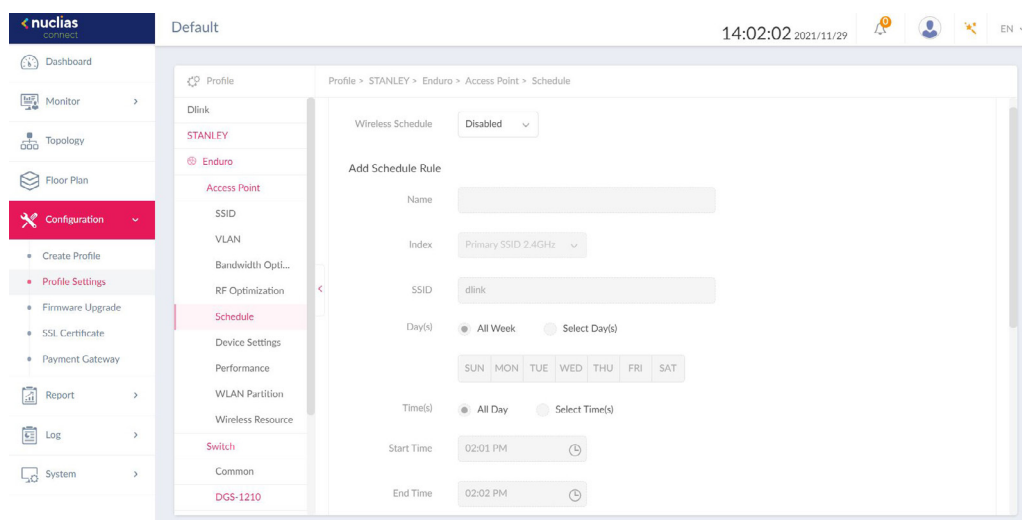
Parameter	Description
Wireless Schedule	Click the drop-down menu to enable or disable the wireless schedule function.
Name	Enter the name of the schedule rule.
Index	Click the drop-down menu to select SSID to which the schedule setting is applied.
SSID	Display the SSID name.
Day(s)	Click the radio button to select the active days for the schedule. <ul style="list-style-type: none"> All Week: Enable the rule for the whole week. Select Day(s): Specify particular day(s) to activate the rule.
Time(s)	Click the radio button to select the active times for the schedule. <ul style="list-style-type: none"> All Day: Enable the rule for the whole day. Select Time(s): Specify a start and end time for the rule.
Start Time	Enter the hours and minutes of the day. This function is only available when Time(s) is set as Select Time(s) .
End Time	Enter the hours and minutes of the day. This function is only available when Time(s) is set as Select Time(s) .
Over Night	Check the box to enable activity overnight.
Add	Click Add to add the rule into the schedule.
Clear	Click Clear to clear the entered rule.

Click  to modify the desired rule.

Click  to delete the desired 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" on page 69 for further information.



Nuclias Connect Configuration Profile Settings Access Point

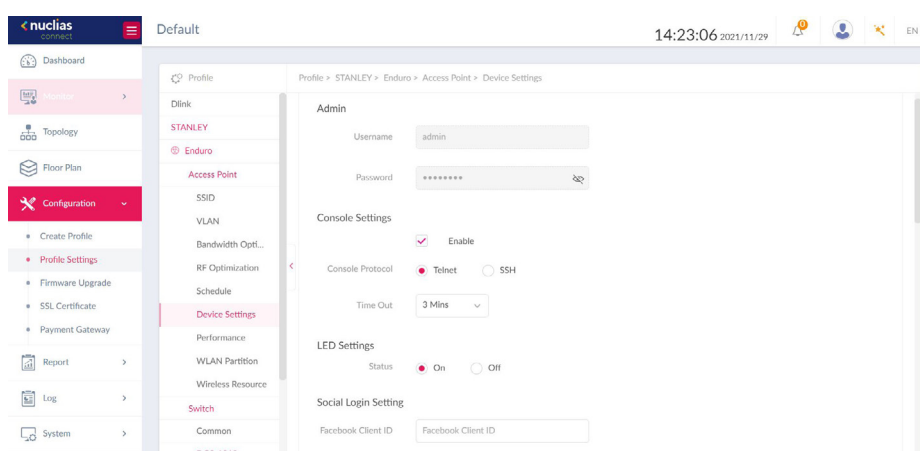
Device Setting

The Device Settings page allows you to view and configure the login and accessibility settings for access points in this network. Advanced wireless settings can be configured for both the 2.4GHz and 5GHz frequency bands. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Device Setting** to view existing settings.

Parameter	Description
Username	Enter the administrative username that is used to access the configuration settings for all access points in the network.
Password	Enter the administrative password that is used to access the configuration settings for to all access points in the network.
Enable	Check the box to enable the console function.
Console Protocol	Click the radio button to select the console protocol that is applied to all access points in the network.
Time Out	Click the drop-down menu to select the active console session time out value.
Enable NTP Server	Check the box to enable the Network Time Protocol (NTP) server function.
NTP Server	Enter the IP address or domain name of the NTP server.
Select Country	Click the drop-down menu to select the country region of APs in the network.
Time Zone	Click the drop-down menu to select the time zone.
Enable Daylight Saving	Check the box to enable the daylight saving function.
DST Start (24HR)	Click the drop-down menu to designate the start date and time for Daylight Saving Time (DST).
DST End (24HR)	Click the drop-down menu to designate the end date and time for Daylight Saving Time (DST).
DST Offset (minutes)	Click the drop-down menu to select DST Offset time.
External Syslog Server	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 related access points. See "Profile Settings" on page 69 for further information.



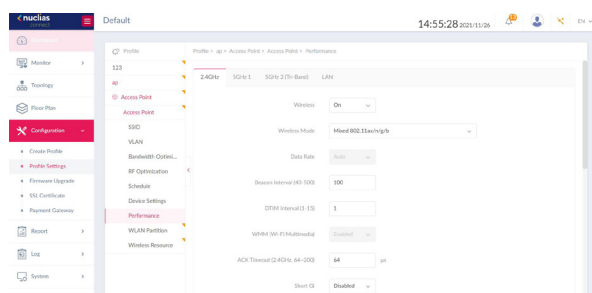
Nuclias Connect Configuration Profile Settings Access Point Performance

2.4GHz/5GHz/5GHz 2 (Tri-Band)

The Schedule page allows you to configure the wireless performance for access points on your network. Additionally, advanced wireless settings can be configured on the page for both the 2.4GHz and 5GHz frequency bands. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Access Point > Device Settings** to view existing settings. Click the 2.4GHz or 5GHz tab to view existing settings.

Parameter	Description
Wireless	Click the drop-down menu to turn on or off the wireless band for the network.
Wireless Mode	Click the drop-down menu to select the wireless mode used in the network.
Data Rate	Click the drop-down menu to select the wireless data rate. The function is only available when Wireless Mode is set as Mixed 802.11g and 802.11b (2.4GHz) or 802.11a Only (5GHz) .
Beacon Interval	Enter the beacon interval value. The default value is 100.
DTIM Interval (1-15)	Enter the DTIM interval value. The default value is 1.
WMM (Wi-Fi Multimedia)	Click the drop-down menu to enable or disable the Wi-Fi Multimedia (WMM) function.
ACK Timeout	Enter the ACK timeout value. The default value is 48.
Short GI	Click the drop-down menu to enable or disable the short GI function.
IGMP Snooping	Click the drop-down menu to enable or disable the IGMP snooping function.
Multicast Rate	Click the drop-down menu to select the multicast rate value.
Multicast Bandwidth Control	Click the drop-down menu to enable or disable the multicast bandwidth control function.
Maximum Multicast Bandwidth	Enter the maximum multicast bandwidth value. The default value is 100. The function is only available when Multicast Bandwidth Control is Enabled .
HT20/40 Coexistence	Click the drop-down menu to enable or disable the HT20/40 coexistence function.
Change DHCP Offers from Multicast to Unicast	Click the drop-down menu to allow or deny the transfer of DHCP offers to unicast function.
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	Click the drop-down menu to select the channel width used by the network.

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

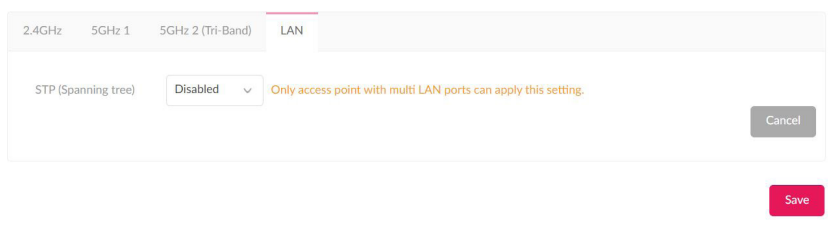


Once the settings are updated, the configuration must be uploaded to the access points. See "Profile Settings" on page 69 for further information.

Nuclias Connect Configuration Profile Settings Access Point Performance

LAN

Under the **LAN** tab, users can enable or disable **STP** (Spanning tree). STP can help ensure that no loops are created when you have redundant paths in your network. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Access Point > Performance > LAN**. Note that only access point with multi LAN ports can apply this setting.



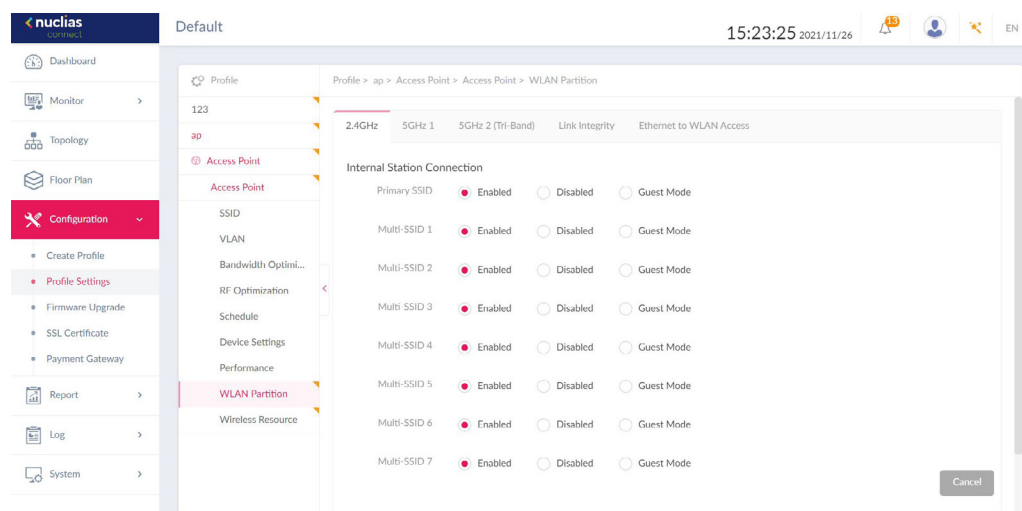
The screenshot shows a configuration window with four tabs: 2.4GHz, 5GHz 1, 5GHz 2 (Tri-Band), and LAN. The LAN tab is selected. Inside the LAN tab, there is a section for 'STP (Spanning tree)' with a dropdown menu set to 'Disabled'. A yellow warning message states: 'Only access point with multi LAN ports can apply this setting.' To the right of the dropdown is a 'Cancel' button. Below the configuration area is a red 'Save' button.

Once the settings are updated, the configuration must be uploaded to the access points. See “Profile Settings” on page 69 for further information.

Nuclias Connect Configuration Profile Settings Access Point

WLAN Partition 2.4GHz/5GHz/ 5GHz 2(Tri-Band)

The WLAN Partition page displays the wireless partitioning settings that allow you to enable/disable associated wireless clients from communicating with each other. Additionally, advanced wireless settings can be configured on the page for both the 2.4GHz and 5GHz frequency bands. Navigate to **Configuration > Profile Settings > [Site] > [Network] > WLAN Partition**. Click the 2.4GHz or 5GHz tab to view existing settings. Click **Save** to save the values and update the screen.



Once the settings are updated, the configuration must be uploaded to the related access points. See “Profile Settings” on page 69 for further information.

Nuclias Connect Configuration Profile Settings Access Point

WLAN Partition Link Integrity

The Link Integrity feature disassociates wireless segments from the AP when the LAN and AP is disconnected. Click the drop-down menu to enable or disable the wireless link integrity function.

Profile > ap > Access Point > Access Point > WLAN Partition

2.4GHz	5GHz 1	5GHz 2 (Tri-Band)	Link Integrity	Ethernet to WLAN Access
--------	--------	-------------------	----------------	-------------------------

Link Integrity

Enabled ▾

Cancel

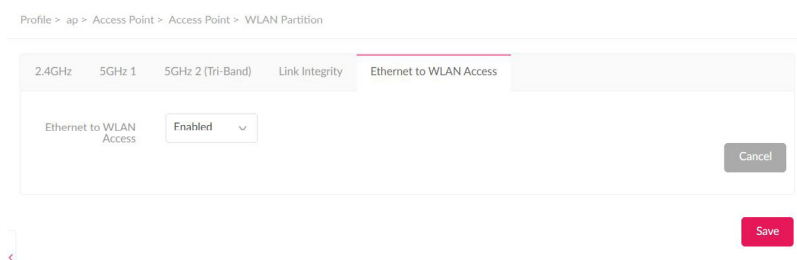
Save

Click **Save** to save the changes. Once the settings are updated, the configuration must be uploaded to the access points. See “Profile Settings” on page 69 for further information.

Nuclias Connect Configuration Profile Settings Access Point

WLAN Partition Ethernet to WLAN Access

The Ethernet to WLAN Access feature allows Ethernet to send and receive data from associated wireless devices. Click the drop-down menu to enable or disable Ethernet to WLAN Access.



Click **Save** to save the changes. Once the settings are updated, the configuration must be uploaded to the access points. See “Profile Settings” on page 69 for further information.

Nuclias Connect Configuration Profile Settings Access Point

Wireless Resource 2.4GHz/5GHz/ 5GHz 2(Tri-Band)

The Wireless Resource function in Nuclias Connect helps provide real-time RF management of the wireless network. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Wireless Resource**. Click the 2.4GHz or 5GHz tab to view existing settings.

Parameter	Description
ACL RSSI Threshold	Check the box to enable ACL RSSI threshold function and click the drop-down menu to select the ACL RSSI threshold percentage.
Aging Out	Click to enable the Aging Out function. From the menu, select a criteria to disconnect a wireless clients. Available options are RSSI and Data Rate.
RSSI Threshold	When RSSI is selected in the Aging out drop-down menu, select a value between 10% to 100%. This parameter sets the minimum RSSI for a wireless clients to respond to a probe. If the determined value is lower than the specified percentage, the wireless client is disconnected.
Data Rate	Click the drop-down menu to select the data rate connection limit. The function is only available when the Aging Out policy is set to Data Rate .
Connection Limit	Click the radio button to enable or disable the function. Connection limit is designed to provide load balancing. This policy allows user access management on the wireless network. The exact number is entered in the User Limit field below. If this function is enabled and the number of users exceed this value, or the network utilization exceeds the specified percentage, the policy will not allow further client association.
User Limit (0~64)	Enter the user connection limit. The default value is 20.
11n Preferred	Click the drop-down menu to enable or disable the preferred use of 802.11n.
Network Utilization	Click the drop-down menu to select the network utilization percentage.

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

The screenshot displays the configuration page for the 5GHz 2 (Tri-Band) profile. The top navigation bar includes tabs for 2.4GHz, 5GHz 1, 5GHz 2 (Tri-Band), Airtime Fairness, Band Steering, and Neighbor AP Detection. The 5GHz 2 (Tri-Band) tab is selected. The main content area contains several settings, each with a checkbox and a dropdown menu or input field. The settings are: ACL RSSI Threshold (checkbox), Aging Out (checkbox), RSSI Threshold (dropdown), Data Rate (dropdown), Connection Limit (checkbox), User Limit (0~64) (input field), 11n Preferred (dropdown), and Network Utilization (dropdown). A 'Cancel' button is located at the bottom right of the form.

Once the settings are updated, the configuration must be uploaded to the access points. See "Profile Settings" on page 69 for further information.

Nuclias Connect Configuration Profile Settings Access Point

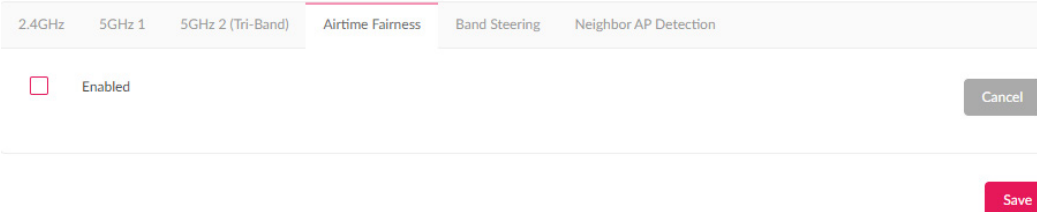
Wireless Resource Airtime Fairness

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.

Note: Devices identified as having slow WiFi speed may be attributed to long connection distance, weak signal strength or older legacy hardware. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Wireless Resource**. Click the **Airtime Fairness** tab to view the existing settings.

Check the box to enable or disable the airtime fairness function.

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



2.4GHz	5GHz 1	5GHz 2 (Tri-Band)	Airtime Fairness	Band Steering	Neighbor AP Detection
<input type="checkbox"/> Enabled					

Cancel

Save

Once the settings are updated, the configuration must be uploaded to the related access points. See "Profile Settings" on page 69 for further information.

Nuclias Connect Configuration Profile Settings Access Point

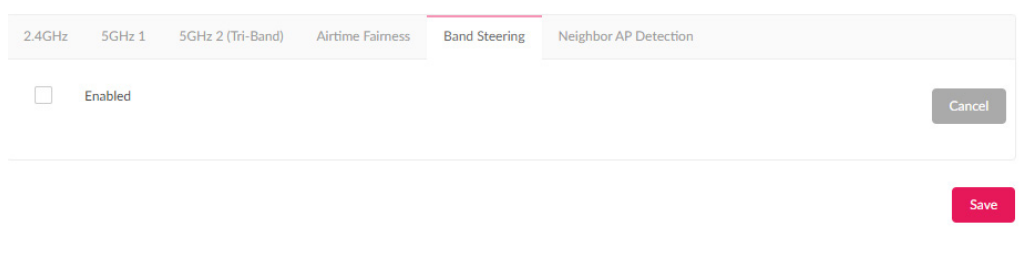
Wireless Resource Band Steering

Band Steering allows dual-band-capable clients to connect to the less crowded 5GHz network, and leave the 2.4GHz network available for clients that support 2.4GHz only.

Navigate to **Configuration > Profile Settings > [Site] > [Network] > Wireless Resource**. Click on the **Band Steering** tab to view the existing setting.

Check the box to enable or disable the wireless band steering function.

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



The screenshot shows a configuration interface with a horizontal tab bar at the top. The tabs are: 2.4GHz, 5GHz 1, 5GHz 2 (Tri-Band), Airtime Fairness, Band Steering (which is the active tab, highlighted with a pink underline), and Neighbor AP Detection. Below the tabs, there is a checkbox labeled "Enabled". To the right of the checkbox is a grey "Cancel" button. At the bottom right of the form area is a red "Save" button.

Once the settings are updated, the configuration must be uploaded to the related access points. See "Profile Settings" on page 69 for further information.

Nuclias Connect

Configuration

Profile Settings

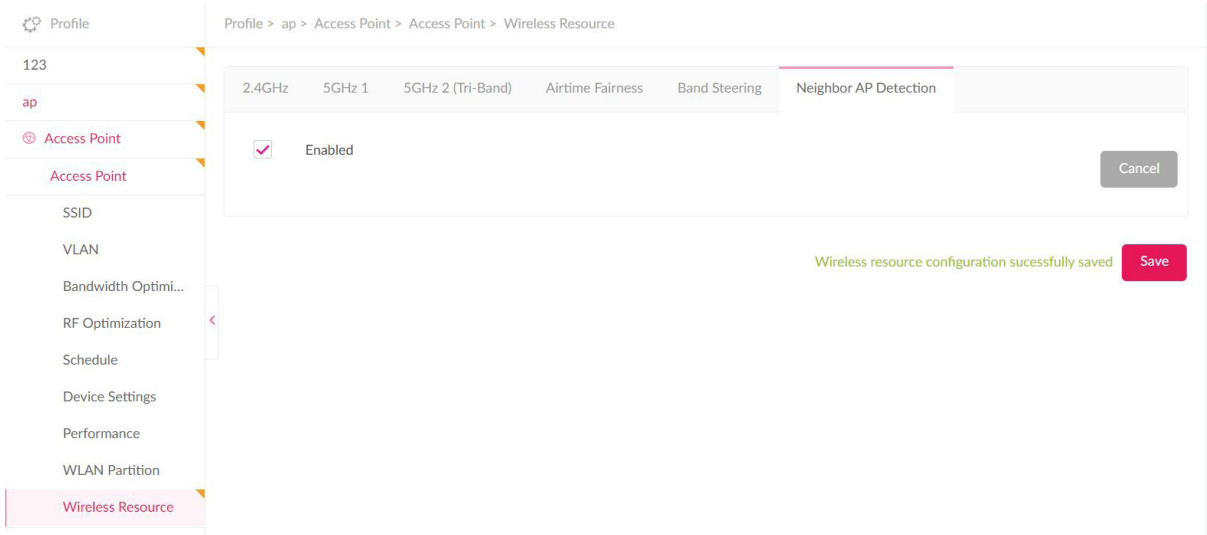
Access Point

Wireless Resource

Neighbor AP Detection

Users can view neighbor information on a specified AP radio to determine the AP location and neighbor relationship, helping locate rogue APs and plan the WLAN.

Check “Enabled” to enable detection, and go to Monitor>Neighbor AP to review AP list.



Once the settings are updated, the configuration must be uploaded to the related access points. See “Profile Settings” on page 69 for further information.

Nuclias Connect Configuration Profile Settings Switch

Common RADIUS Server

In the RADIUS Server page, you can forward access requests from your switches to one or more specified remote RADIUS servers. Navigate to **Configuration > Profile Settings > Switch > Common > RADIUS Server** to set up remote RADIUS server for all switches in the network.

To add a RADIUS server, enter the RADIUS authentication server, the UDP port and the secret used to communicate with the server. Alternatively, click **Copy** to copy RADIUS server from other network. Once completed, click **Add** to add a new RADIUS server, or **Clear** to remove the entries.

In the **RADIUS Server Table** below, a summary of all the RADIUS Servers details including the **number**, **RADIUS server**, **port** and **secret** is displayed. Under the Action field, click to edit the RADIUS server. Click to delete the selected RADIUS server. Click **Save** when completed.

RADIUS Server Table

The max. number of radius server is 32, 32 remain

No.	RADIUS Server	RADIUS Port	RADIUS Secret	Action
 No data found				

1 - 5 of 0 total Items: 0

<< < 1 / 1 > >> 5 items per page

Save

Nuclias Connect Configuration Profile Settings Switch

Common Time Profile

Under the Time Profile page, users can set up time profile for all the switches in the network. Navigate to **Configuration > Profile Settings > Switch > Common > Time Profile** to set up the time profile.

In the **Add Time Profile** page, enter a name for the profile. Select the work days for the switch. Next, enter the **Start** and **End** time using the drop-down menu. Alternatively, click **Copy** to copy the time profile from other network. Once the time is set, click **Add** to add a schedule, or **Clear** to remove all values.

The screenshot shows the Nuclias Connect web interface. The left sidebar contains navigation links: Dashboard, Topology, Floor Plan, Configuration (selected), Report, Log, and System. The Configuration menu is expanded, showing options like Create Profile, Profile Settings (selected), Firmware Upgrade, SSL Certificate, and Payment Gateway. The main content area displays the 'Add Time Profile' form. The form has a 'Name*' field (1-32 characters), a 'Days*' field with checkboxes for Sun, Mon, Tue, Wed, Thu, Fri, Sat, and an 'All week' option. Below these are 'Start Time' and 'End Time' fields, each with a dropdown menu. At the bottom right of the form are 'Copy', 'Add', and 'Clear' buttons. Below the form is a 'Time Profile Table' with a search bar and a table header. The table shows one profile: 'Dlink' with 'All week' days, '01:03' start time, and '01:05' end time. The table also includes edit and delete icons for each profile.

In the Time Profile Table, a summary of the time profile, including the name, days, start/end time is displayed. Use the drop-down menu to filter the time profiles by either **Name** or **Days**. Enter a relevant keyword to narrow the search. Click to start the search. Under the Action field, click to edit the time profile. Click to delete the time profile. Click **Save** when completed.

Time Profile Table

The max. number of time profiles is 8, 7 remain

Search By: Name Search 'Keyword'

No.	Name	Days	Start Time	End Time	Action
1	Dlink	All week	01:03	01:05	

1 - 15 of 1 total items: 1

1 / 1 15 items per page

Save




Nuclias Connect Configuration Profile Settings Switch

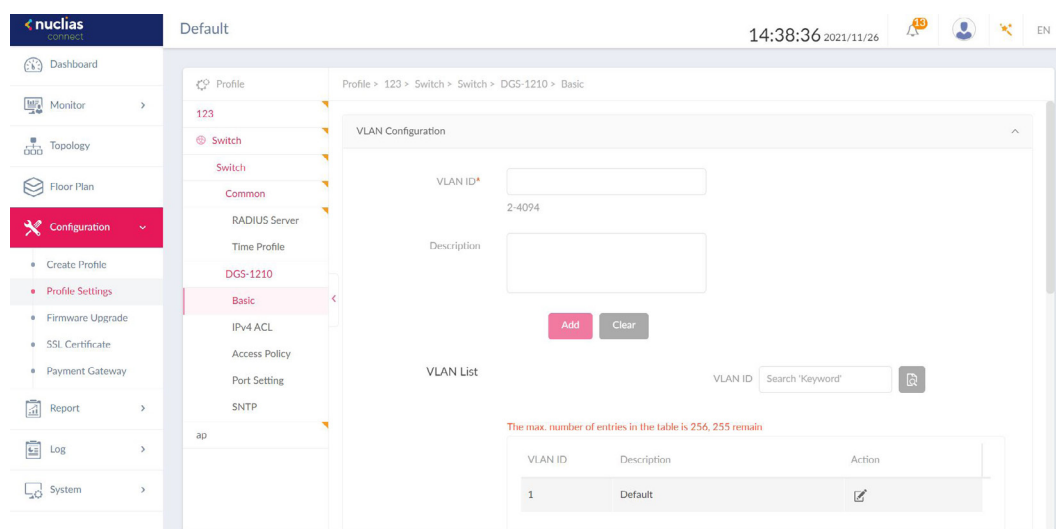
Basic

Under the **Basic** tab, users can configure global switch settings such as VLAN, IGMP Snooping, Quality of service and more. Navigate to **Configuration > Profile Settings > Switch > Your Device > Basic** to configure the switch. Below describes the functionality of each configuration options.

VLAN Configuration

In this section, users can add, edit, or delete a VLAN. Enter a VLAN ID in the VLAN ID field, the range of 2 to 4094. Next, enter a description for the VLAN. Once complete, click Add to add a VLAN, or Clear to clear the entry.

In the VLAN List section, a summary of VLAN is displayed. Enter keyword in the VLAN ID search field to locate a VLAN. Click  to start the search. Under the Action field, click  to edit a VLAN. Click  to delete a VLAN. Click **Save** when complete.



Voice VLAN Configuration

In this section, users can view and configure global Voice VLAN settings and Voice VLAN OUI (Organizationally Unique Identifier). In the Voice VLAN field, select Enabled or Disabled. If Enabled, select Voice VLAN ID and Voice VLAN COS from the drop-down menu. On the right side of Voice VLAN ID field, users can view the number of member ports belonging to the voice VLAN. Click the numbers to be directed to the Port Setting page.

In the Voice VLAN OUI section, Voice VLAN is disabled. When enabled, users can add self-defined OUI for the voice VLAN. To do so, enter a description for ease of identification. Click **Add** to add a new Voice VLAN, or **Clear** to remove entered values. Up to 10 entries can be entered.

Voice VLAN Configuration

Voice VLAN
☐ Enabled
☒ Disabled

Voice VLAN ID *

Pick one...
2-4094

0, 0, 0, 0, 0 member ports belonging to this Voice VLAN currently

Voice VLAN COS

5

Voice VLAN OUI

OUI Address
3c:1e:04:16:53:20

Mask
ff:ff:ff:00:00:00











Description

Add
Clear

The max. number of user defined entries in the table is 10, 10 remain

When Voice VLAN is enabled, a default Voice VLAN OUI list is displayed in the summary list below. These entries cannot be edited nor deleted.

The max. number of user defined entries in the table is 10, 10 remain

OUI Address	Mask	Description	Action
00:01:e3:00:00:00	ff:ff:ff:00:00:00	Siemens	 
00:03:6b:00:00:00	ff:ff:ff:00:00:00	Cisco	 
00:09:6e:00:00:00	ff:ff:ff:00:00:00	Avaya	 
00:0f:e2:00:00:00	ff:ff:ff:00:00:00	Huawei & 3COM	 
00:60:b9:00:00:00	ff:ff:ff:00:00:00	NEC & Philips	 

IGMP Snooping Configuration

IGMP snooping allows switches to be aware of multicasting groups and forward network traffic accordingly. In this section, users can enable or disable the IGMP Snooping function. When enabled, enter the VLAN ID of the VLAN. The max number of VLANs is 256.

IGMP Snooping Configuration

IGMP Snooping

☐ Enabled

☒ Disabled

VLAN

1-4094, e.g. 1-4,7,9 or All.

STP Configuration

RSTP (Rapid Spanning Tree Protocol) can ensure a loop-free topology and speedy convergence time. In this section, users can enable or disable RSTP on all switches in the network.

STP Configuration

RSTP

☐ Enabled

☒ Disabled

DHCP Server Screen Configuration

DHCP (Dynamic Host Configuration Protocol) server screening provides a higher security by filtering illegal DHCP server packets. Select **Enabled** to turn on DHCP Server Screening. When **Enabled** is selected, enter the **Allowed DHCP Server IP** in the field.

DHCP Server Screen Configuration

DHCP Server Screen

☐ Enabled

☒ Disabled

Allowed DHCP server IP

Only support 1 entry, e.g. 10.90.90.90

Jumbo Frame Configuration

Jumbo frames are Ethernet frames with massive payload. They are used to reduce frame overload, increase system throughput and reduce CPU utilization. In the Jumbo Frame field, select **Enabled** or **Disabled**.

Jumbo Frame Configuration

Jumbo Frame

☐ Enabled

☒ Disabled

Quality of Service

The QoS feature can prioritize certain types of data with the use of differentiated services model. The priorities are marked in each packet using Differentiated Services Code Point (DSCP) for traffic classification. To set the DSCP to CoS (Class of Service) queue, choose a value from the drop-down menu and set a name for it.

Note: One DSCP value can only be mapped to one CoS queue value.

[Edit DSCP to CoS Queue Map](#)

DSCP Value	Cos Queue Value	Name
0	1	Dlink
1	0	Default
2	0	Default
3	0	Default
4	0	Default

LBD Configuration

The Loopback Detection (LBD) feature can detect loops occurring on one or across different ports. In the LBD field, click **Enabled** to turn on the feature. It is disabled by default.

LBD Configuration

LBD

☐ Enabled

☒ Disabled

DDP Configuration

The D-Link Discovery Protocol (DDP) is a communication protocol defined by D-Link. When enabled, your device will become discoverable and can be managed by the DNC server. Features from DNA (D-Link Network Assistant) like IP settings, firmware upgrade, reboot and reset function will also be supported.

In the DDP field, click **Enabled** to turn on, or **Disabled** to turn off this feature. It is enabled by default.

DDP Configuration

DDP

☒ Enabled

☐ Disabled

Local Credential Configuration


The username and password of your device is listed here.

Local Credential Configuration

Username

admin

Password

•••••••• 

Nuclias Connect Configuration Profile Settings Switch

IPv4 ACL

The IPv4 ACL (Access Control List) feature for the switch can help improve network performance and security by blocking selected traffic. Navigate to **Configuration > Profile Settings > Site > Network > Switch > Your Device > IPv4 ACL** to configure the settings.

In the User defined IPv4 ACL Rules section, the following fields are presented:

Field	Description
Sequence No.	Set the sequence number. The range is 1-65535. Select Auto to auto-assign the sequence number
Policy	Select to permit or deny what traffic goes through the switch.
Source	Enter the source IP address. When the Protocol is set to Any , all traffic destination will be evaluated.
Destination	Enter the destination IP address. When the destination is set to Any , all traffic destination will be evaluated.
Comment	Enter a description for the rule.
Protocol	Select between TCP , UDP , or Any .
Src Port	Specify the number of the source port. The valid value is 0-65535. When the Src Port is set to Any , all traffic source will be evaluated.
Dst Port	Specify the number of the destination port. The valid value is 0-65535. When the Dst Port is set to Any , all traffic source will be evaluated.

Once complete, click **Add** to add the rule, or **Clear** to clear all values.

In the **IPv4 ACL Rule Table** section, a summary of all IPv4 ACL Rule is displayed. Under the Action field, click **Edit** to edit the ACL rule; Click **Delete** to delete the ACL rule. Click **Save** to save the changes.

User Defined IPv4 ACL Rules

Sequence No.

☒ Auto

Policy

Deny

Protocol

Any

Source

Any

Src Port

Any

Destination

Any

Dst Port

Any

Comment*

Add

Clear

IPv4 ACL Rule Table

The max. number of user defined entries in the table is 768, 767 remain




Sequence No.	Policy	Protocol	Source	Src Port	Destination	Dst Port	Comment	Action
10	Permit	UDP	Any	6000	192.168.1.0/24	6000	Test	

Nuclias Connect Configuration Profile Settings Switch

Access Policy

D-Link switches support 802.1X authentication, MAC authentication and port security to prevent unauthorized client from accessing the network. Navigate to **Configuration > Profile Setting > Site > Network > Switch > Your Device > Access Policy** to configure the settings.

In the **Policy Name** field, enter a name for the policy. In the **Remote RADIUS Server** section, specify up to 3 RADIUS Servers for the switches to forward access requests. Authentication requests will be processed by each of the RADIUS servers in the order that they are submitted. Click **Select** to select existing RADIUS servers created via the RADIUS Server page. A pop window will be presented to confirm your selection. Click **OK** to confirm, or **Cancel** to close the window.

Once the RADIUS Servers is selected, a summary of the RADIUS servers will be listed in the table. In the **Action** field, click  to move the entry up, click  to move the entry down. Click  to delete the entry.

Policy Name *

Remote RADIUS *

The max. number of entries in the table is 3, 2 remain

No.	RADIUS Server	RADIUS Port	RADIUS Secret	Action
1	10.90.90.1	1812 	  

In the **Access Policy Type** field, select 802.1x Port Based. This will allow only one user to be authenticated per port by a remote RADIUS server.

In the Guest VLAN field, specify a guest VLAN ID or disable it from the drop-down menu. The VLAN ID range is 1 to 4094. One switch only supports one Guest VLAN. When a VLAN ID is selected, the member port information will be presented. Click the number to be directed to the Port Settings page

In the Switch Ports field, the number of switch ports that's applying to the policy is listed. Click the numbers to be directed to the Port Settings page.

Access Policy Type

Guest VLAN

10, 20, 26, 28, 52 member ports belonging to this Guest VLAN currently

Switch Ports 0, 0, 0, 0, 0 ports using this policy currently

Access Policy saved successfully


Save

Reset


Nuclias Connect Configuration Profile Settings Switch

Port Setting

Navigate to **Configuration > Profile Settings > Network > Switch > Your Switch > Port Setting**, a summary of each of the switch port groups is displayed. Note that the number of port groups depends on the switch series.


To filter the search, from the **Search By** drop down menu, select **VLAN/Port/Access Policy**, and select Port Type **Access/Trunk/All**. Under the Search column, enter a relevant keyword to narrow the search. Click  to start the search. The summary includes information such as **Port number, Link, Port type, VLAN, Allowed VLAN, Port State, PoE, RSTP, LBD, DDP, Port Shutdown Schedule, PoE Supply Schedule, and Access Policies**.


Note that under the Link field, the value is **Default** (System default value) and cannot be modified in Profile Configuration. Links can only be modified in Standalone mode via Monitor > Switch > Switch Port, or Monitor > Device Detail page > Ports.

To make changes to a port or port group, select the port(s) and click  to make the desired changes. Scroll down to view the Port Setting table. Once complete, click **Save** to save the changes.

Profile > STANLEY > Enduro > Switch > DGS-1210 > Port Setting

10 Ports 20 Ports 26 Ports 28 Ports 52 Ports

Search By VLAN Port Type All Type Search 'Keyword' 



<input type="checkbox"/>	Port	Link	Port Type	VLAN	Port State	PoE	RSTP	LBD
<input type="checkbox"/>	1	Default	Access	1	Enabled	Enabled	Enabled	Disabled
<input type="checkbox"/>	2	Default	Access	1	Enabled	Enabled	Enabled	Disabled
<input type="checkbox"/>	3	Default	Access	1	Enabled	Enabled	Enabled	Disabled
<input type="checkbox"/>	4	Default	Access	1	Enabled	Enabled	Enabled	Disabled
<input type="checkbox"/>	5	Default	Access	1	Enabled	Enabled	Enabled	Disabled
<input type="checkbox"/>	6	Default	Access	1	Enabled	Enabled	Enabled	Disabled
<input type="checkbox"/>	7	Default	Access	1	Enabled	Enabled	Enabled	Disabled
<input type="checkbox"/>	8	Default	Access	1	Enabled	Enabled	Enabled	Disabled

Nuclias Connect Configuration Profile Settings Switch

SNTP

The SNTP (Simple Network Time Protocol) function allows the switch to synchronize clocks on a network. Navigate to **Configuration > Profile Settings > Site > Network > Switch > Your Switch > SNTP** to configuration the settings.

Under the SNTP tab, you can configure **Automatic Time Configuration** and **Time Zone Settings**.

In the Automatic Time Configuration section, click **Enable SNTP Server** to enable or disable it. Once enabled, specify the IPv4 address or domain name of the primary SNTP server from which the system time is retrieved in the **SNTP Server 1** field, and the secondary SNTP server in the **SNTP Server 2** field.

Automatic Time Configuration

☒ Enable SNTP Server

SNTP Server1

SNTP Server2

In the Time Zone Settings section, users can configure time zones and daylight saving for SNTP. From the **Time Zone** field, select your local time zone. Click **Enable Daylight Saving** to enable or disable daylight saving.

In the **DST Start (24HR)** field, enter the month, date, and time in which DST will start at. In the **DST End (24HR)** field, enter the month, date, and time in which DST will end at. In the **DST Offset** field, specify the amount of time that will constitute the local DST offset - 30, 60, 90, or 120 minutes. The default is 60 min. Click **Save** when complete.

Time Zone Settings

Time Zone

☒ Enable Daylight Saving

DST Start (24HR) at

DST End (24HR) at

DST Offset

Save

Nuclias Connect

Configuration

Firmware Upgrade

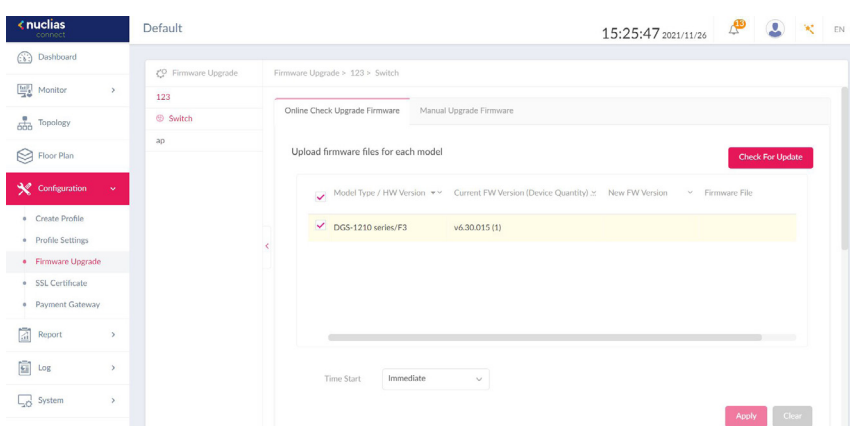
The Firmware Upgrade function allows users to perform a firmware upgrade. For online update, please confirm your device is online. For manual upgrade, please visit D-Link website of your region to see if newer firmware available.

Navigate to **Configuration > Firmware Upgrade > [Site] > [Network]**.

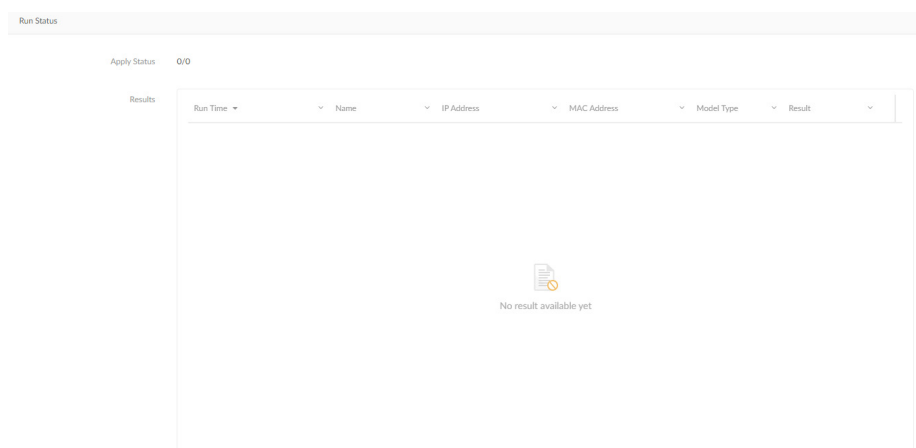
Block	Description
Online Check Upgrade Firmware	Click to configure online upgrade.
Check For Update	Click to check if newer firmware is available on online server.
Manual Upgrade Firmware	Click to configure manual upgrade.
Change	Click to select a firmware file to upload. Files are model specific.
Time Start	Click the drop-down menu to select a specific time or update immediately.

Click **Apply** to save the above configuration settings.

Click **Clear** to delete the defined settings.



The firmware upgrade status and result can be seen at the **Run Status** section. The results can be sorted by **Run Time, Name, IP Address, MAC Address, Model Type and Result**.



Nuclias Connect

Configuration

SSL Certificate

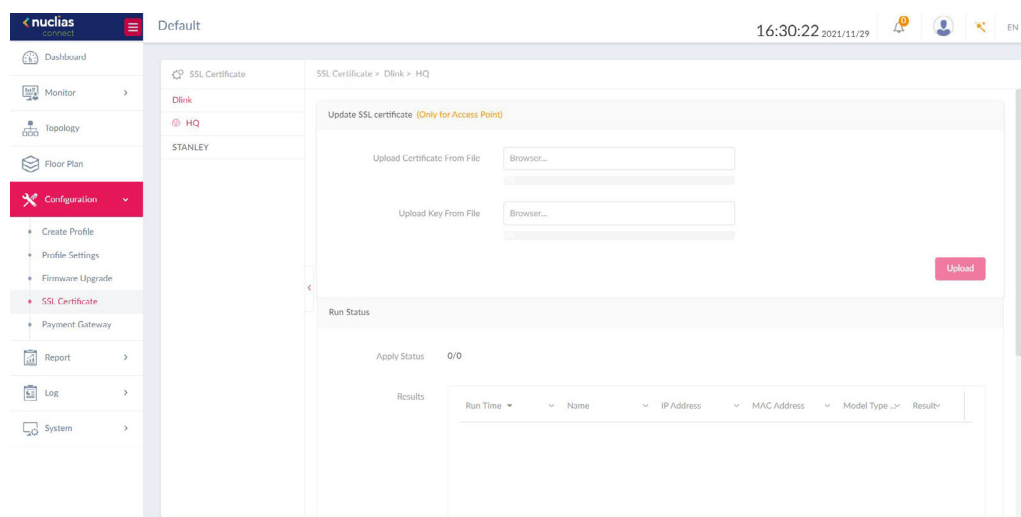
The SSL Certificate function provides the means to install an SSL certificate for use on the network. To accomplish this task, an intermediate certificate is required. The intermediate certificate is used to establish the trust of the SSL certificate by binding it to the Certificate Authority's root certificate. To complete the certificate trust configuration, the SSL Certificate function requires the certificate file to be uploaded.

In the **Update SSL certificate** section, the following parameters can be configured.

Note that this setting is only applicable to Access Points.

Options	Description
Upload Certificate From File	Click Browser... to select the SSL certificate file located on the drive to upload.
Upload Key From File	Click Browser... to select the SSL key file located on the local drive to upload.

Click **Upload** to initiate the file upload. The upload status and result will appear in the below area.



Nuclias Connect

Configuration

Payment Gateway

The payment gateway is a function that allows e-commerce services within the network. The Payment Gateway page will show payment settings and options necessary to enable payment services.

Navigate to **Configuration > Payment Gateway**.

Parameter	Description
PayPal Currency	Click the drop-down menu to select the currency code for the 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 + to enter the option.


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

The screenshot shows the Nuclias Connect web interface. On the left is a sidebar menu with options: Dashboard, Monitor, Topology, Floor Plan, Configuration (selected), Create Profile, Profile Settings, Firmware Upgrade, SSL Certificate, Payment Gateway (highlighted), Report, Log, and System. The main content area is titled 'Payment Settings'. It contains the following fields: 'PayPal Currency*' with a dropdown menu showing 'USD'; 'PayPal Client ID*' with a text input field; 'PayPal Secret*' with a text input field; and 'Options*' which is a table with two rows. The first row has 'Duration' set to '0', a unit dropdown set to 'Minutes(s)', and 'Cost' set to '0'. The second row has 'Duration' as an empty text field, a unit dropdown set to 'Pick one...', and 'Cost' as an empty text field. To the right of the 'Options' table are two red buttons: a minus sign (-) and a plus sign (+). A red 'Save' button is located at the bottom right of the form area. The top of the interface shows the time '16:31:19' and the date '2021/11/29'.

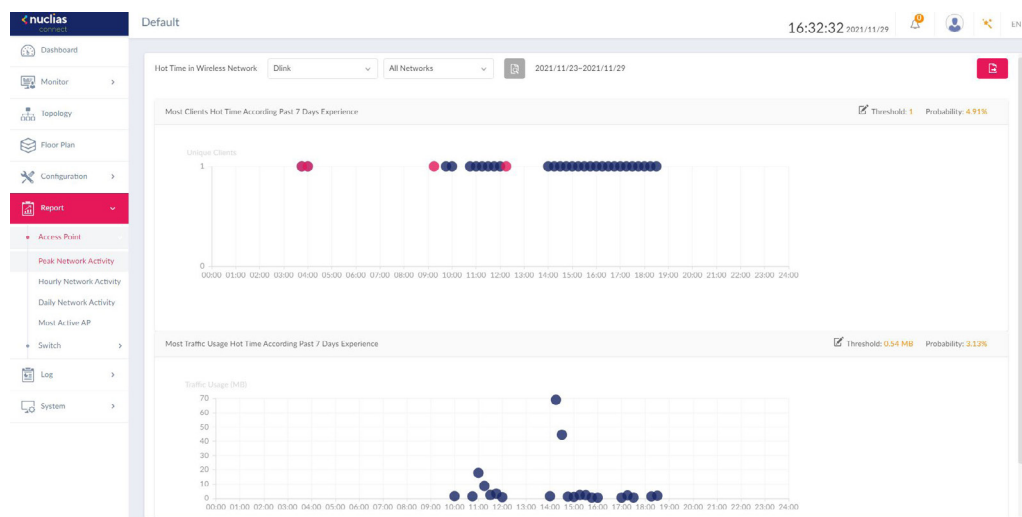
Nuclias Connect Report Access Point Peak Network Activity

The Peak Network Activity function allows administrators to monitor wireless traffic on the network. Wireless activity for all or specific sites and networks can be displayed according to unique clients and traffic usage.

Navigate to **Report > Peak Network Activity** to view the information.

To view a network activity report, select the site and network from the corresponding drop-down menu and click  to view the report.

Once a report has been generated, click  to save the report to a local PDF file.



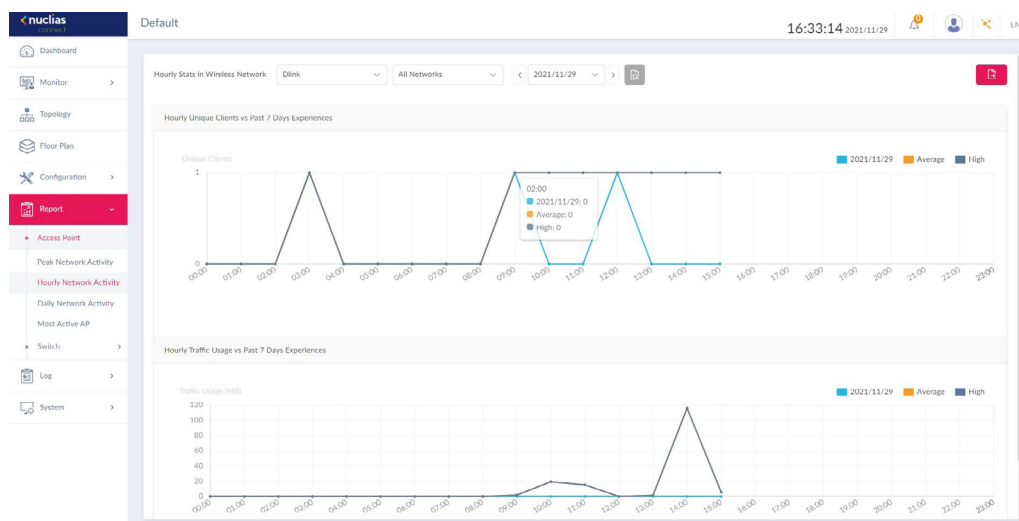
Nuclias Connect Report Access Point Hourly Network Activity

The Hourly Network Activity function allows administrators to monitor wireless traffic on the network. Wireless activity for all or specific sites and networks is displayed according to unique clients and traffic usage as reported by the hour.

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

To start a daily report, select the site and network from the corresponding drop-down menu and click  to view the report.


Once a report is generated, click  to save the report to a local PDF file.



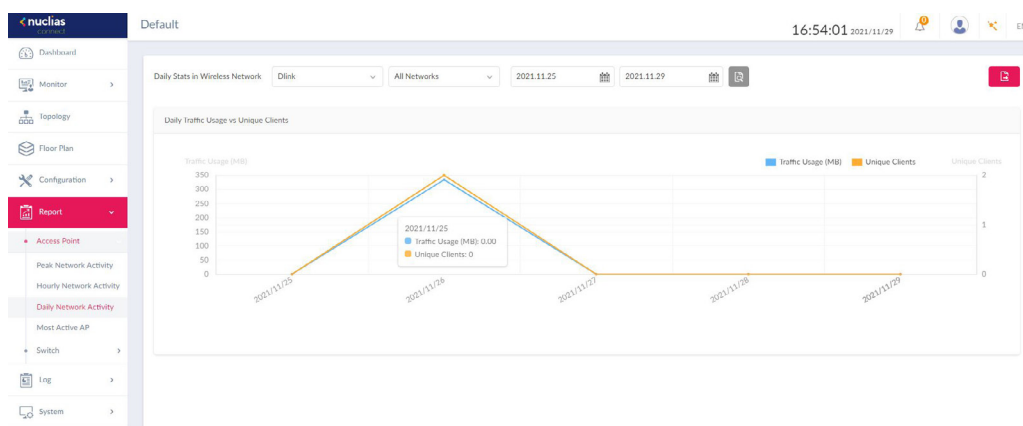
Nuclias Connect Report Access Point Daily Network Activity

The Daily Network Activity function allows administrators to monitor daily wireless traffic on the network. Wireless activity for unique clients and traffic usage is displayed according to unique clients and traffic usage as reported by the day.

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



To display a specific client's traffic usage, select a site, network, and define the starting and ending dates of the search. Once the search parameters are defined, click  to view the report.


Once a report is generated, click  to save the report to a local PDF file.




Nuclias Connect Report Access Point

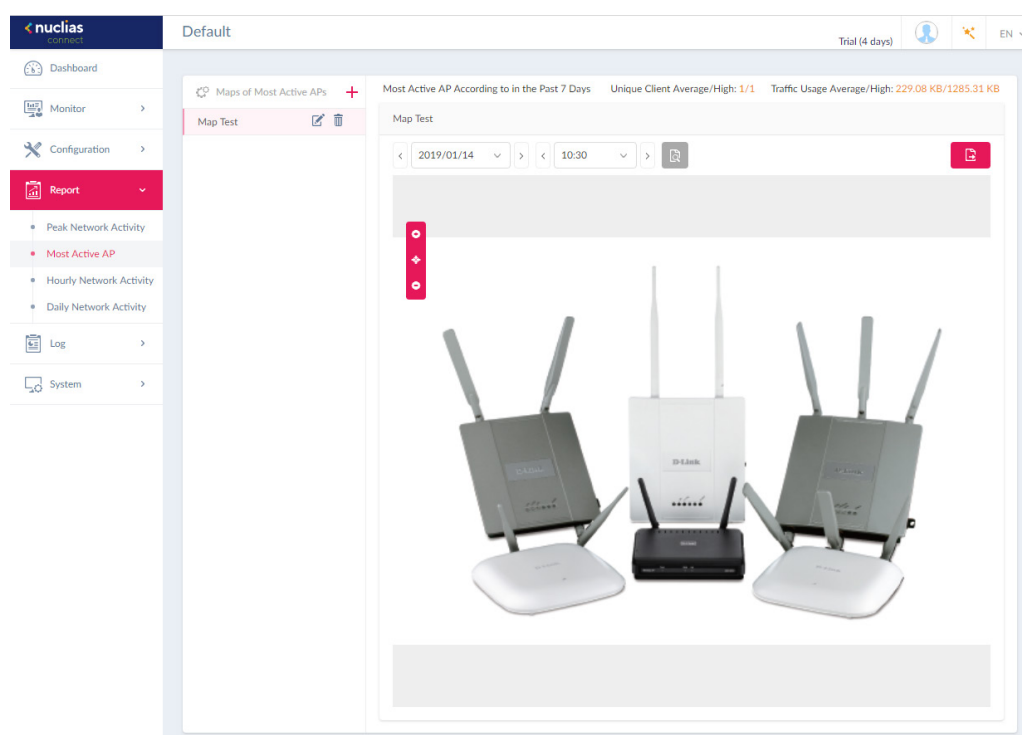
Most Active AP

To view a specific client's traffic usage, select a client from the most active APs column. Available maps can be edited or deleted by clicking  or . In the **Edit Map of Most Active APs** page, enter the name of the map and click the **Select AP** drop-down menu to select an AP from a list of available APs. Once defined, click **Save** to complete the process.

To add a new map, click  to open the **Create Map of Most Active APs**. Enter the map name in the name field. Customize the map by dragging and dropping an image (supported file formats: *.png,*.jpg; max. size: 10M) or browsing a local folder to select an image.


To view a network AP active map report, select the date and time, and click  to view the report.

Once a report has been generated, click  to save the report to a local PDF file.

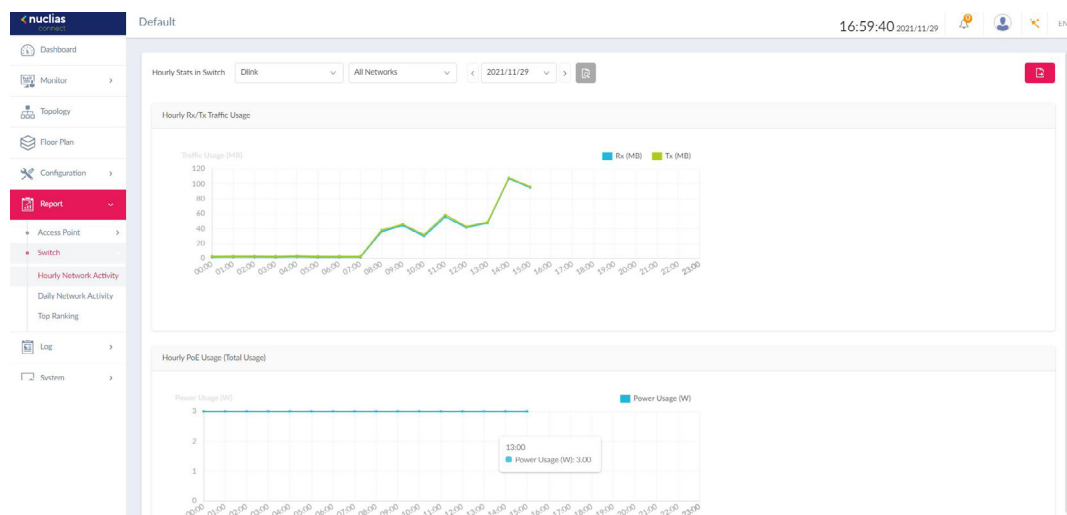


Nuclias Connect Report Switch Hourly Network Activity

The Hourly Network Activity function allows administrators to monitor daily traffic and power usage on the network. Traffic usage and PoE Usage is reported by the hour. Navigate to **Report > Switch > Hourly Network Activity** to generate and view the report.


To display clients' traffic usage and PoE usage, select a site, network, and define the starting and ending dates of the search. Once the search parameters are defined, click  to view the report.

Once a report is generated, click  to save the report to a local PDF file.

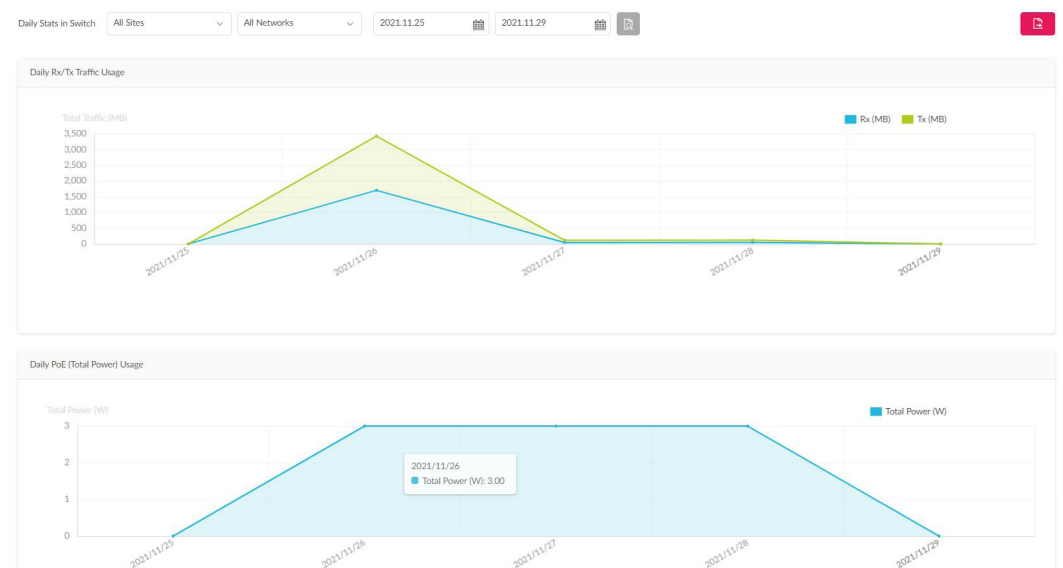


Nuclias Connect Report Switch Daily Network Activity

The Daily Network Activity function allows administrators to monitor daily traffic and power usage on the network. Navigate to **Report > Switch > Daily Network Activity** to generate and view the report.

To display clients' traffic usage and PoE usage, select a site, network, and define the starting and ending dates of the search. Once the search parameters are defined, click  to view the report.

Once a report is generated, click  to save the report to a local PDF file.




Nuclias Connect Report Switch Top Ranking

The Top Ranking report allows administrators to view a range of switch traffic reports sorted by top 10 rankings on the site and network.

The following ranking reports are available: **Top Total Traffic (Tx)**, **Top Total Traffic (Rx)**, **Top Port Traffic (Tx)**, **Top Port Traffic (Rx)**, **Top Port Errors (Tx)**, **Top Port Discards (Rx)**, **Top Port Multicast (Rx)**, **Top Port Broadcast (Rx)**, **Top Port Utilization**, **Top PoE Power Consumption**, and **Top CPU Utilization**.

Navigate to **Report > Top Ranking** to view the report.

To filter the top ranking report, select the site and network from the corresponding drop-down menu and click  to view the report.

Once a report is generated, click  to save the report to a local PDF file.




Nuclias Connect

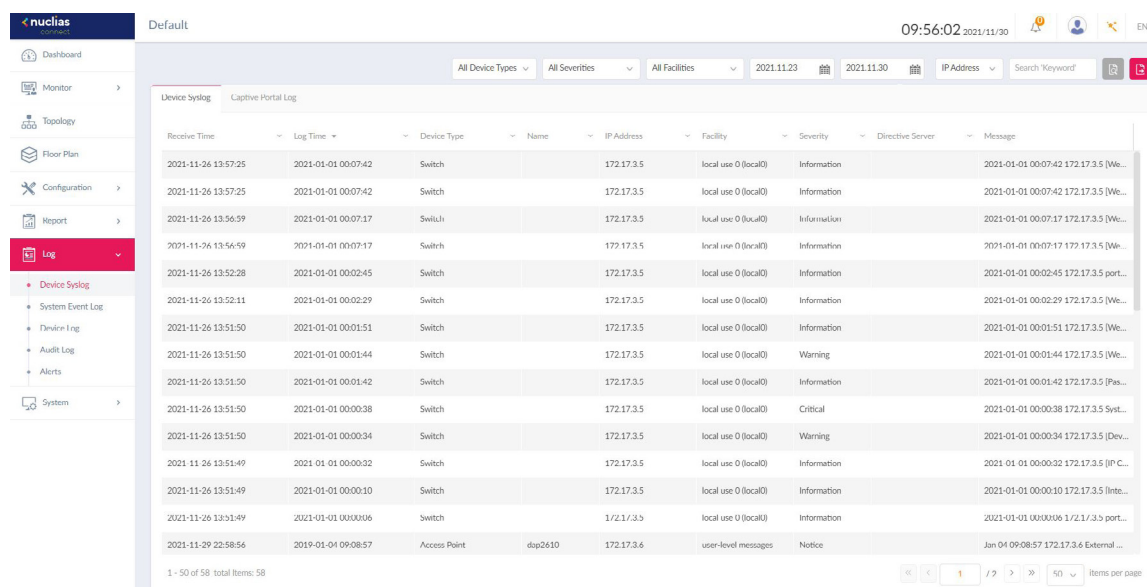
Log

Device Syslog

The Syslog function allows administrators to view alert messages for events concerning system logs. Log messages for the system and captive portals can be viewed here. Navigate to **Log > Syslog** to view the relevant information.

To start a syslog report, select the event severity, facility system, and define the period of time to report. Click the drop-down menu to define the type of search criteria to view, IP Address or Trap Details. Fill in the keyword field and click  to view the generated report.

Once a report is generated, click  to save the report to a local PDF file.



The screenshot displays the Nuclias Connect web interface. On the left is a sidebar menu with options: Dashboard, Monitor, Topology, Floor Plan, Configuration, Report, Log (selected), Device Syslog, System Event Log, Device Log, Audit Log, Alerts, and System. The main area is titled 'Device Syslog' and 'Captive Portal Log'. It features a search bar with filters for 'All Device Types', 'All Severities', 'All Facilities', and date ranges '2021.11.23' to '2021.11.30'. A search criteria dropdown is set to 'IP Address', and a search keyword field is present. Below the search bar is a table of log entries with columns: Receive Time, Log Time, Device Type, Name, IP Address, Facility, Severity, Directive Server, and Message. The table contains 15 rows of data, mostly from 'Switch' devices with 'local use 0 (local0)' as the facility. The last row is from an 'Access Point' with facility 'user-level messages'. At the bottom, it shows '1 - 50 of 58 total items: 58' and a pagination control set to '50' items per page.


Receive Time	Log Time	Device Type	Name	IP Address	Facility	Severity	Directive Server	Message
2021-11-26 13:57:25	2021-01-01 00:07:42	Switch		172.17.3.5	local use 0 (local0)	Information		2021-01-01 00:07:42 172.17.3.5 (We...
2021-11-26 13:57:25	2021-01-01 00:07:42	Switch		172.17.3.5	local use 0 (local0)	Information		2021-01-01 00:07:42 172.17.3.5 (We...
2021-11-26 13:56:59	2021-01-01 00:07:17	Switch		172.17.3.5	local use 0 (local0)	Information		2021-01-01 00:07:17 172.17.3.5 (We...
2021-11-26 13:56:59	2021-01-01 00:07:17	Switch		172.17.3.5	local use 0 (local0)	Information		2021-01-01 00:07:17 172.17.3.5 (We...
2021-11-26 13:52:28	2021-01-01 00:02:45	Switch		172.17.3.5	local use 0 (local0)	Information		2021-01-01 00:02:45 172.17.3.5 port...
2021-11-26 13:52:11	2021-01-01 00:02:29	Switch		172.17.3.5	local use 0 (local0)	Information		2021-01-01 00:02:29 172.17.3.5 (We...
2021-11-26 13:51:50	2021-01-01 00:01:51	Switch		172.17.3.5	local use 0 (local0)	Information		2021-01-01 00:01:51 172.17.3.5 (We...
2021-11-26 13:51:50	2021-01-01 00:01:44	Switch		172.17.3.5	local use 0 (local0)	Warning		2021-01-01 00:01:44 172.17.3.5 (We...
2021-11-26 13:51:50	2021-01-01 00:01:42	Switch		172.17.3.5	local use 0 (local0)	Information		2021-01-01 00:01:42 172.17.3.5 (Pas...
2021-11-26 13:51:50	2021-01-01 00:00:38	Switch		172.17.3.5	local use 0 (local0)	Critical		2021-01-01 00:00:38 172.17.3.5 Syst...
2021-11-26 13:51:50	2021-01-01 00:00:34	Switch		172.17.3.5	local use 0 (local0)	Warning		2021-01-01 00:00:34 172.17.3.5 (Dev...
2021-11-26 13:51:49	2021-01-01 00:00:32	Switch		172.17.3.5	local use 0 (local0)	Information		2021-01-01 00:00:32 172.17.3.5 (IP C...
2021-11-26 13:51:49	2021-01-01 00:00:10	Switch		172.17.3.5	local use 0 (local0)	Information		2021-01-01 00:00:10 172.17.3.5 (Inte...
2021-11-26 13:51:49	2021-01-01 00:00:06	Switch		172.17.3.5	local use 0 (local0)	Information		2021-01-01 00:00:06 172.17.3.5 port...
2021-11-29 22:58:56	2019-01-04 09:08:57	Access Point	dsp2610	172.17.3.6	user-level messages	Notice		Jun 04 09:08:57 172.17.3.6 External ...

Nuclias Connec

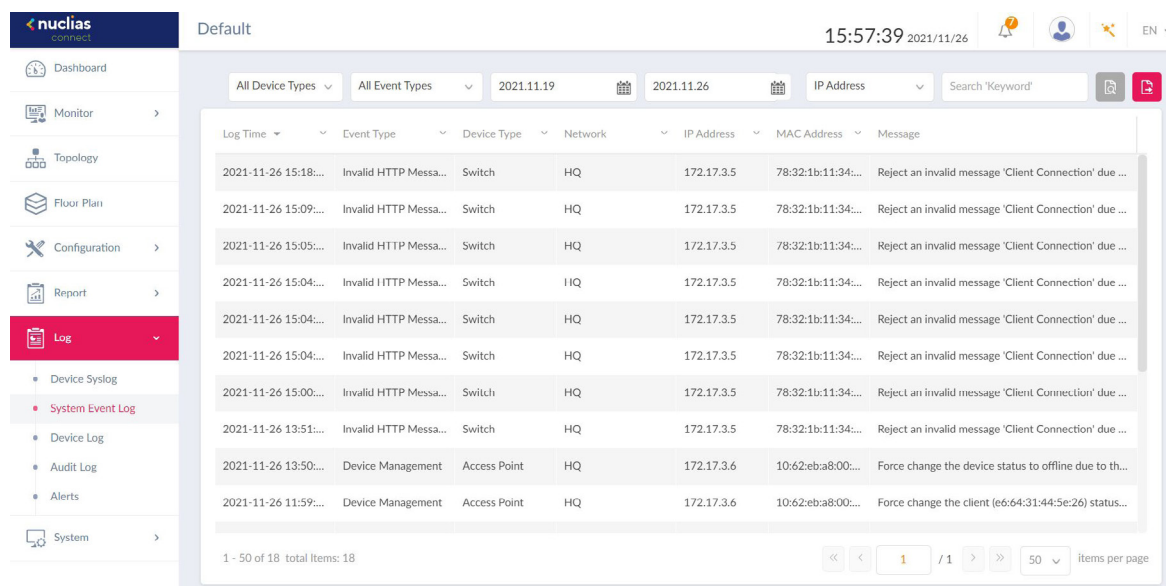
Log

System Event Log

The System Event Log function allows administrators to view alerts that may require attention and necessary action to continue operation and prevent failures. Navigate to **Log > System Event Log** to view the relevant information.

To generate a System Event Log report, select the event severity and define the period of time to report. Click the drop-down menu to define the type of search criteria to view, IP Address or Trap Details. Fill in the keyword field and click  to view the generated report.

Once a report is generated, click  to save the report to a local PDF file.



Log Time	Event Type	Device Type	Network	IP Address	MAC Address	Message
2021-11-26 15:18:...	Invalid HTTP Messa...	Switch	HQ	172.17.3.5	78:32:1b:11:34:...	Reject an invalid message 'Client Connection' due ...
2021-11-26 15:09:...	Invalid HTTP Messa...	Switch	HQ	172.17.3.5	78:32:1b:11:34:...	Reject an invalid message 'Client Connection' due ...
2021-11-26 15:05:...	Invalid HTTP Messa...	Switch	HQ	172.17.3.5	78:32:1b:11:34:...	Reject an invalid message 'Client Connection' due ...
2021-11-26 15:04:...	Invalid HTTP Messa...	Switch	HQ	172.17.3.5	78:32:1b:11:34:...	Reject an invalid message 'Client Connection' due ...
2021-11-26 15:04:...	Invalid HTTP Messa...	Switch	HQ	172.17.3.5	78:32:1b:11:34:...	Reject an invalid message 'Client Connection' due ...
2021-11-26 15:00:...	Invalid HTTP Messa...	Switch	HQ	172.17.3.5	78:32:1b:11:34:...	Reject an invalid message 'Client Connection' due ...
2021-11-26 13:51:...	Invalid HTTP Messa...	Switch	HQ	172.17.3.5	78:32:1b:11:34:...	Reject an invalid message 'Client Connection' due ...
2021-11-26 13:50:...	Device Management	Access Point	HQ	172.17.3.6	10:62:eba8:00:...	Force change the device status to offline due to th...
2021-11-26 11:59:...	Device Management	Access Point	HQ	172.17.3.6	10:62:eba8:00:...	Force change the client (e6:64:31:44:5e:26) status...


Nuclias Connect

Log

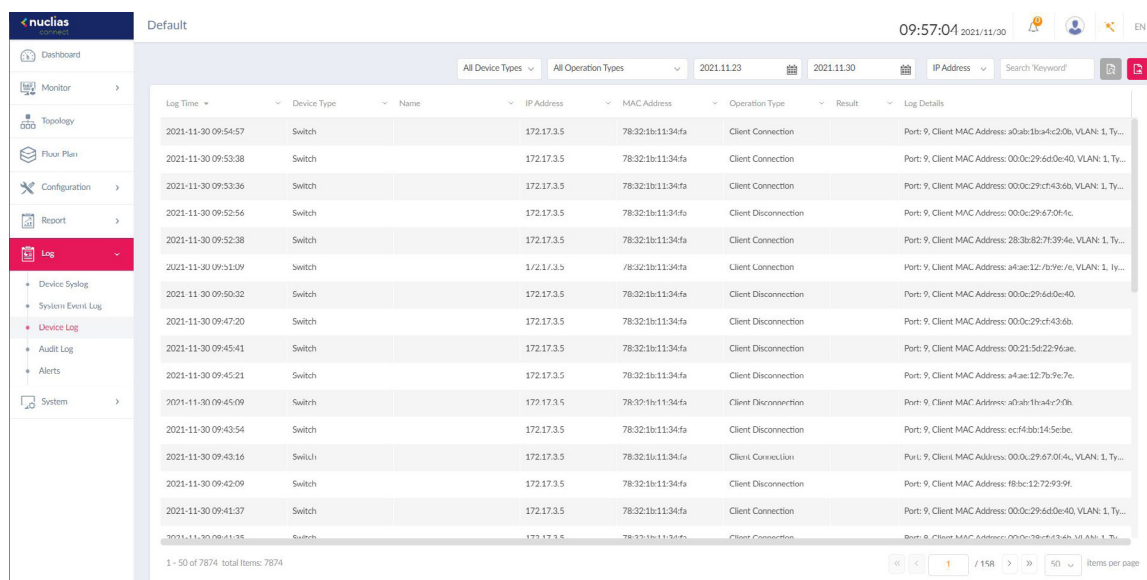
Device Log

The Device Log function allows administrators to view alert messages from a device's embedded memory. The system and network messages includes a time stamp and message type. The log information includes but not limited to the following items: Synchronize device settings, upgrading firmware, upload configuration, and blocking clients.

Navigate to **Log > Device Log** to display the function information.

To start a Device Log, select the operation type and define the period of time to report. Click the drop-down menu to define the type of search criteria to view, IP address or Trap Details. Fill in the keyword field and click  to view the generated report.

Once a report is generated, click  to save the report to a local PDF file.



Log Time	Device Type	Name	IP Address	MAC Address	Operation Type	Result	Log Details
2021-11-30 09:54:57	Switch		172.17.3.5	78:32:1b:11:34:fa	Client Connection		Port: 9, Client MAC Address: a0ab:1ba4:c20b, VLAN: 1, Ty...
2021-11-30 09:53:38	Switch		172.17.3.5	78:32:1b:11:34:fa	Client Connection		Port: 9, Client MAC Address: 00:0c:29:6d0e40, VLAN: 1, Ty...
2021-11-30 09:53:36	Switch		172.17.3.5	78:32:1b:11:34:fa	Client Connection		Port: 9, Client MAC Address: 00:0c:29:cf436b, VLAN: 1, Ty...
2021-11-30 09:52:56	Switch		172.17.3.5	78:32:1b:11:34:fa	Client Disconnection		Port: 9, Client MAC Address: 00:0c:29:670f4c
2021-11-30 09:52:38	Switch		172.17.3.5	78:32:1b:11:34:fa	Client Connection		Port: 9, Client MAC Address: 28:3b:82:7f394e, VLAN: 1, Ty...
2021-11-30 09:51:09	Switch		172.17.3.5	78:32:1b:11:34:fa	Client Connection		Port: 9, Client MAC Address: a4ae:127b9e7e, VLAN: 1, Ty...
2021-11-30 09:50:32	Switch		172.17.3.5	78:32:1b:11:34:fa	Client Disconnection		Port: 9, Client MAC Address: 00:0c:29:6d0e40
2021-11-30 09:47:20	Switch		172.17.3.5	78:32:1b:11:34:fa	Client Disconnection		Port: 9, Client MAC Address: 00:0c:29:cf436b
2021-11-30 09:45:41	Switch		172.17.3.5	78:32:1b:11:34:fa	Client Disconnection		Port: 9, Client MAC Address: 00:21:5d2296ae
2021-11-30 09:45:21	Switch		172.17.3.5	78:32:1b:11:34:fa	Client Disconnection		Port: 9, Client MAC Address: a4ae:127b9e7e
2021-11-30 09:45:09	Switch		172.17.3.5	78:32:1b:11:34:fa	Client Disconnection		Port: 9, Client MAC Address: a0ab:1ba4:c20b
2021-11-30 09:43:54	Switch		172.17.3.5	78:32:1b:11:34:fa	Client Disconnection		Port: 9, Client MAC Address: ec44bb145ebc
2021-11-30 09:43:16	Switch		172.17.3.5	78:32:1b:11:34:fa	Client Connection		Port: 9, Client MAC Address: 00:0c:29:670f4c, VLAN: 1, Ty...
2021-11-30 09:42:09	Switch		172.17.3.5	78:32:1b:11:34:fa	Client Disconnection		Port: 9, Client MAC Address: f8bc:1272939f
2021-11-30 09:41:37	Switch		172.17.3.5	78:32:1b:11:34:fa	Client Connection		Port: 9, Client MAC Address: 00:0c:29:6d0e40, VLAN: 1, Ty...
2021-11-30 09:41:35	Switch		172.17.3.5	78:32:1b:11:34:fa	Client Connection		Port: 8, Client MAC Address: 00:0c:29:cf436b, VLAN: 1, Ty...

1 - 50 of 7874 total items: 7874

Nuclias Connect

Log

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
2021-11-30 09:34:35	Login	admin	Login	Login on 172.17.161.255.
2021-11-30 09:34:16	Login	admin	Login	Login on 172.17.161.255.
2021-11-29 18:51:01	Login	admin	Login	Login on 172.17.160.76.
2021-11-29 18:51:10	Logout	admin	Logout	Logout on 172.17.160.76.
2021-11-29 18:23:24	Login	admin	Login	Login on 172.17.160.76.
2021-11-29 18:22:10	Logout	admin	Logout	Logout on 172.17.160.76.
2021-11-29 17:51:04	Login	admin	Login	Login on 172.17.160.76.
2021-11-29 17:16:00	Logout	admin	Logout	Logout on 172.17.161.255.
2021-11-29 16:43:10	Logout	admin	Logout	Logout on 172.17.160.76.
2021-11-29 16:06:36	Login	admin	Login	Login on 172.17.161.255.
2021-11-29 16:05:00	Logout	admin	Logout	Logout on 172.17.161.255.
2021-11-29 15:58:18	Login	admin	Login	Login on 172.17.160.76.
2021-11-29 15:48:10	Logout	admin	Logout	Logout on 172.17.160.76.
2021-11-29 15:32:42	Login	admin	Login	Login on 172.17.160.76.

To generate an Audit Log report, select the entries by Operation Type (operations that performed on the object entities) and Object Entity (i.e. 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 is generated, click to export it as a local Excel file. The file will be saved to your browser's download directory and will be named as follows: Nuclias_Connect_log type_YYYY_MMDD_HHMMSS.

Nuclias Connect

Log

Alerts

This type of log records alert events such as new firmware release, port linked or blocked, device online status.

Default 09:59:14 2021/11/30

All Alert Events 2021.11.23 2021.11.30 IP Address Search 'Keyword'

Log Time	Network	Name	IP Address	MAC Address	Alert Event	Message	Action
2021-11-26 13:51:...	HQ		172.17.3.5	78:32:1b:11:34:...	Device restarted	2021-01-01 00:00:38 172.17.3.5 System st...	
2021-11-26 13:50:...	HQ	dap2610	172.17.3.6	10:62:eba8:00:...	Device offline	Device is disconnected.	
2021-11-26 11:59:...	HQ	dap2610	172.17.3.6	10:62:eba8:00:...	Device offline	Device is disconnected.	
2021-11-26 11:06:...	HQ	dap2610	172.17.3.6	10:62:eba8:00:...	Device offline	Device is disconnected.	
2021-11-26 10:52:...	HQ	dap2610	172.17.3.6	10:62:eba8:00:...	Device offline	Device is disconnected.	
2021-11-26 10:45:...	HQ	dap2610	172.17.3.6	10:62:eba8:00:...	Device offline	Device is disconnected.	
2021-11-26 10:41:...	HQ	dap2610	172.17.3.6	10:62:eba8:00:...	Device offline	Device is disconnected.	

1 - 50 of 7 total items: 7

Items per page

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 is generated, click to export it as a local Excel file. The file will be saved to your browser's download directory and will be named as follows: Nuclias_Connect_log type_YYYY_MMDD_HHMMSS.

Nuclias Connect

System

Device Management

Navigate to **System > Device Management** to view both managed and unmanaged devices on the network. To view more detailed information about the device, navigate to **Log > Device Log**.

First select the site and network, then click on the respective tab to view either managed or unmanaged devices.

The **Move to...** button on the upper right corner of each tab allows you to move devices between Managed and Unmanaged. When a device is moved to Unmanaged, you'll have to option to remove the device from the network by clicking the Delete button.

The list of devices can be sorted by the following criteria: Status, Local IP Address, NAT IP address, MAC Address, Model Type, HW Version, FW Version, Managed Time, Backup FW Version. The Menu button contains more fields to which you can add to the list to view.

The screenshot displays the Nuclias Connect web interface. The left sidebar shows the navigation menu with 'System' selected, and 'Device Management' highlighted. The main content area shows the 'Managed' tab for the 'STANLEY' network. At the top right, the time is 10:05:41 and the date is 2021/11/30. Below the tabs, there are filters for 'Device Type' (All Type) and 'Search By' (Local IP Address). A search bar with the placeholder 'Search Keyword' is also present. A 'Move to Unmanaged' button is located in the top right corner of the device list. The device list table has columns for Status, Local IP Address, NAT IP Address, MAC Address, Model Type, HW Version, FW Version, and a menu icon. Two devices are listed:


Status	Local IP Address	NAT IP Address	MAC Address	Model Type	HW Version	FW Version	Managed Time
<input type="checkbox"/>	172.17.3.5	172.17.3.5	78:32:1b:11:34:fa	DGS-1210-28P	F1	v6.30.014	2021/11/30 10:05:41
<input type="checkbox"/>	172.17.3.6	172.17.3.6	10:62:eba8:00:f0	DAP-2610	A1G	v2.06B02	2021/11/30 10:05:41

At the bottom, a pagination bar shows '1 - 50 of 2 total items: 2' and a dropdown for '50 items per page'.

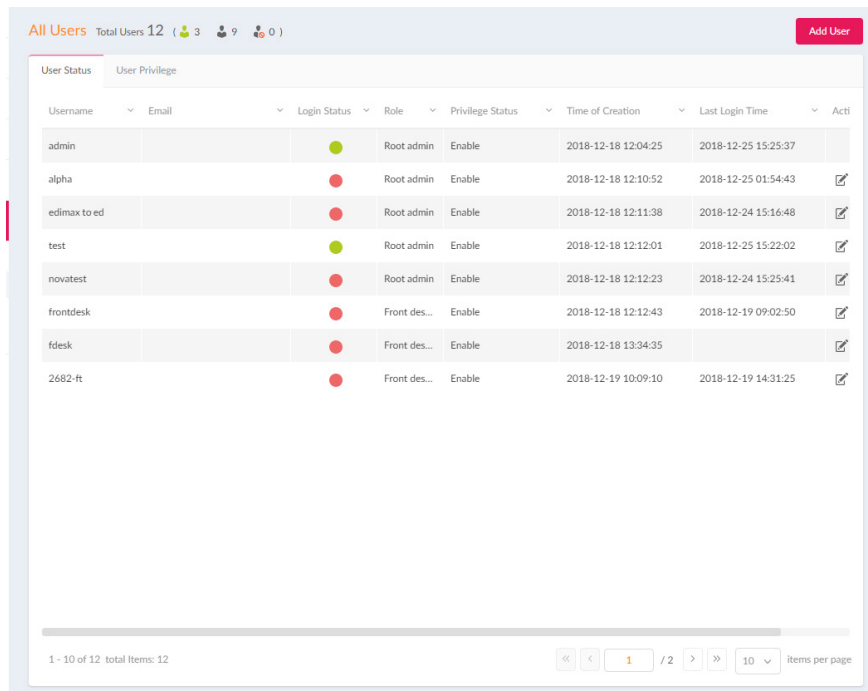
Nuclias Connect System User Management User Status








The User Status page allows administrators to view, edit, or delete the current status of all registered user profiles. When the Login Status shows green ●, the user is logged in. When the Login Status shows red ●, the user is logged out.

Navigate to **System > User Management** to view the relevant information.

To edit a user profile, click the edit button  corresponding to the user. The username, password, email, privilege, privilege status, location, contact number as well as the user description are available for edit. Note that the administrator account cannot be deleted or have its username and privilege settings modified.

Once the user settings are completed, click **Save** to confirm or **Cancel** to return to the previous menu.

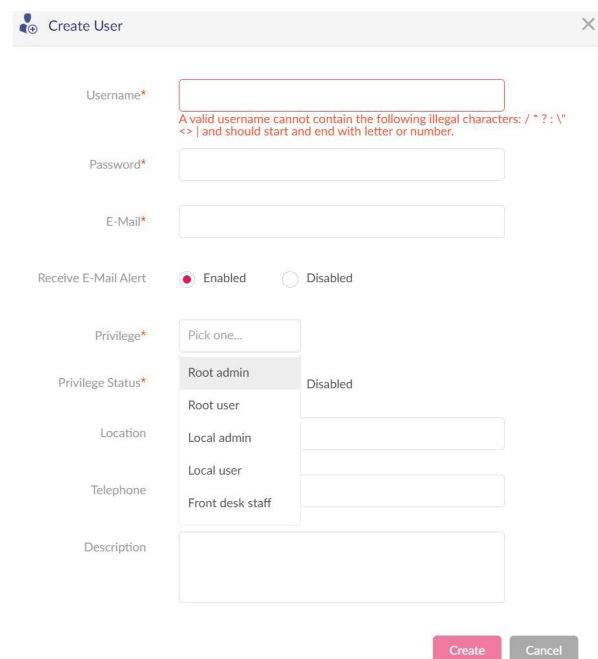


Username	Email	Login Status	Role	Privilege Status	Time of Creation	Last Login Time	Acti
admin		●	Root admin	Enable	2018-12-18 12:04:25	2018-12-25 15:25:37	
alpha		●	Root admin	Enable	2018-12-18 12:10:52	2018-12-25 01:54:43	
edimax to ed		●	Root admin	Enable	2018-12-18 12:11:38	2018-12-24 15:16:48	
test		●	Root admin	Enable	2018-12-18 12:12:01	2018-12-25 15:22:02	
novatest		●	Root admin	Enable	2018-12-18 12:12:23	2018-12-24 15:25:41	
frontdesk		●	Front des...	Enable	2018-12-18 12:12:43	2018-12-19 09:02:50	
fdesk		●	Front des...	Enable	2018-12-18 13:34:35		
2682-ft		●	Front des...	Enable	2018-12-19 10:09:10	2018-12-19 14:31:25	

To add a user to the selected network, click **Add User** to open the **Create User** page. In this page, enter the new user information. Fields marked with an asterisk (*) are required in order to complete the new entry. Once the information is filled in, click **Create** to save the new user profile. Alternatively, click **Cancel** to return to the previous screen without saving.

The following explains the profile privileges available in the Privilege drop-down menu.

Options	Description
Root admin	Manage all sites/networks on this server.
Local admin	Manage your own network.
Root user	View all sites/networks on this server.
Local user	View your own network.
Front desk user	Able to generate and manage passcodes.



Create User

Username*

A valid username cannot contain the following illegal characters: / * ? : \ " < > | and should start and end with letter or number.

Password*

E-Mail*

Receive E-Mail Alert

☒ Enabled

☐ Disabled

Privilege*

Pick one...

Root admin

Root user

Local admin

Local user

Front desk staff

Privilege Status*

Disabled

Location

Telephone

Description

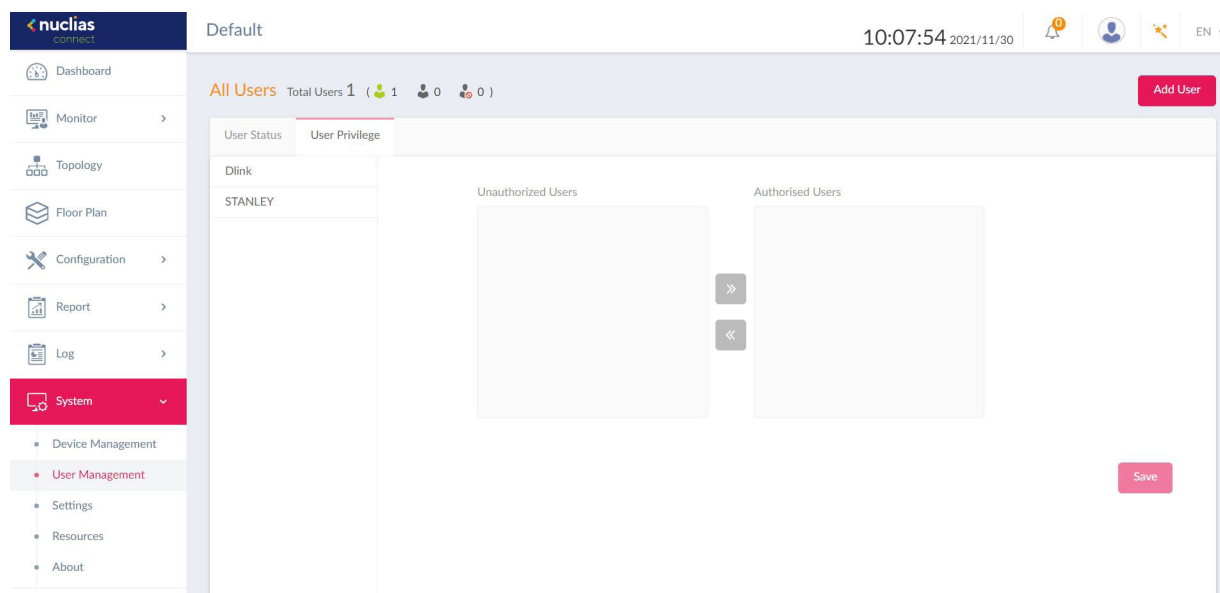
Create

Cancel

Nuclias Connect System User Management User Privilege

The User Privilege function allows administrators to add, view, and authorize/unauthorize users on a selected network. Navigate to **System > User Management** and click on the **User Privilege** tab to display the relevant information.

To authorize or unauthorize an existing user, click an available site and then the target network. The available users for the network are displayed on the ensuing screen. From the Unauthorized Users column, click the radio box of the target user. Once a user is selected, click **>>** to move to the respective column to authorize the user. The same process is used to unauthorize a user.



Nuclias Connect

System

Settings

General

The Settings page displays General, Connection, SMTP, Backup, REST API, Single Sign-On (SSO), Alerts, and FOTA information.

Under the General tab, there are options to customize system settings, which includes adding a logo and enabling the captcha feature. Device time and date and live packet interval settings are also available.

Navigate to **System > Settings** to configure your device settings.

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

Parameter	Description
Org Name	Enter a description to set the organization name.
Logo	Click Browser to select a file to be used as the interface logo. A local file can be selected by using the browse function or by dragging and dropping a file into the frame. Supported file types include PNG or JPG images.
Login Captcha	Click the drop-down menu to enable or disable the login Captcha function.

Click **Save** to save the settings.

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

Parameter	Description
Country	Click the drop-down menu to select the country region of the switches/APs in the network.
Time Zone	Click the drop-down menu to select the time zone.
Live Packet Interval	Click the drop-down menu to select the live packet interval time.

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

The screenshot shows the Nuclias Connect web interface. On the left is a sidebar menu with options: Dashboard, Settings, Topology, Floor Plan, Configuration, Report, Log, System (selected), Device Management, User Management, Settings, Resources, and About. The main content area is titled 'Default' and has tabs for General, Connection, SMTP, Backup, REST API, Single Sign-On (SSO), Alerts, and FOTA. The 'General' tab is active, showing 'Customized Settings' and 'Device Settings' sections. In 'Customized Settings', 'Org Name' is 'Default', 'Logo' has a drag-and-drop area with a 'Browser' button, and 'Login Captcha' is 'Disabled'. In 'Device Settings', 'Country' is 'United States', 'Time Zone' is '(GMT+08:00) Taipei', and 'Live Packet Interval' is '1 Min'. Both sections have a 'Save' button.

Nuclias Connect

System

Settings

Connection

The Connection tab displays device access address, port, and SSL certificate settings.

Navigate to System > Settings and click the Connection tab to display the relevant information.

In the Connection Setting section, the following parameters can be configured:

Parameter	Description
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; IP mapping is required for instances behind a firewall or router.
Device Access Port	Enter the Nuclias Connect server application's listen port number. The default value is 8443. For remote AP management behind a firewall or router, the inbound port must be opened.
CoreServer Access Port	Enter the server application's service port number. The default value is 8443.
Web Access Port	The web access ports as defined during the installation. The values are predefined.

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

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

Parameter	Description
Upload Certificate From File	Click Browse... to select the SSL certificate file located on the local drive.
Upload Key From File	Click Browse... to select the SSL key file located on the local drive.

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

The screenshot shows the Nuclias Connect web interface. The left sidebar contains navigation links: Dashboard, Monitor, Topology, Floor Plan, Configuration, Report, Log, System (selected), Device Management, User Management, Settings, Resources, and About. The main content area is titled 'Default' and shows the 'Connection' tab selected. The 'Connection Settings' section includes fields for Device Access Address (172.17.3.10), Device Access Port (8443), CoreServer Access Port (8443), and Web Access Port (30001). Below these fields is a 'Save' button. The 'Update SSL Certificate' section includes fields for 'Upload Certificate From File' and 'Upload Key From File', each with a 'Browse...' button and a 'Save' button. The top right of the interface shows the time 10:28:28, date 2021/11/30, and user information.

Nuclias Connect

System

Settings

SMTP

The SMTP tab displays customizable settings for the simple mail transfer protocol (SMTP). This is necessary in order to send emails on behalf of the system such as reset password validation emails.

Navigate to **System > Settings** and click on the **SMTP** tab to display the function information.

Parameter	Description
SMTP Host	Enter the SMTP server's IP address or domain name.
Port	Enter the SMTP server's port number.
From Email Address	Enter the sender's email address.
From Name	Enter the sender's name.
Security Type	Click the drop-down menu to select the security type to be used in the e-mail system. The options include None or SSL.
Encoding Type	Click the drop-down menu to select the encoding type to match the supported e-mail client. The options include UTF-8 or ASC-II.
Authentication	Click the drop-down menu to select the authentication mechanism during login. The options include Anonymous or SMTP Authentication.
Test Email	Enter the recipient e-mail address to initiate a test e-mail through the SMTP configuration. Click Test to start the test function.

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

The screenshot displays the Nuclias Connect web interface. On the left is a sidebar menu with various system management options. The main panel is titled 'Default' and contains several tabs: General, Connection, SMTP (which is active), Backup, REST API, Single Sign-On (SSO), Alerts, and FOTA. Below the tabs is a 'Customized Settings' section with the following fields and controls:

- SMTP Host***: A text input field with the placeholder 'Host'.
- Port***: A dropdown menu currently showing '25'.
- From Email Address***: A text input field with the placeholder 'From Email Address'.
- From Name***: A text input field with the placeholder 'From Name'.
- Security Type**: A dropdown menu currently showing 'None'.
- Encoding Type**: A dropdown menu currently showing 'UTF-8'.
- Authentication**: A dropdown menu currently showing 'Anonymous'.
- Test E-Mail**: A text input field with the placeholder 'Test E-Mail', followed by a pink 'Test' button.

At the bottom of the settings section is a pink 'Save' button.

Nuclias Connect

System

Settings

Backup

The Backup tab displays customizable settings for backing up configuration settings or logs. Navigate to System > Settings and click on the Backup tab to display the function information.

In the Auto Backup Settings section, parameters regarding auto backup can be configured:

Parameter	Description
Auto Backup	Click on drop-down list to enable or disable auto backup.
Interval Time	The interval time for backup
Backup File	Configuration backup
Backup Path	Click "Change" button to change default path

In the **Backup Settings** section, device configuration and logs can be backed up, downloaded to a local hard drive, or deleted.

Click "Backup Now" to backup the configuration file or log files.

Click the Download button to download the backup file to the management computer's hard drive.

Click the Delete button to delete the backup configuration files or log files that are stored on the device.

Check the Overwrite box to overwrite old log when the hard disk reaches full capacity.

In the Restore Settings section, device configuration can be restored from local hard drive.

Select a configuration file to restore a configuration.

Nuclias Connect

System

Settings

REST API

REST API is a software interface that allows two applications to communicate with each other over the internet and through devices. Enable it to allow Nuclias Connect communicate with third-party application through REST API.

REST API

Please note that the network without network ID cannot be accessed by REST API.

REST API

Disabled

Save

Nuclias Connect System Settings Single Sign-On (SSO)

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

There are three steps in the registration process.

Step 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.

nuclias connect

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
Asia

Country
Taiwan

Next

Already have an account? [Log in](#)

Step 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 to enable the account creation button.

Click **Create Account** to continue.

STEP 2
Create your Nuclias account that you may log in either Nuclias Connect or Nuclias Cloud.

nuclias connect

tester@aaa.com

Peter

ANT

Taiwan

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

Address

☒ I have read and agree to the [Terms](#) and [Privacy](#)

Create account

Step 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
Verify your email.

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

Close

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

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

Parameter	Description
Enable single sign on	Check to enable single-sign-on.
Nuclias Account	Enter your Nuclias Account username.
Nuclias Password	Enter your Nuclias Account password.

The Nuclias Connect Portal provides you with an easy way to view and connect to Nuclias Connect.

Requirements for use include:

- A Nuclias account
- DNC-100 with single-sign-on enabled

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

The Portal provides the following information:

Parameter	Description
Number	Number of the DNC-100 on the list.
Status	The connection status between the Nuclias Connect portal and DNC-100.
Name	Name of the Nuclias Connect. You can change this name by clicking on it then typing on the available text box.
Host	Displays both the device IP address and its public IP address.
Sites	Number of sites managed by DNC-100.
Networks	Number of networks managed by DNC-100.
Devices	Number of devices managed by DNC-100.
Clients	Number of clients connected to devices managed by DNC-100.
Version	Software version of DNC-100.
Actions	Click Launch to open the DNC-100 Nuclias Connect interface. Please note that IP mapping is required for instances behind a firewall or router. Click Forget to unlink DNC-100 from the Nuclias Connect portal. (Forget is only available when the device is offline.)

Nuclias Connect

System

Settings

Alerts

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

To receive Email alerts, check the Email box next to the Events, and go to **System>Settings>User Management**, edit the user and select “Receive Email Alert” to allow users to receive email alerts from Nuclias Connect.

Site/Network Events	Alerts	Email
Firmware Upgraded Failed	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Device Has Been Removed From Network	<input type="checkbox"/>	<input type="checkbox"/>
Profile Has Been Changed	<input type="checkbox"/>	<input type="checkbox"/>
Profile Failed To Be Applied	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Device Events	Alerts	Email
Device Restarted	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Offline	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device Online	<input type="checkbox"/>	<input type="checkbox"/>
Port Link Down	<input type="checkbox"/>	<input type="checkbox"/>
Port Blocked	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Save

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

Nuclias Connect

System

Settings

FOTA

The FOTA (Firmware Over-The-Air) feature enables users to wireless upgrade to the latest firmware. Click the box to enable automatic firmware check. Once Auto Check is enabled, you can then set a check interval between 1-720 hours.

Note that when Auto Check is enabled, the Alert and Email settings will also be enabled.

The screenshot shows the Nuclias Connect web interface. The top navigation bar includes the Nuclias Connect logo, a 'Default' label, a trial status 'Trial (5 days), click to activate', the time '15:21:38', the date '2021/11/09', and user profile icons. The left sidebar contains a menu with items: Dashboard, Monitor, Topology, Floor Plan, Configuration, Report, Log, System (expanded), Device Management, User Management, Settings (highlighted), Resources, and About. The main content area displays the 'FOTA' settings page. At the top of this page are tabs for General, Connection, SMTP, Backup, REST API, Single Sign-On (SSO), Alerts, and FOTA. A note states: 'Please note that the Alerts setting and Email setting of New Firmware release in System>Settings>Alerts will be enabled if the Auto Check is enabled.' Below this, there is a checkbox labeled 'Check Firmware Version Automatically' which is checked. Underneath, a 'Check Interval' is set to '24' in a text box, with '(1-720)Hours' indicated to the right. A red 'Save' button is positioned below the interval field.

Nuclias Connect

System

Resources

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



Nuclias Connect

System

About

The **About** page displays a list of supported switches and access points.

Navigate to **System > About** to view the information.

The list can be updated by clicking **Update Online**. If an update is available, new supported device will also be displayed.

Default

Trial (5 days), click to activate 15:26:27 2021/11/09

Version: 1.2.0.5 (Not Activated) [Update Online](#)

Device Type: All Device Types Search By: Model Type Search 'Keyword'

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

1 - 20 of 27 total Items: 27

Navigation: << < 1 / 2 > >> 20 items per page