D-Link

2021 | Business Class Networking

# NUCLIAS CONNECT
# User Manual

V 1.10

nuclias connect

# Table of Contents

# 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 APs** | 1500 APs | 100 APs |
| **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 NIC[1]** | Gigabit Ethernet Card | Gigabit Ethernet Card |
| **Monitor Resolution** | 1080P | 1080P |
| **Platform (Windows)** | Windows 10 Server 2019 (64-bit) | Windows 10 Professional (64-bit) |
| **Platform (Linux[2])** | Ubuntu<br>CentOS 7 | Ubuntu<br>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.

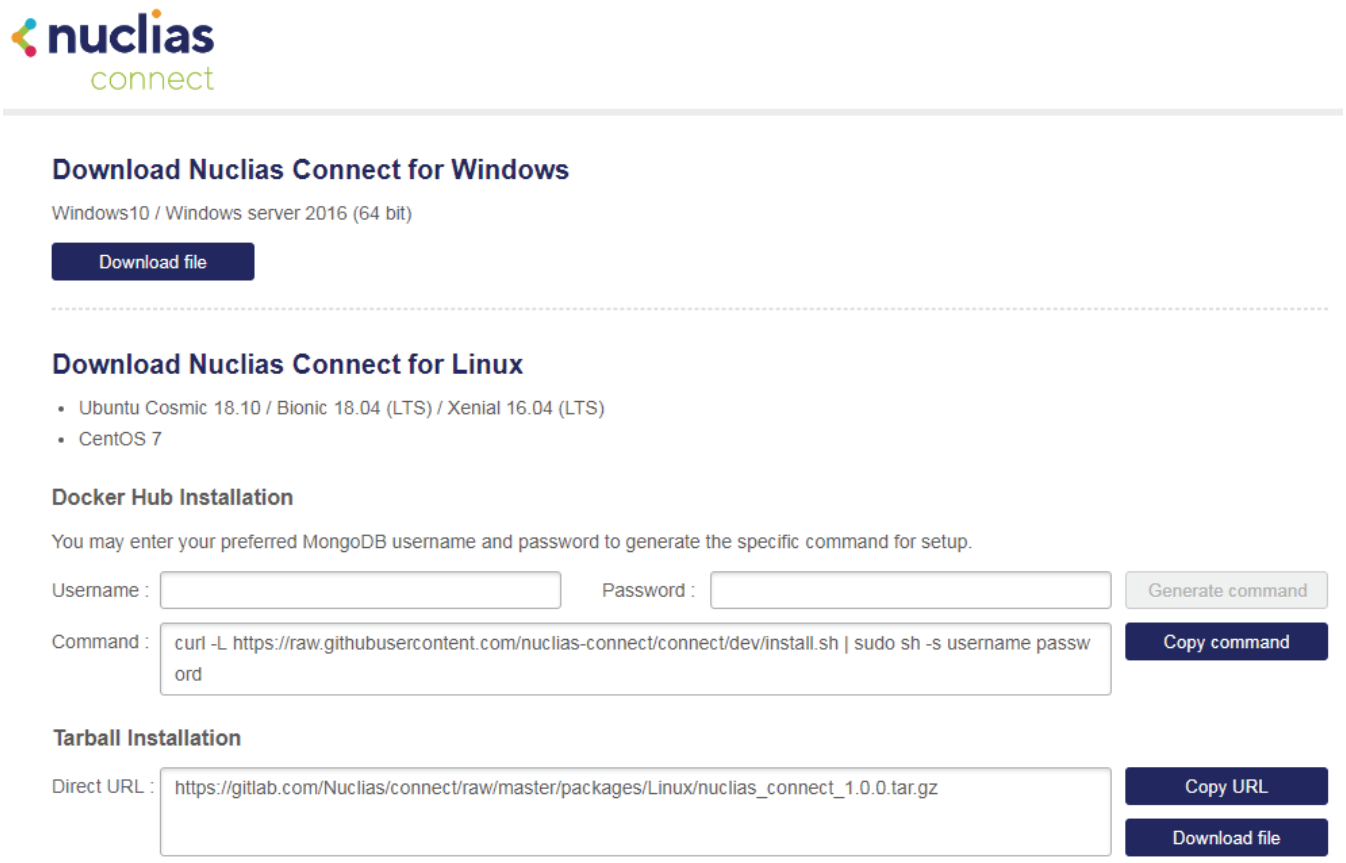
The following software applications must be installed in the following order:

- 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 DAP 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 apear as per the following figure.



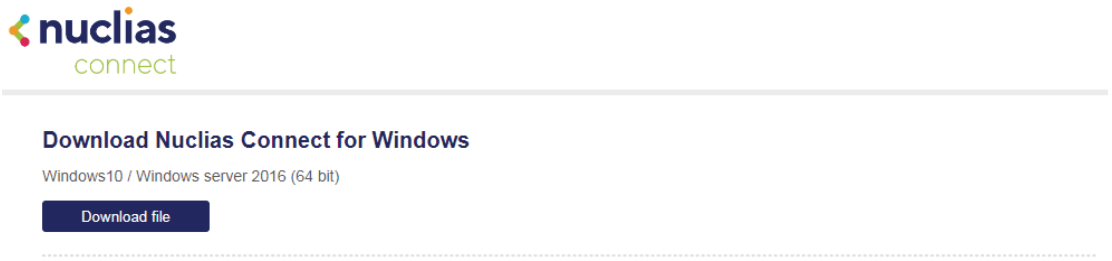
# Software Installation

## 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.




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

Once 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

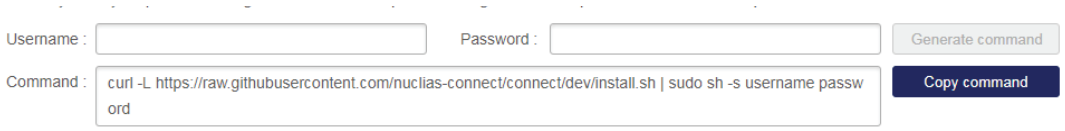
A specific command line can be downloaded from the Nuclias Connect download website.

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.


Click on the **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

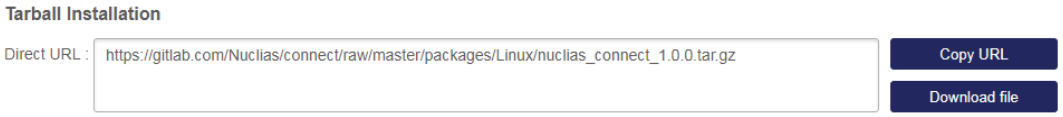
Nuclias Connect is also available for Linux through a compressed tarball file. Use the following information to obtain the correct Nuclias Connect package.

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.




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

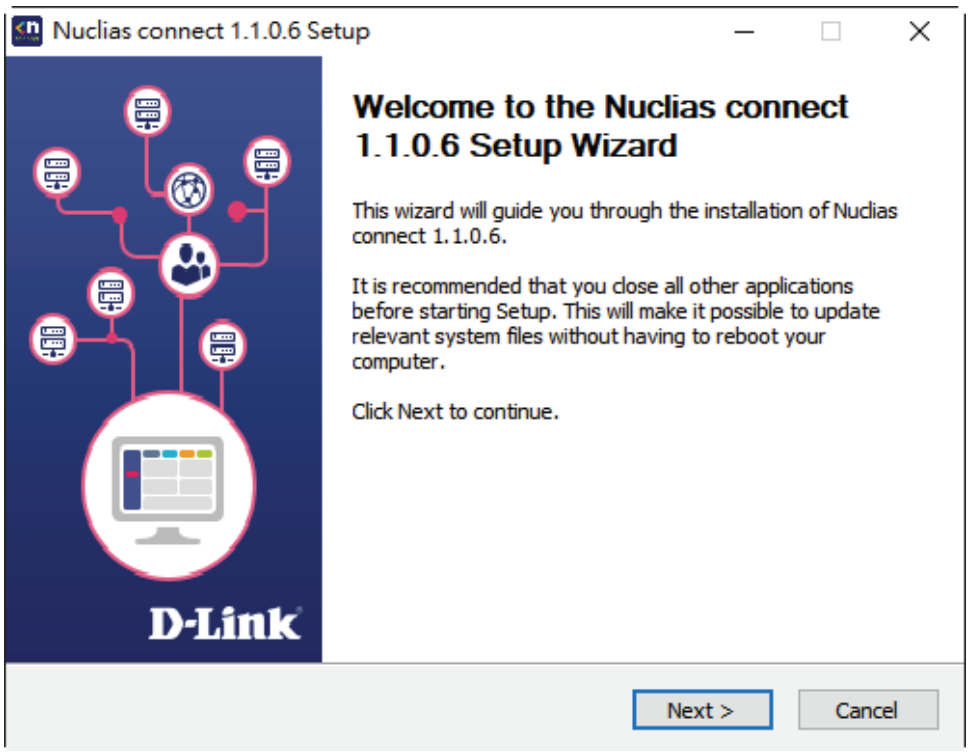
Once download is complete, you can begin the installation.

# Software Installation Nuclias Connect Server Installation

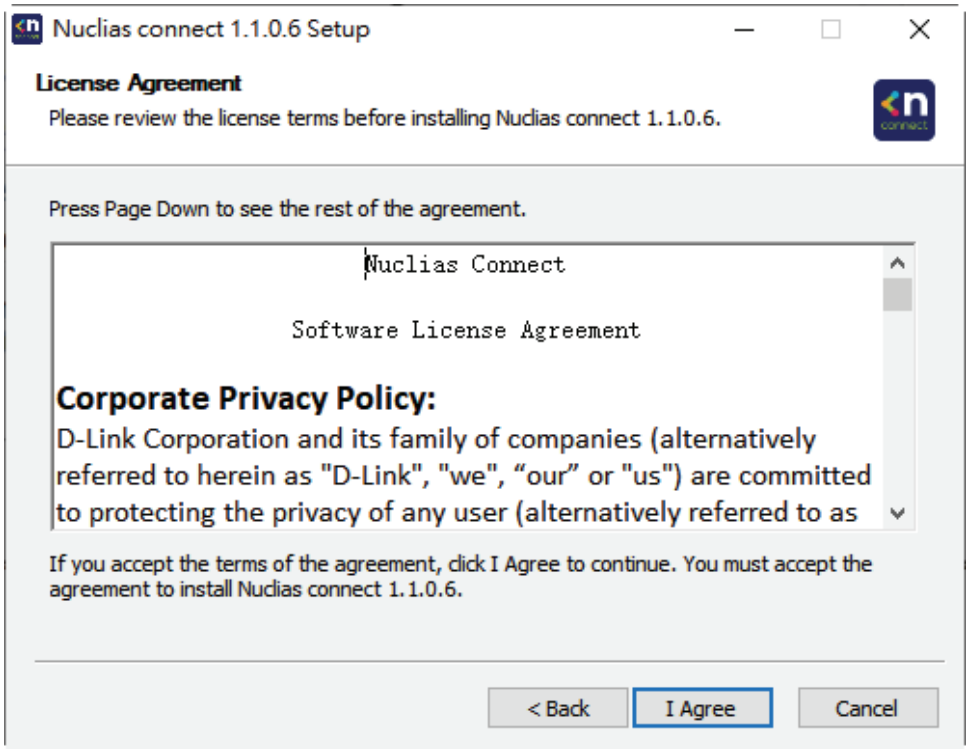
## Windows Installation

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.



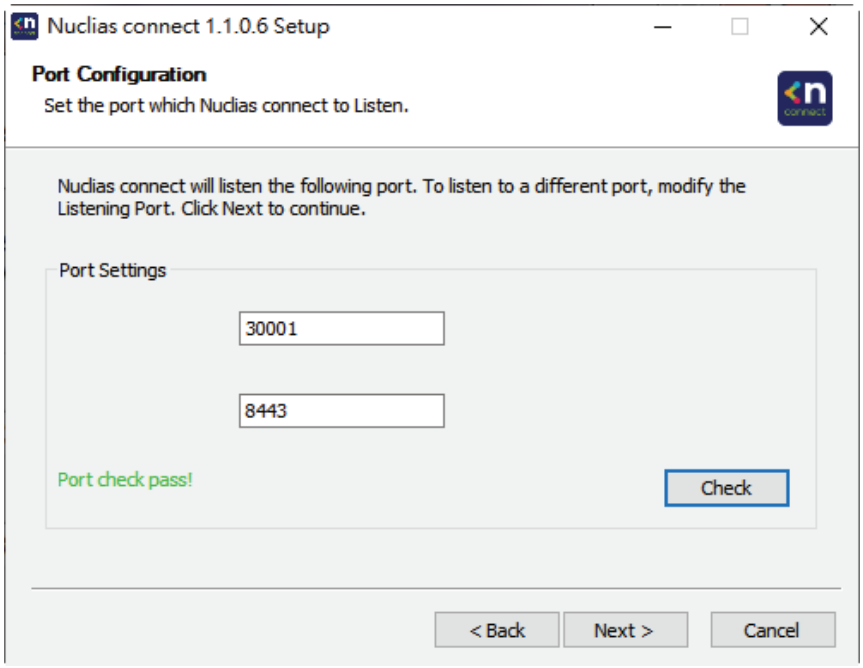

The License Agreement window will appear. Before installing review the license terms. Once accepted, click the **I Agree** button to continue.



# Software Installation Nuclias Connect Server Installation Linux OS 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.

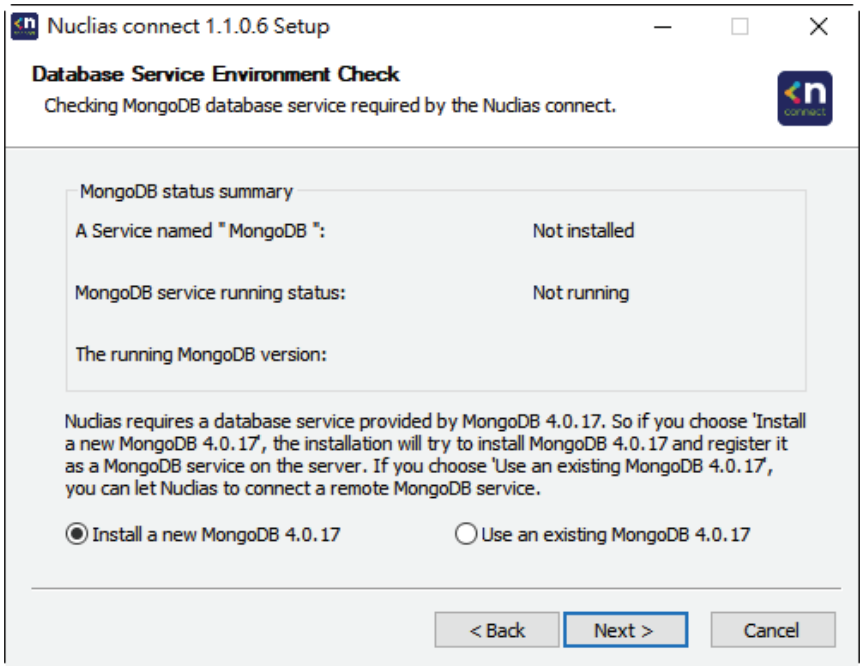
Click the **< Back** button to return to the previous step. Click the **Next >** button to continue to the next step. Click the **Cancel** button to stop and exit the installation.




The **Database Service Environment Check** window displays. At this stage, the setup performs a systems check for the required MongoDB database services. A report is visible in the MongoDB status summary field displaying the installed, if any, 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.

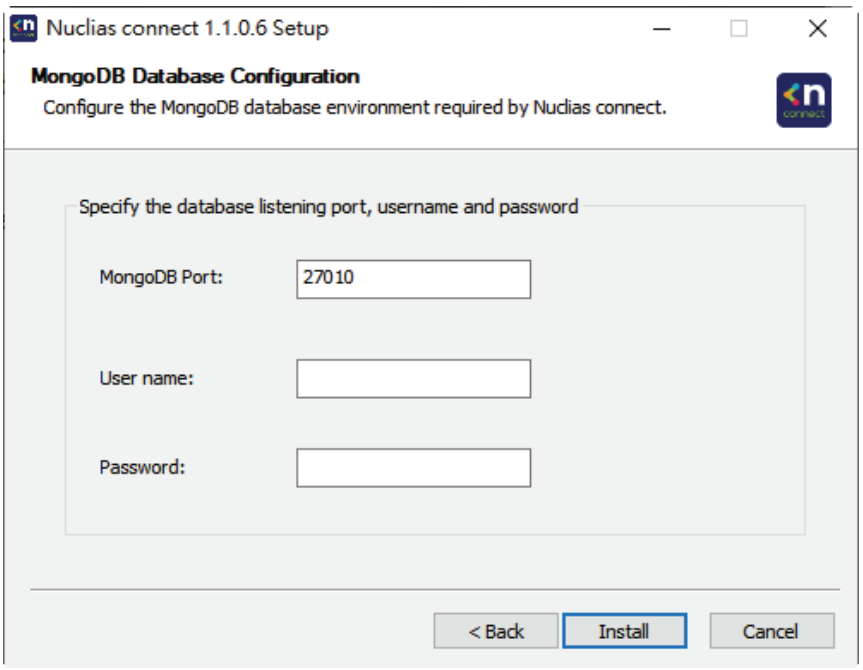
Click the **< Back** button to return to the previous step. Click the **Next >** button to continue to the next step. Click the **Cancel** button to stop and exit the installation.



# Software Installation Nuclias Connect Server Installation Windows Installation

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

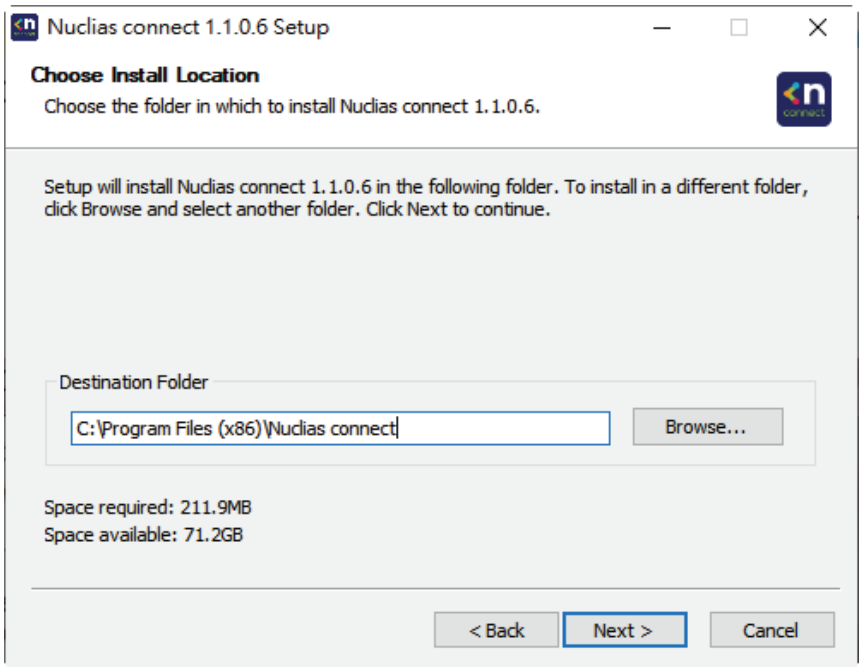
Click the **< Back** button to return to the previous step. Click the **Next >** button to continue to the next step. Click the **Cancel** button to stop and exit the installation.




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.

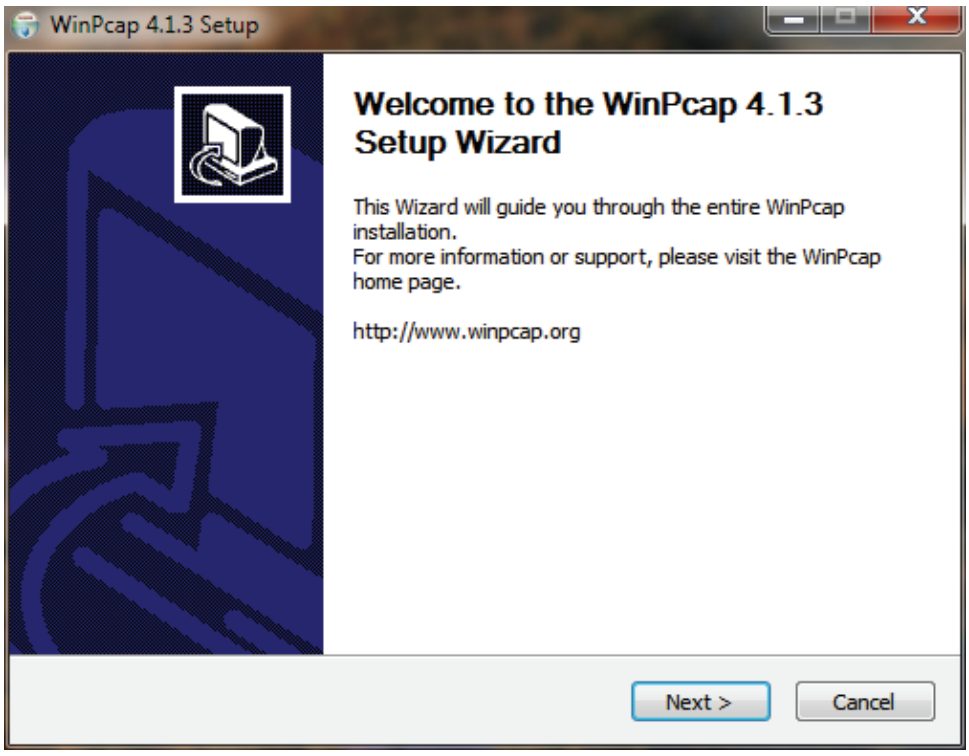


# Software Installation Nuclias Connect Server Installation

## Windows Installation

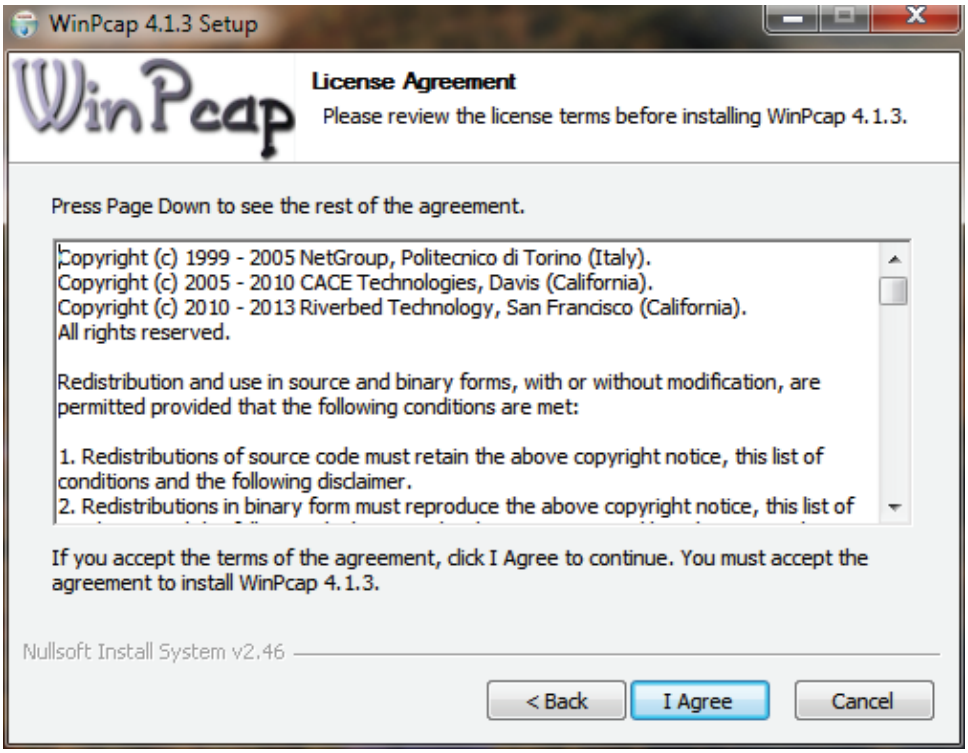
The **WinPcap Setup Wizard** window will appear. The WinPcap installation allows link-layer network access in Windows environments, allowing applications to capture and transmit network packets bypassing the protocol stack, this includes kernel-level packet filtering, a network statistics engine and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

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



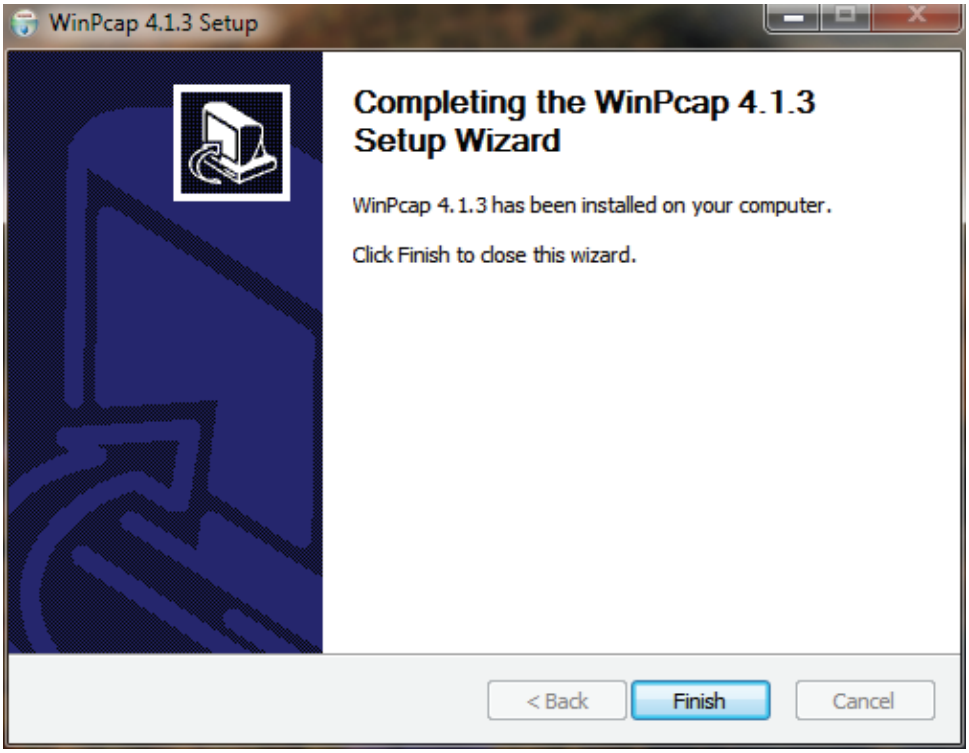

The **License Agreement** window will appear. Review the license terms before installing WinPcap. Once the agreement is accepted, click **I Agree** to continue.

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



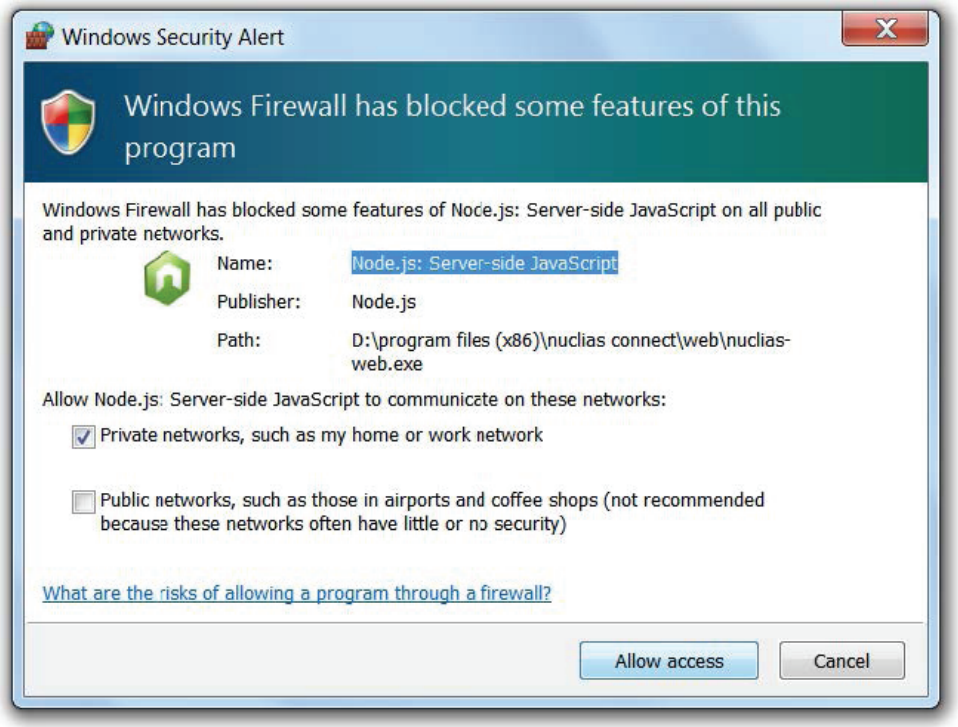
# Software Installation Nuclias Connect Server Installation Windows Installation

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



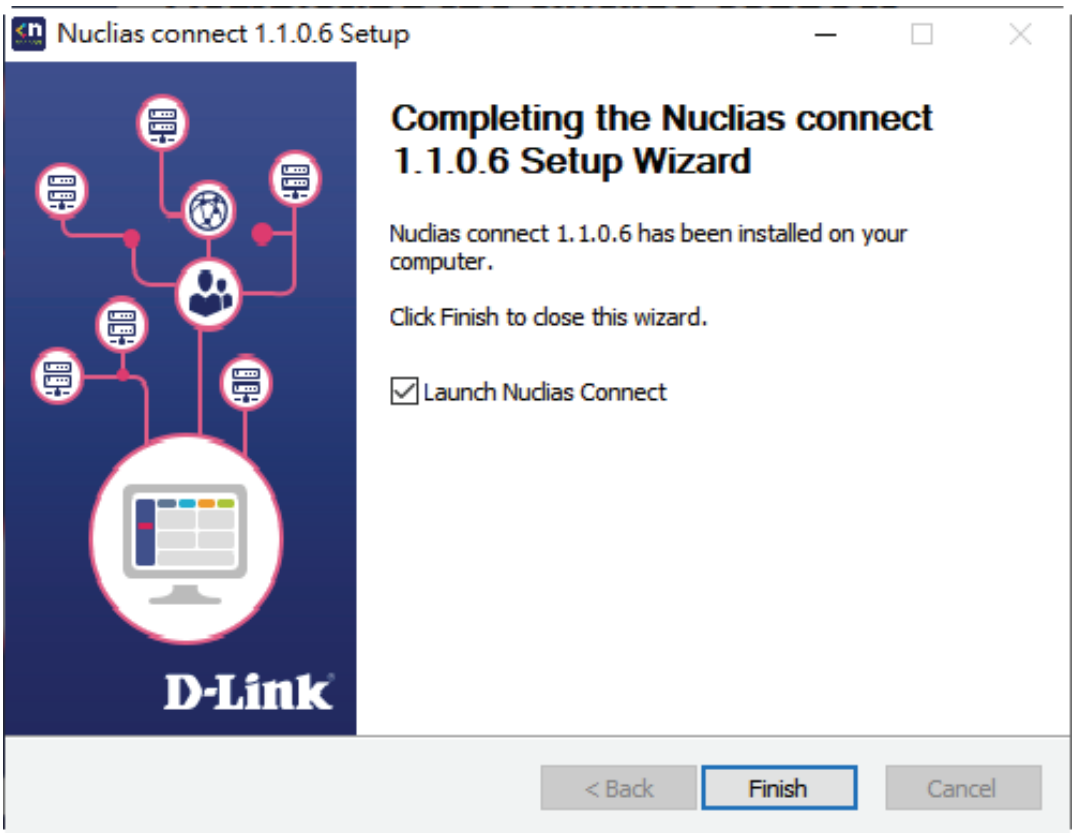

Once the WinPcap tool has been installed, the Nuclias Connect setup wizard will continue with the installation.

A Windows Security Alert window may display a warning that certain features are blocked from installation, such as the Server-side JavaScript. If the pop-up window appears, select the network setting—in the following figure **Private networks, such… network** was selected — 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.

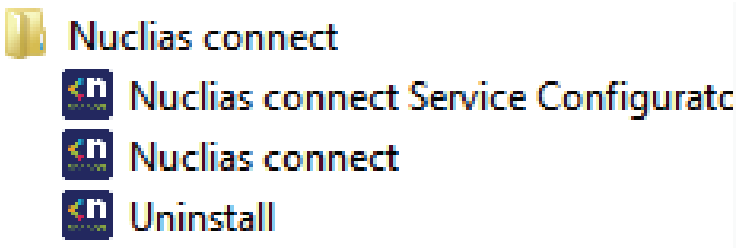


# Software Installation Nuclias Connect Server Installation Windows Installation

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 Nuclias Connect Server Installation Windows Installation

# Running the Nuclias Connect Server

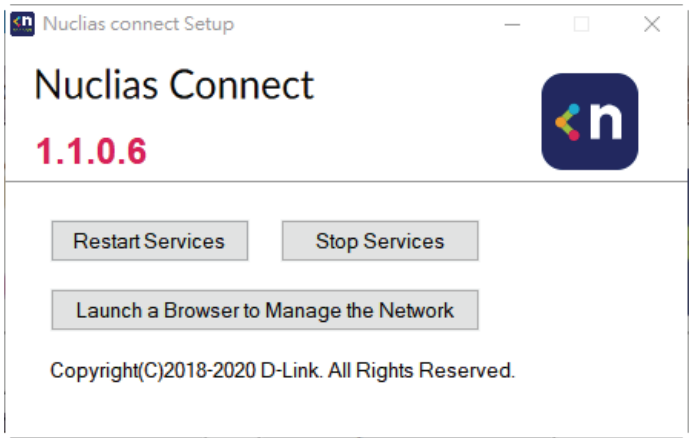
This section describes how to run the Nuclias Connect Server application. After the installation is completed, the following applications will appear on the Programs listing.

**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.

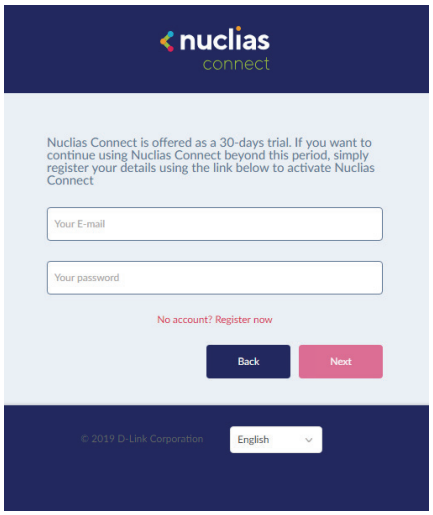
The Nuclias Connect configuration interface is accessible through a browser window. Click **Launch a Browser to Manage the Network** to open a default browser window.




# 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.

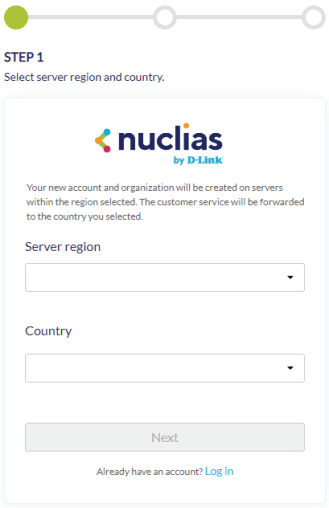


# Software Installation
## Nuclias Connect Server Installation
## Windows Installation

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.

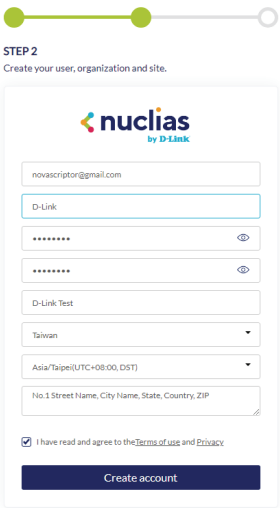
The account is created on the servers within the selected region and the selected country. Your account data will be stored in the reginoal server based on your selected region and country.




**NOTE:** If you already have an account, you may use this account to login without creating a new account.

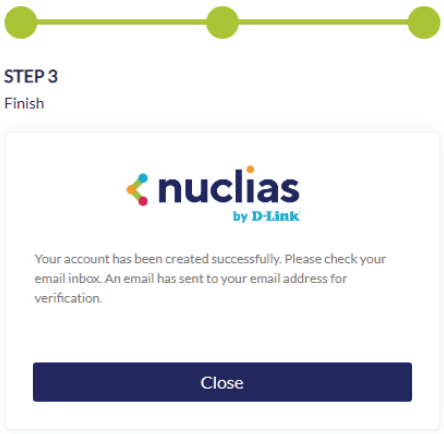
Once the region and country have been entered, you will see the the user, organization, and site page. Enter the required information and agree to the Terms of Use and Privacy agreement to enable the account creation button.

Click **Create Account** to continue.



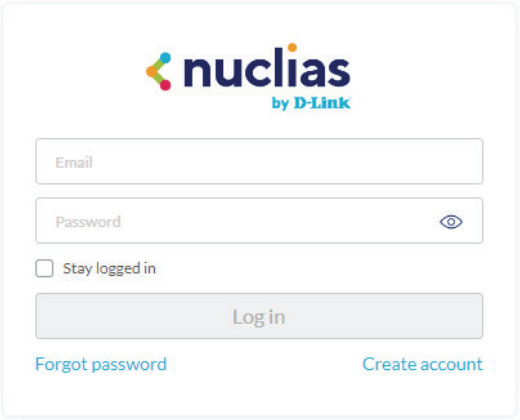
# Software Installation Nuclias Connect Server Installation Windows Installation

If the registration was a sucess, 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.

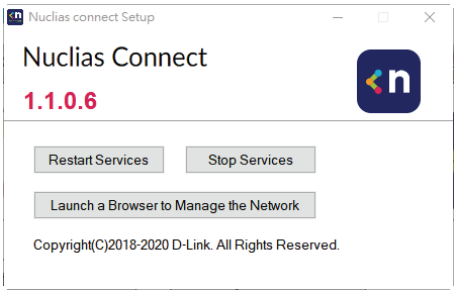
You will be redirected to the Login page. If you do not have Nuclias Cloud-enabled devices you may skip this step.



Software Installation Nuclias Connect Server Installation Windows Installation

# Launch Nuclias Connect

The 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).



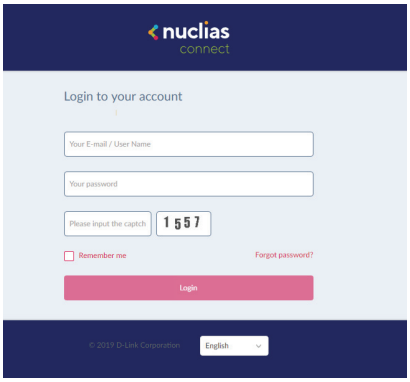

On the locally installed software, use the Nuclias Service Configurator or the Nuclias Connect shortcuts to open the interface in a browser.

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 launch 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.

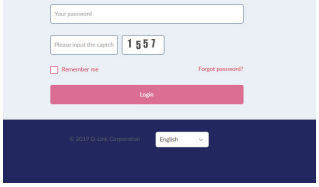




Enter the modified username and password in the respective fields.

Enter the Captcha code as shown on screen.

**NOTE:**

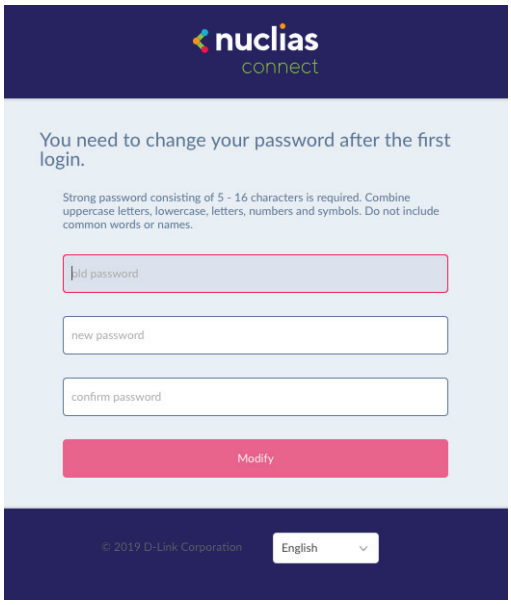
- The Remember me function can be selected to save the password entry for future use.
- The Forgot password? function provides an option to reset your password in the event that you've forgotten your current password.
- The interface supports Multilanguage options. By clicking the language drop-down menu, a different language can be selected.



# Software Installation Nuclias Connect Server Installation Windows 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. By combining uppercase and lowercase characters, numbers and symbols a strong password can be created.




**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 order, before continuing on to the next item in 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). For this section, Docker CE is used in the writing. 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 priviledges

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.

# 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/system/system/multi-user.target.wants/containerd.service/lib/system/system /
conatinerd.service.
Setting up Ubuntu-fan  (0.12.12) ...
Created symlink /etc/system/system/multi-user.target.wants/Ubuntu-fan.service/lib/system/system /
Ubuntu-fan.service.
Setting up docker.io (18.09.4-0ubuntu1) ...
Adding group ‘docker’ (GID 130)
Done.
Created Symlink /etc/system/system/sockets.target.wants/docker.socket □ /lib/system/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
```

# Install Docker Compose

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

# Prerequisites

Docker Engine must be installed prior to ithe 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 Nuclias Connect Server Installation Linux OS 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 of the downloaded tar package. For 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 sevice 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
```

```
-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, use the following 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 for use in a web browser is found below. This instance's address is 172.17.5.47, but yours may be different.

```
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, MULTICAT, 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:bcbd:6cda:4dc3/64 scope link noprefixroute
     valid_lft forever preferred_lft forever
3: wlp2s0: <NO-CARRIER,BROADCAST, MULITCAST,UP>      mtu 1500 qdisc noqueu 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, MULITCAST,UP>     mtu 1500 qdisc noqueu state DOWN group
default qlen 1000
   link/ether 02:42:11:ff:39:9f brd ff:ff:ff:ff:ff:ffs
   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.

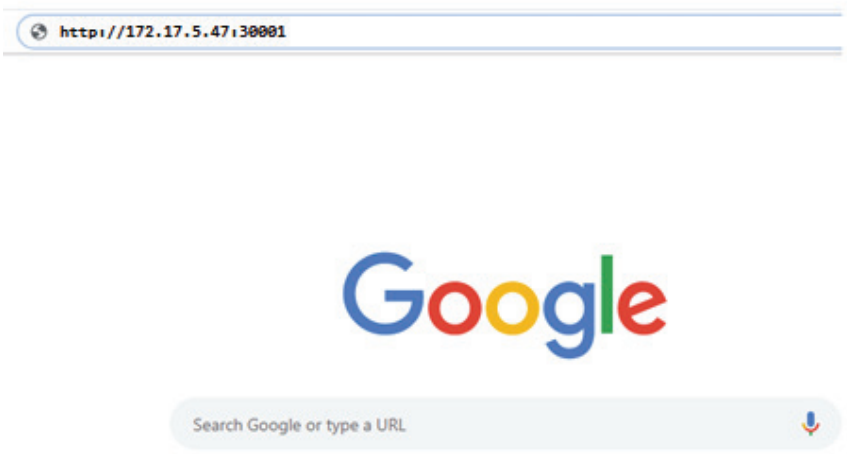
To obtain the defined IP address to access the Nuclias Connect through a web browser see "" on page 24.

The default settings for the Nuclias Connect are as follows:

- Web port: 30001

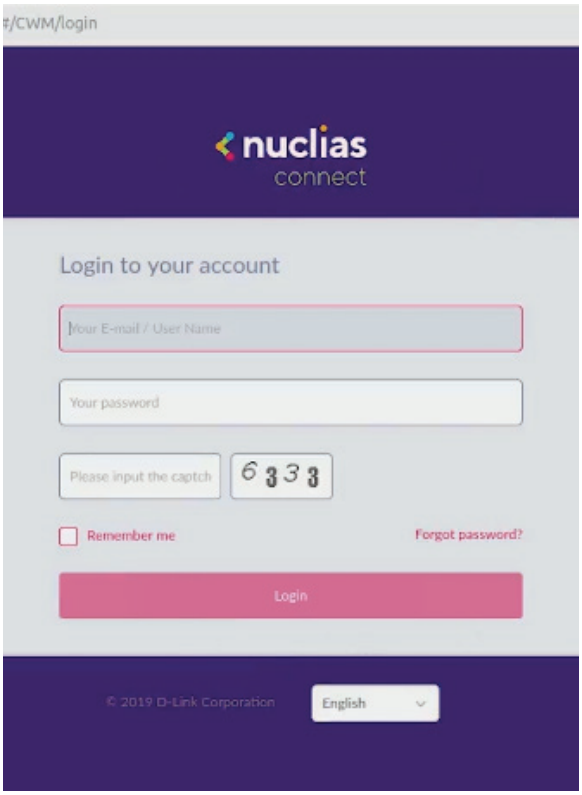
From the desktop, open a web browser.

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.

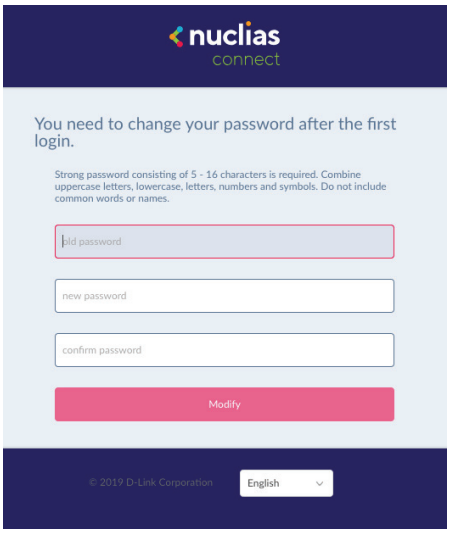
The Nulicas Connect main login screen will appear as seen in the following figure.



# 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.

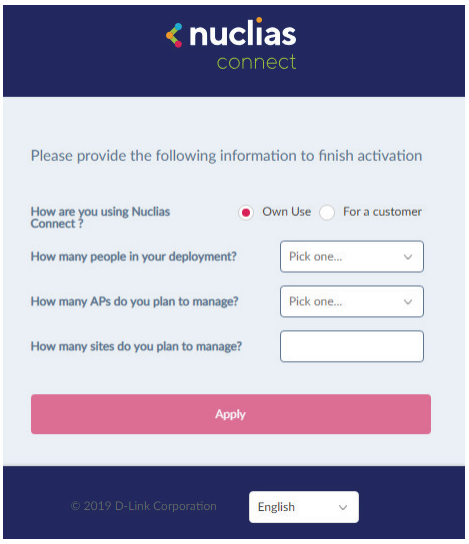
Click Modify to continue.



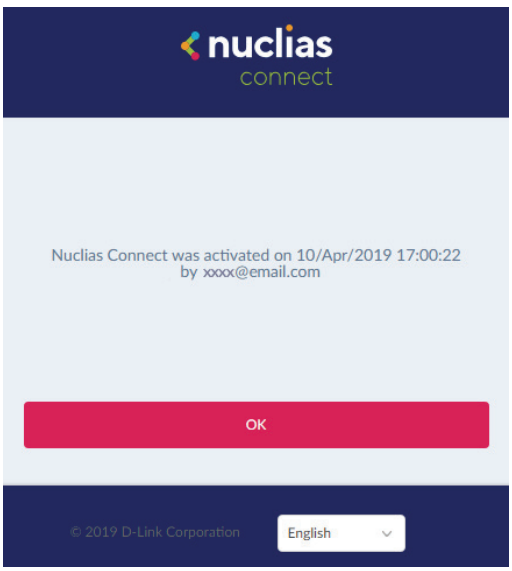

After a successful password change, you will be required to provide some installation information to continue the activation.

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.



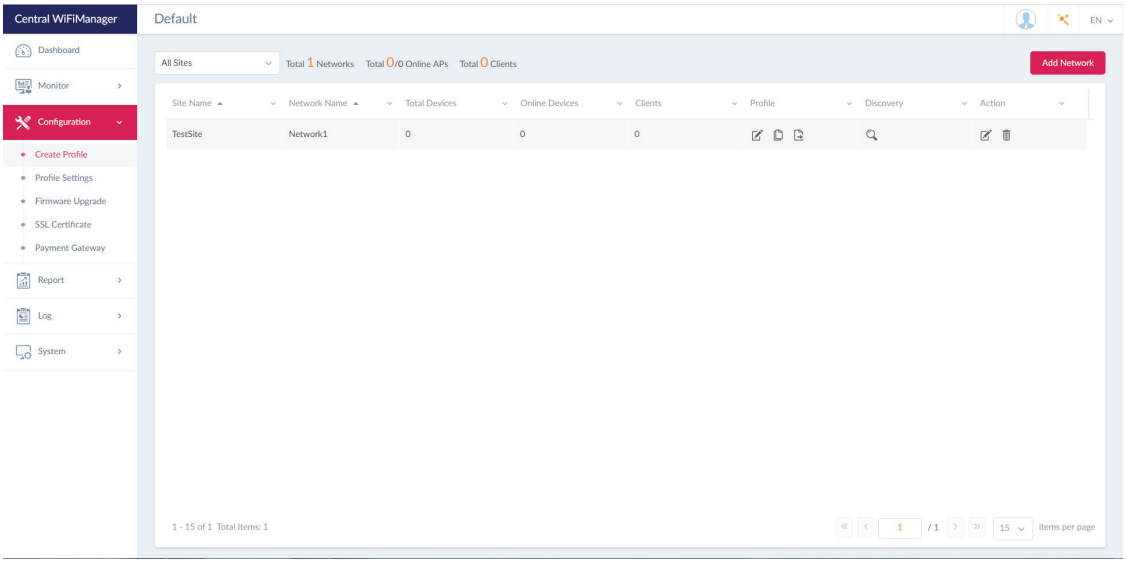
# Software Installation Nuclias Connect App

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.

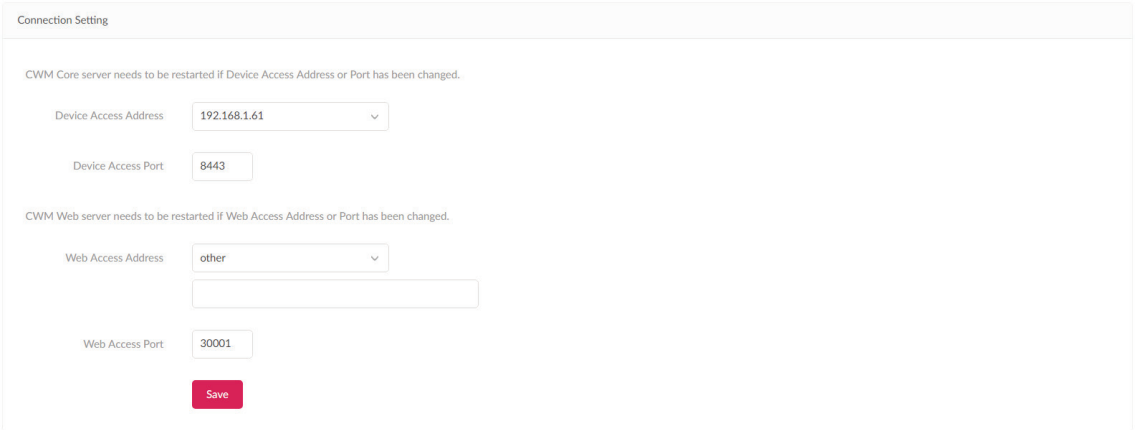
This section provides information on exporting the required network profiles from the Nuclias server for managing connected DAPs. Additional information explaining the functionality of the Nuclias Connect App is also included.

## 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. Select **Configuration** and then click the **Export** ( ) icon to export the network profile to your computer.




When 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.



# Software Installation Nuclias Connect App

## Discover and Configure APs Using the Nuclias Connect App

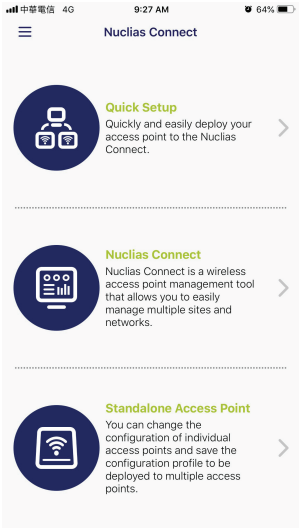
The Nuclias Connect App is a wireless access management tool that provides the means to easily manage single or multiple sites and networks from your smartphone or tablet. With the Nuclias Connect App, you can quickly deploy standalone DAPs to the Nuclias Connect, scan a network for D-Link access points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

**NOTE:**
- The Nuclias Connect App cannot discover 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 DAP 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 DAPs and save the configuration profile to be deployed to multiple DAPs.

### *Quick Setup*

After opening the Nuclias Connect App, the following window will appear (iOS). Tap on Quick Setup to start the setup process.

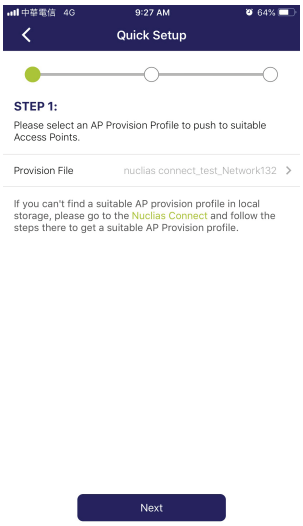


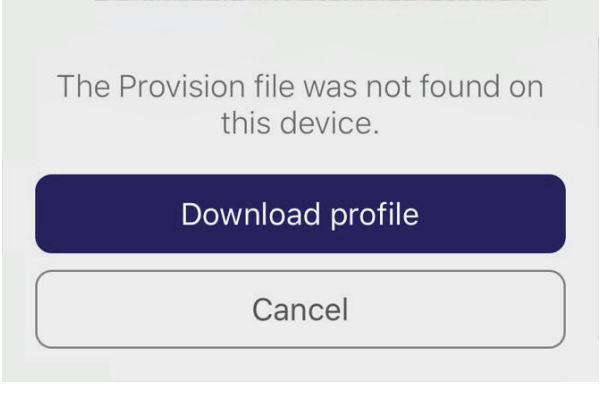

The next step is to select an AP provision profile. The profile is used to push to the selected DAPs. Tap **Quick Setup** to begin the deployment of a standalone DAP to the Nuclias Connect server.

The **Step 1** screen will appear. In the below fiture the Provision File entry shown 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** in order to specify a connection to the Nuclias Connect controller.

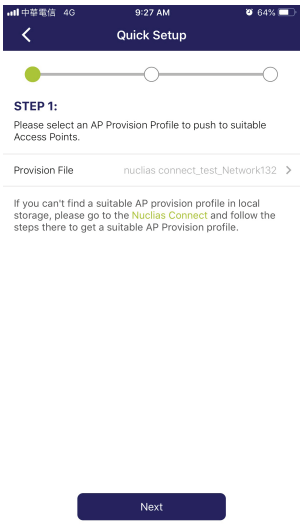


# Software Installation Nuclias Connect App

Once a Nuclias Connect controller connection is established, you will see it 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.

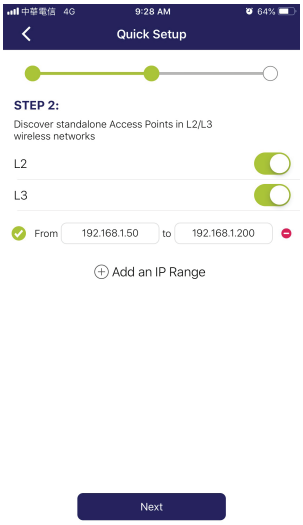

The process will continue and the App wil return to the previous screen. From the Step 1 page, tap **Next** to continue.

Step 2 will appear. From this page, you can discover standalone DAPs 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.

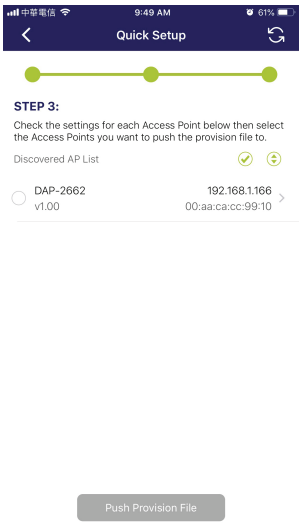


# Software Installation Nuclias Connect App

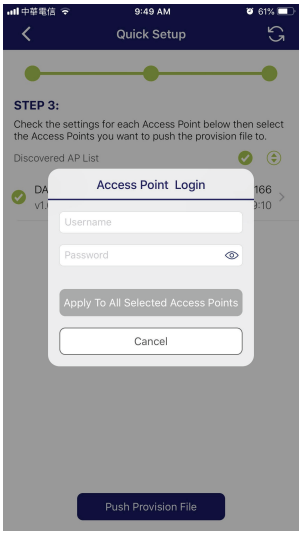
After the scanning the network range, the Step 3 page will list any detected access points.

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

Tap **Push Provision File** to continue.




The DAP login pop-up window displays. 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 DAP.




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.

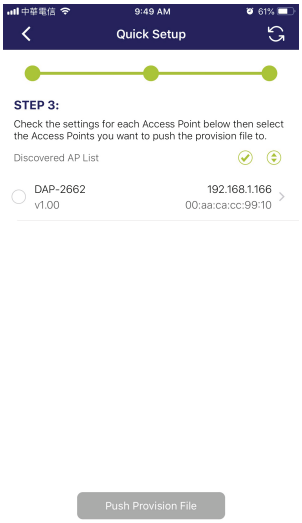
| Parameter | Description |
|---|---|
| **Cancel** | Tap to discard any changes and continue the process. |
| **Done** | Tap to accept any changes and continue the process. |
| **Model Name** | Displays the model name for the listed DAP device. |
| **MAC** | Displays the MAC address of the listed DAP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

# Software Installation Nuclias Connect App

| Parameter | Description |
|---|---|
| **DHCP Mode** | Tap to enable or disable the DHCP mode function. When enabled, the DAP 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 DAP device (s). The App will return to the Step 3 page and will display the status of the Push function. The discovered DAPs 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.

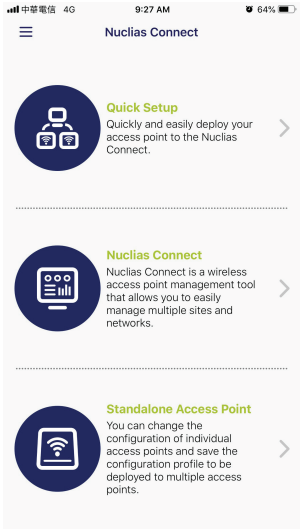


# Software Installation Nuclias Connect App

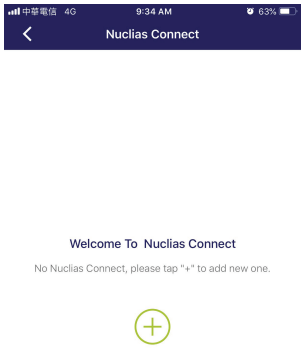
***Nuclias Connect***

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 no previous Nuclias Connect controller was paired it will ask you to create a new Nuclias Connect pairing. Tap the add (⊕) button to start the process.



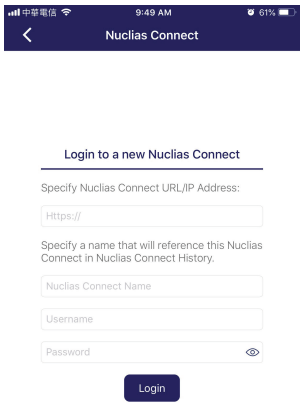

The following page lists the information required to log in to a designated Nuclias Connect controller. Enter the required information in each field.

| Parameter | Description |
|---|---|
| **Specify NuciasConnect 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 easily identify the paired Nuclias Connect server. |

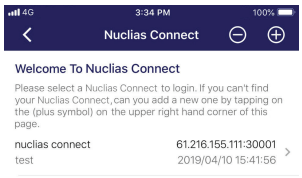
# Software Installation Nuclias Connect App

| 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.



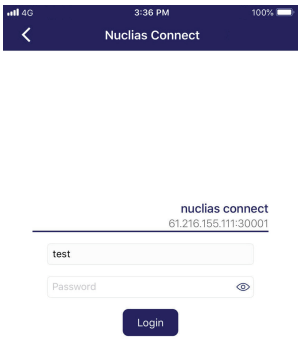

After a successful login, the pairing will be added to the listing and will be available for future login selection.



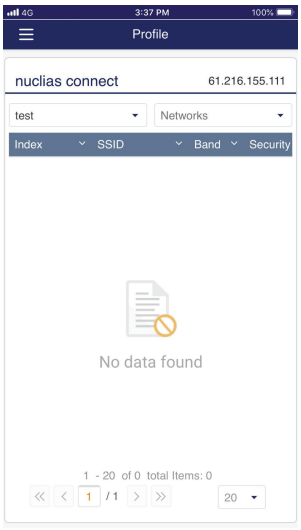

Tap on a Nuclias Connect server from the list.

# 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 to the Nuclias Connect server. Through the use of the App, profiles can be downloaded to the local device, after which, it can be pushed to supported DAPs.

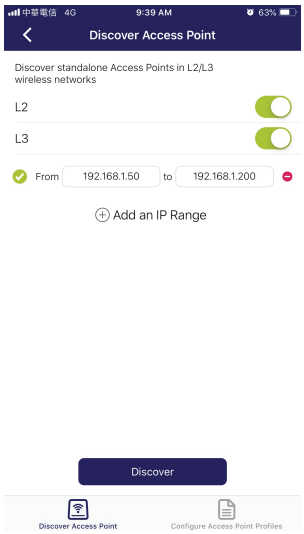
# Software Installation Nuclias Connect App

***Standalone Access Point***

**Discover DAPs**

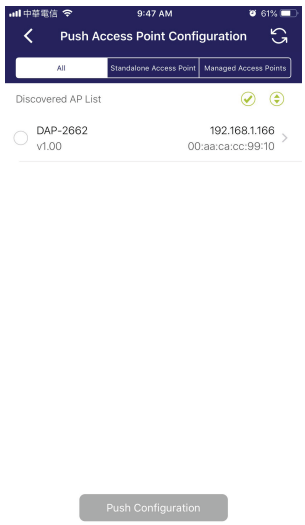
The Discover DAP function allows you to discover any DAP devices in a L2/L3 wireless network.

From this page, you can discover standalone DAPs 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.



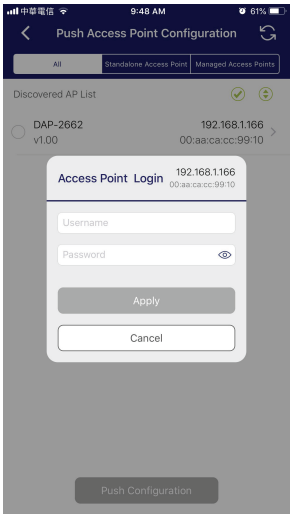

Once the range is defined, tap **Next** to initiate the discovery process.
Alternatively, tap Configure Access Point Profiles from the bottom of the page to add or delete any local profiles. See Configure Access Point Profiles.

After the scanning the network range, the Step 3 page will list any detected access points.
Tap the radio button next to the DAP to select it. The selected local provision file will be pushed to the selected DAP.
Tap **Push Provision File** to continue.



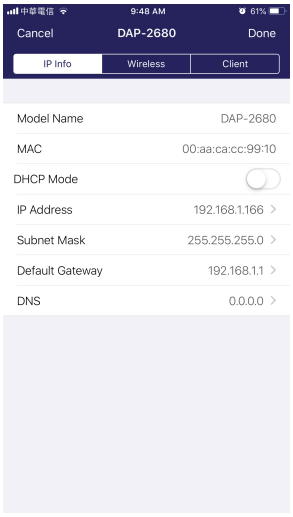
# Software Installation Nuclias Connect App

The DAP 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 DAP. Tap **Apply** to continue.




Once a successful login is established, the DAP interface menus will appear. The IP information, Wireless, and Client menus will be listed as follows.

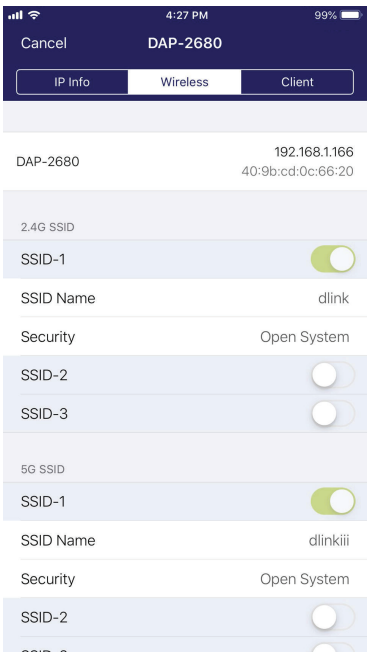
| Parameter | Description |
|---|---|
| **Cancel** | Tap to discard any changes and continue the process. |
| **Model Name** | Displays the model name for the listed DAP device. |
| **MAC** | Displays the MAC address of the listed DAP device. |
| **DHCP Mode** | Tap to enable or disable the DHCP mode function. When enabled, the DAP 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. |

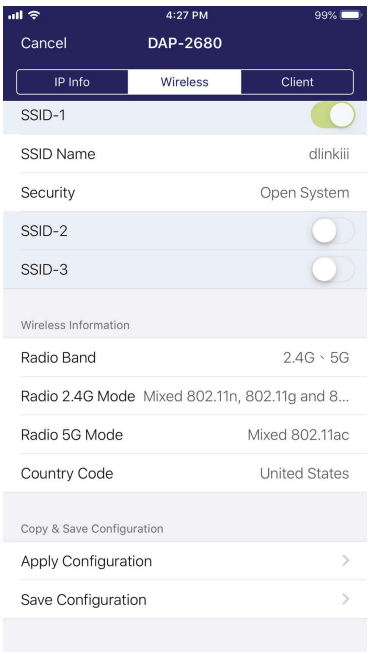


# Software Installation Nuclias Connect App

The Wireless settings menu is listed in the following figure.

| Parameter | Description |
|---|---|
| **Cancel** | Tap to discard any changes and continue the process. |
| **DAP** | 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, 80211g 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, 80211a; 802.11a Only; 802.11n; Mixed 802.11ac. |
| **Country Code** | Displays the assigned country designation for the DAP. |
| **Copy & Save Configuration** | |
| **Apply Configuration** | Tap to select an alternate discovered DAP device to push the current configuration. |
| **Save Configuration** | Tap to name and archive the current configuration profile. |



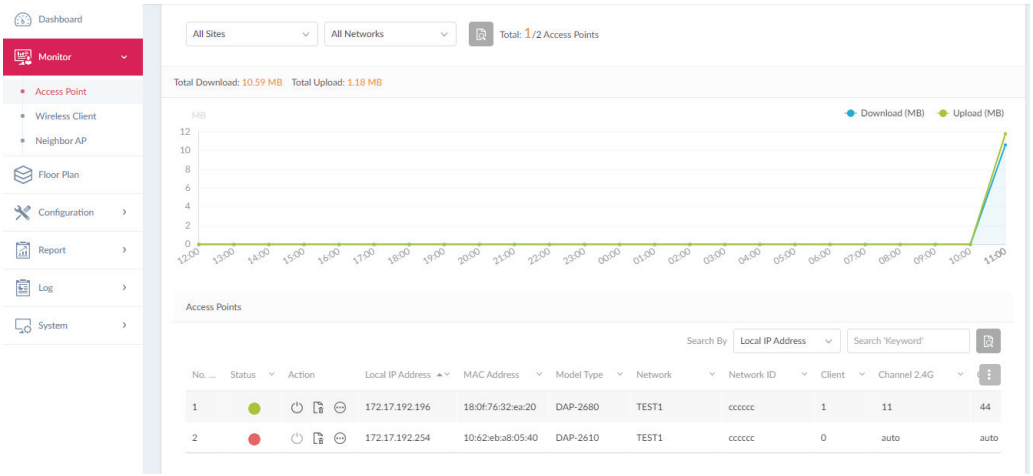



Software Installation Nuclias Connect App

## Verify Managed Access Points

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

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

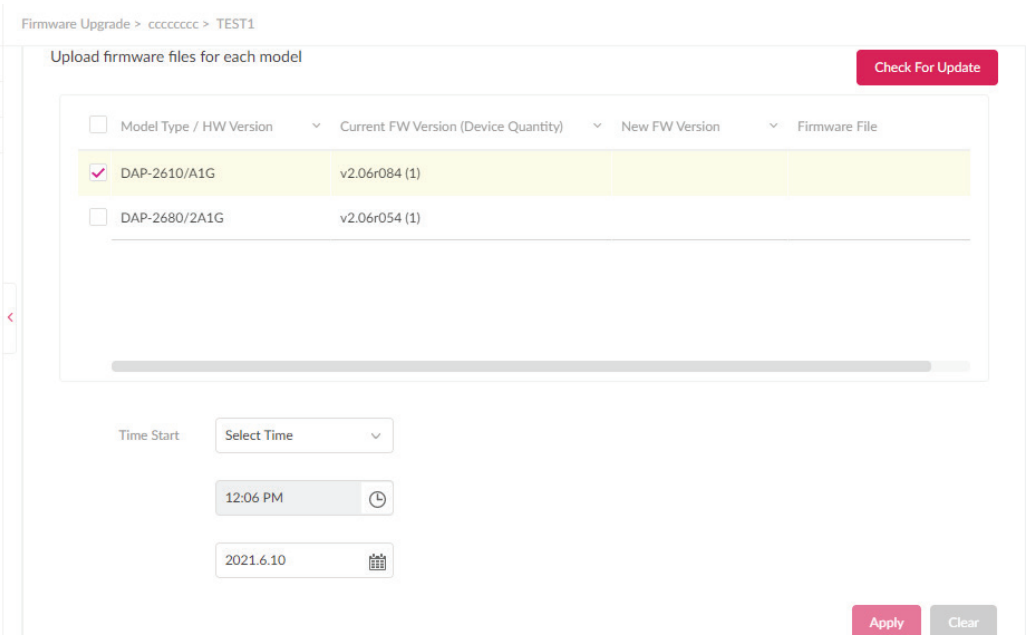



## Upload New or Updated Configuration

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

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

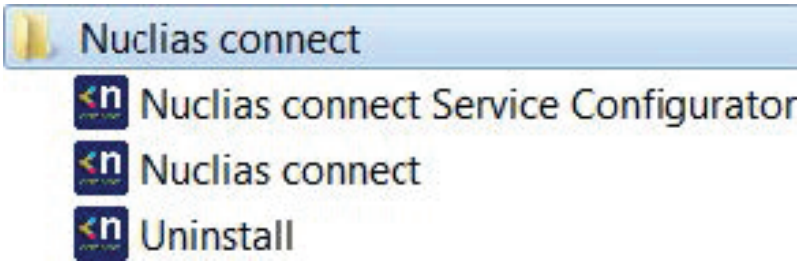
From the ensuing screen, select the firmware to upload by clicking the **Change** button. From the Time Start field, select Immediate and click **Apply** to immediately upgrade the firmware to the selected access points on the network. Alternatively, click the drop-down menu and use the Select Time option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



# Nuclias Connect Configuration

In this section, the Nuclias Connect client application.

After the software installation was complete the following applications will be available.



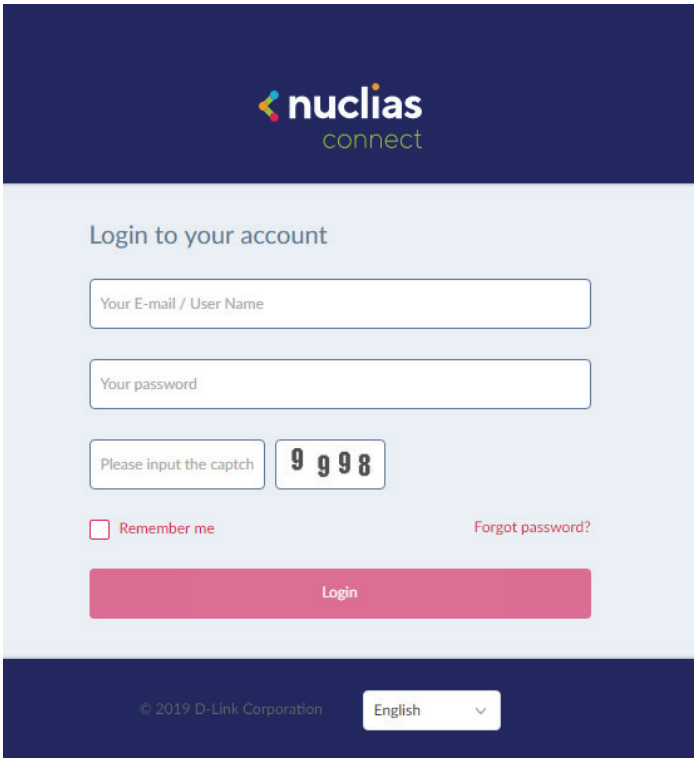

Click on the **Nuclias Connect** link to open the client application.

Nuclias Connect uses a secure HTTPS connection to connect to the Nuclias Connect Controller By default, this 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 into the web browser. Open the web browser on the remote computer (Internet Explorer or Google Chrome are recommend) 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 .

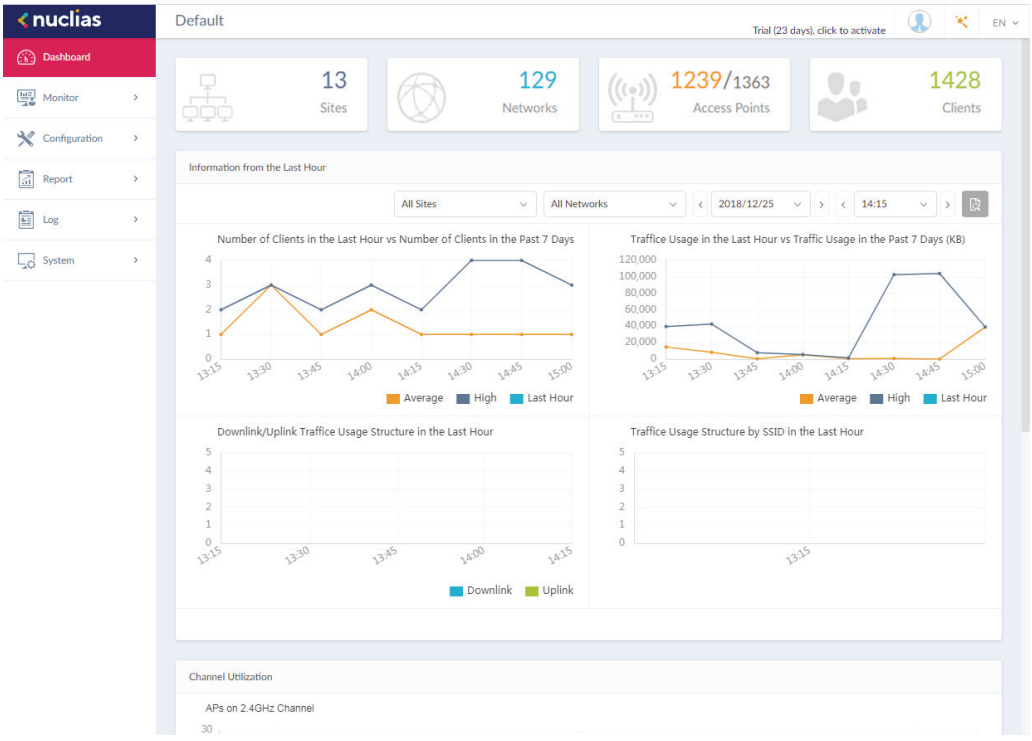
**NOTE:** By default, the user name and password are admin. Supported languages include: English (default), Traditional Chinese, Simplified Chinese, Korean, Japanese, French, Spanish, German, Russian, Italian, and Turkish.



# Nuclias Connect Dashboard

After successfully logging into the server, the **Dashboard** page will appear. A summary of information of all connected access points and wireless clients is available on this page.

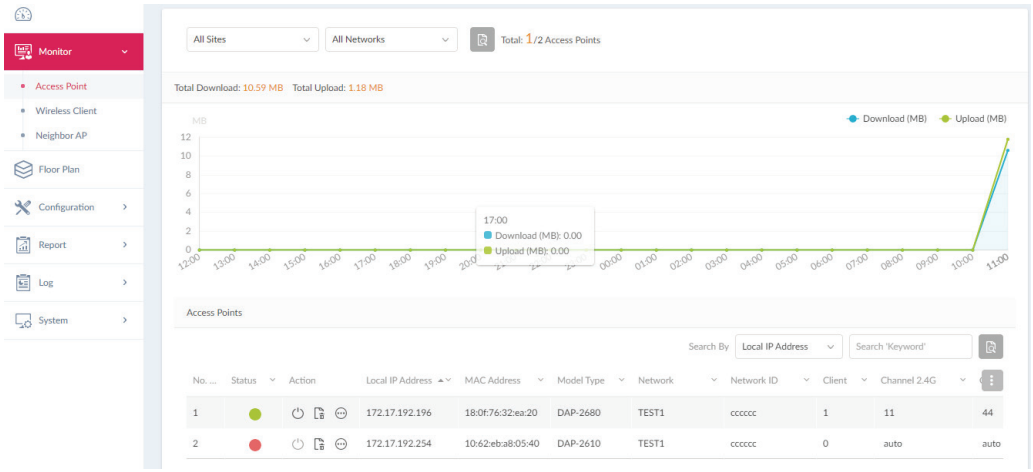
| Block | Description |
|---|---|
| **Sites** | Displays the number of created profiles, also called sites. |
| **Networks** | Displays the total number of created networks. |
| **Access Points** | Displays the total number of available and online access points. |
| **Clients** | Displays the total number of wireless clients connected to the network. |
| **Information from the Last Hour** | Displays log information for the number of clients, traffic usage, downlink/uplink traffic usage, and traffic usage by SSID. |
| **Channel Utilization** | Displays the utilization rate for both 2.4 and 5 GHz bandwidth. |
| **Last Events** | Displays a shortened log version of the latest events across all or selected sites. |



# Nuclias Connect Monitor Access Point

By clicking on **Monitor** in the left panel, the Usage and Total Access Points frames will appear. On this frame, you can view a report of all or a selected number wireless clients and networks managed by the application.

Three reports can be generated using **Site**, **Network**, or **Local IP** address.




The following figure represents a typical report. This report can be refined by selecting the a specific Site from the first drop-down menu, and then selecting the network in the second drop-down menu.

| Block | Description |
|---|---|
| **Usage** | Displays a report listing the RX (kB) / TX (kB) usage for the specified site and network. |
| **Total X Access Points** | Displays a report listing all detected wireless clients. |

In the **Search By** drop-down field, select an attribute (**Local IP Address**, **Local IPv6 Address**, **NAT IP Address**, **MAC Address**, **Model Type**, or **FW Version**) to specify the search function or enter a keyword related to the target device in the Search field.

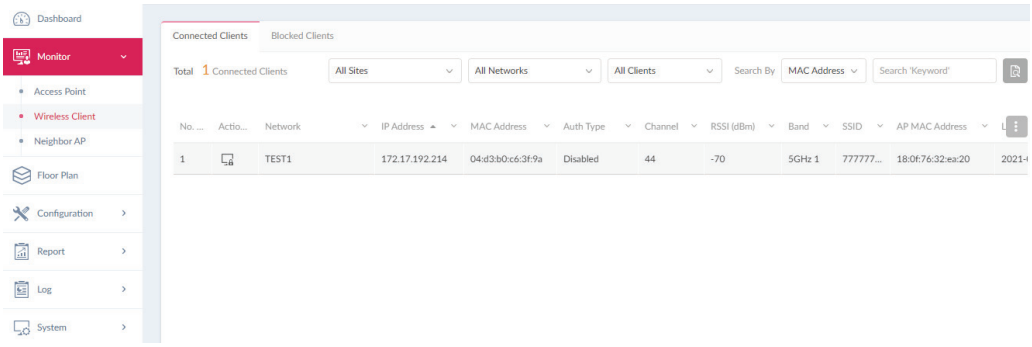
Click to start the process. Any relevant devices meeting the search criteria will be listed in the frame.

# Nuclias Connect Monitor Wireless Client Connected Clients

After clicking on **Monitor** in the left panel, the Connected Clients frame displays. On this frame, you can view a report of all connected clients managed by the application.

Three association reports can be generated by **Site**, **Network**, and **Clients**.

The following figure represents a typical report. This report can be refined by selecting a specific Site from the first drop-down menu, and then selecting a network and client.




This page shows a report that was generated by connected wireless clients. This report can be refined by selecting the date and time **From** and **To**, and then selecting the **Type**, either **By MAC Address** or **By Alias**, and also additionally entering **Key Words** in the text box provided.

In this report a list of wireless client connections, 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.

In the Search field, enter a keyword related to the target device and click to start the process. Any relevant devices meeting the search criteria will be listed in the frame.

# Nuclias Connect Monitor Wireless Client Blocked Clients

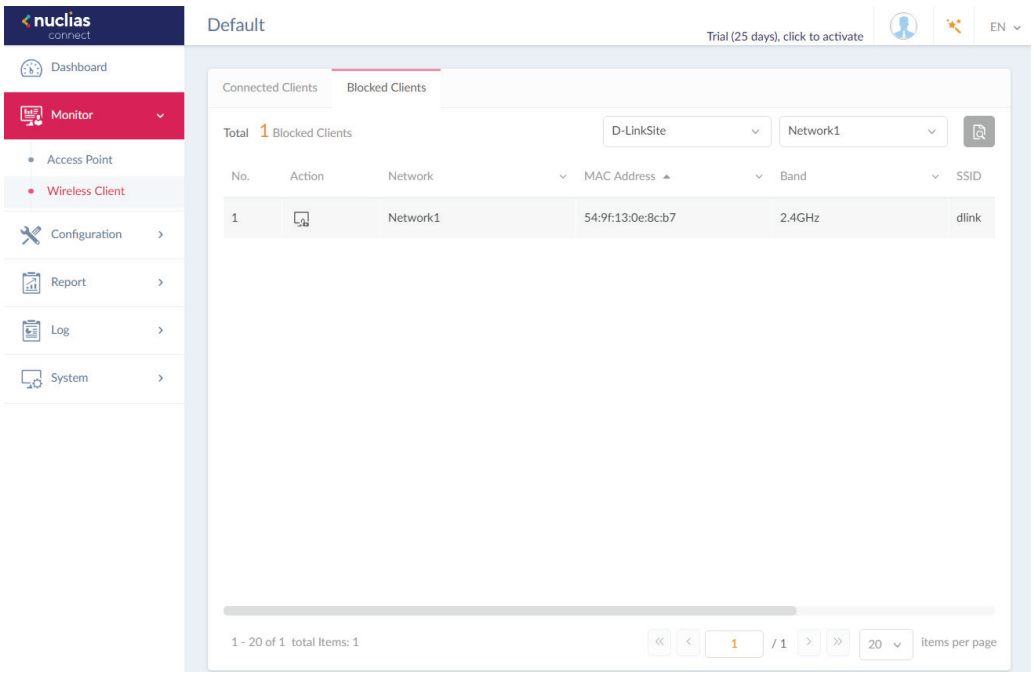
After clicking on **Monitor** in the left panel, the Connected Clients frame will appear. Click on the **Blocked Clients** tab. On this frame, you can view a report of all blocked clients detected by the application. This report can be generated through **Site** and **Network** criteria.

The following figure represents a typical report. This report can be refined by selecting a specific Site from the first drop-down menu, and also then selecting the network.

In this report a list of blocked wireless client connections are displayed.

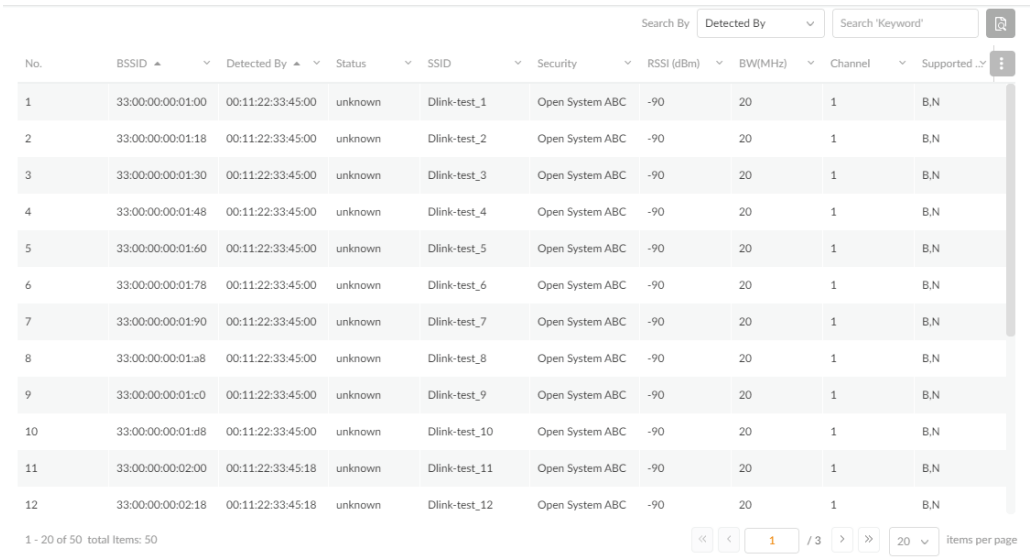
In the Search field, click the drop-down menu and select a Site then select a Network. Click to start the process. Any relevant devices meeting the search criteria will be listed in the frame.

The report lists the following information: **No.**, **Action**, **Network**, **MAC Address**, **Band**, **SSID**, and **Auth. Type**.



# Nuclias Connect Monitor Neighbor AP

After clicking on Neighbor AP in the left panel, the neighbor AP list displays. To enable this function you have to go to Configuration>Profile Settings>Site>Network>Wireless Resource>Neighbor AP Detection and click enabled button first.




| 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 |

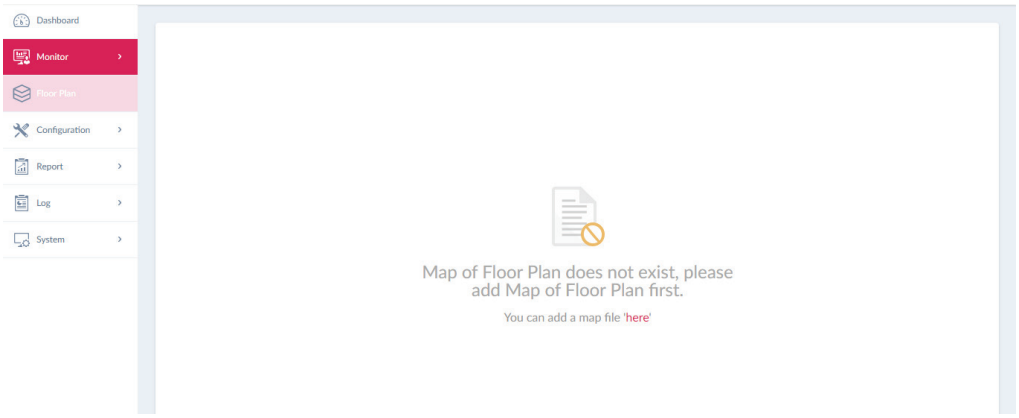
1 - 20 of 50 total Items: 50 1 / 3 20 items per page

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.

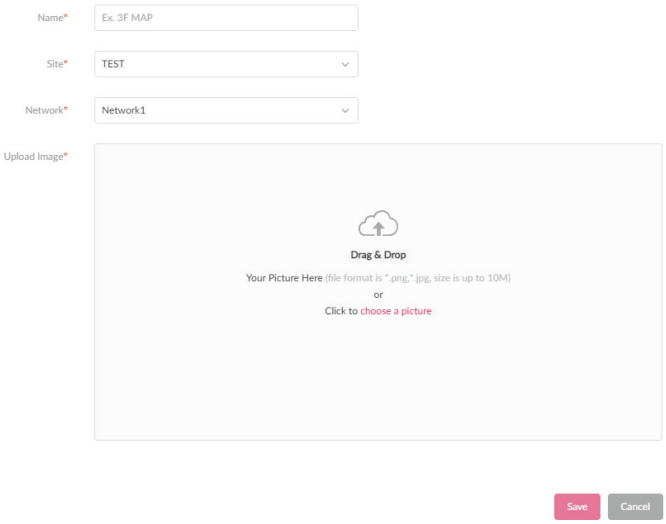
# Nuclias Connect Floor Plan

Floor plan is a drawing to scale, showing a view from above, of the relationships between rooms, spaces, traffic patterns, and other physical features at one level of a structure.

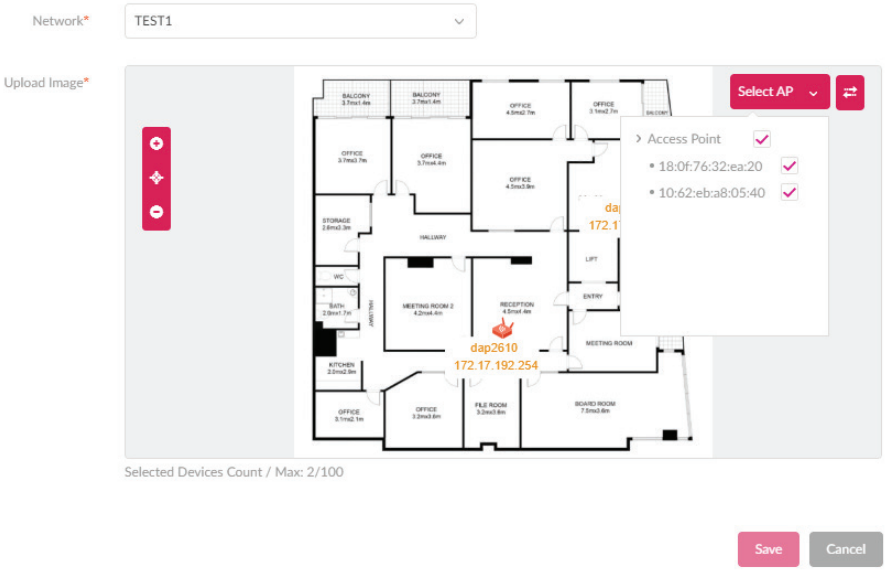
Click "here" to add a new floor image, enter the name and select Site and Network,




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




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



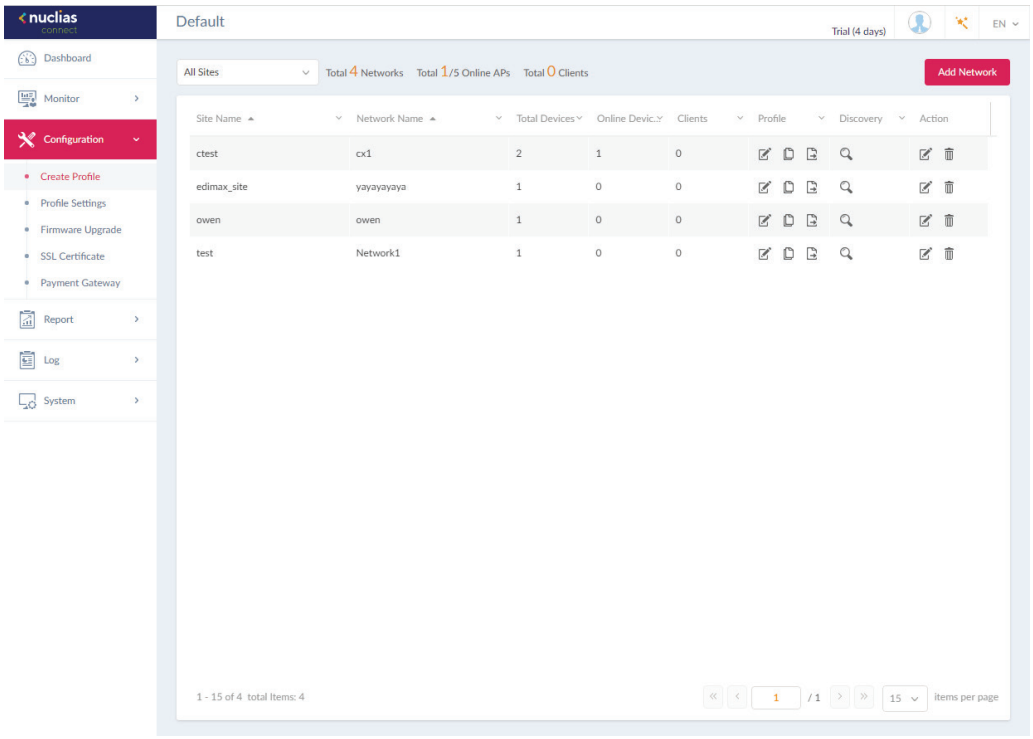
# Nuclias Connect Configuration Create Profile

The Create Profile function allows for the addition of new sites and networks.

By clicking on **Configuration > Create Profile** the Default frame displays listing all available sites and networks, see the following screen for further information.

Click **Add Network** to create a new site and/or network.

| Block | Description |
|---|---|
| **Edit Profile** | Opens site details page, editing is available for selected site's security, access control, and user authentication settings. |
| **Copy Profile to this Network** | Copies existing profile to a designated site and network. |
| **Export Network Profile** | Exports 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 the results (Configurable and Managed devices) of the search. |
| **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** | Deletes the selected network configuration. |



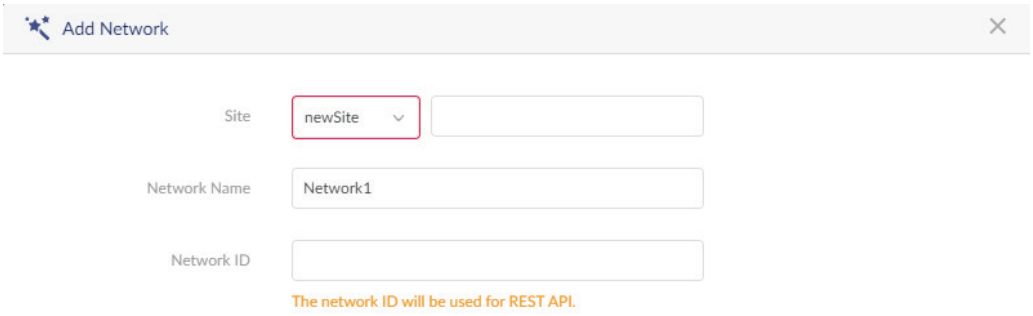
# Nuclias Connect Configuration Create Profile Add Network

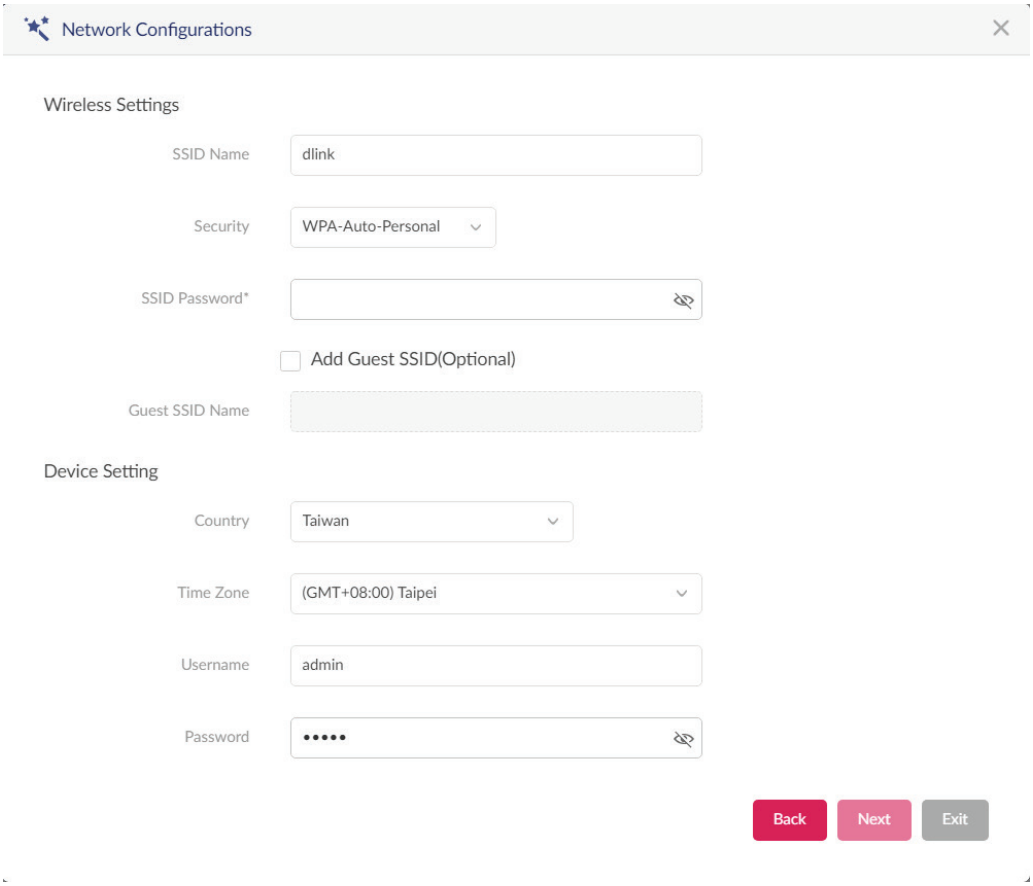
From the Create Profile link, click on **Add Network** to create a new network.

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

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

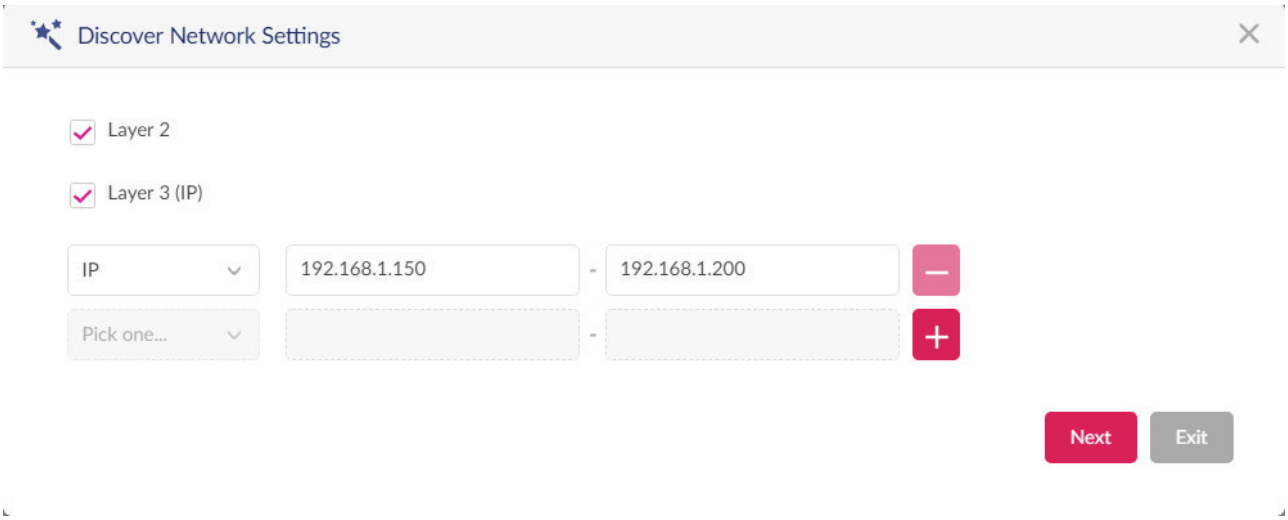
The Network Configurations page will appear. Enter the wireless and device settings to define the network configuration. Click **Next** to continue. To return to the previous page, click **Back** or click **Exit** to discontinue the configuration process. The Network ID is optional item and it will be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



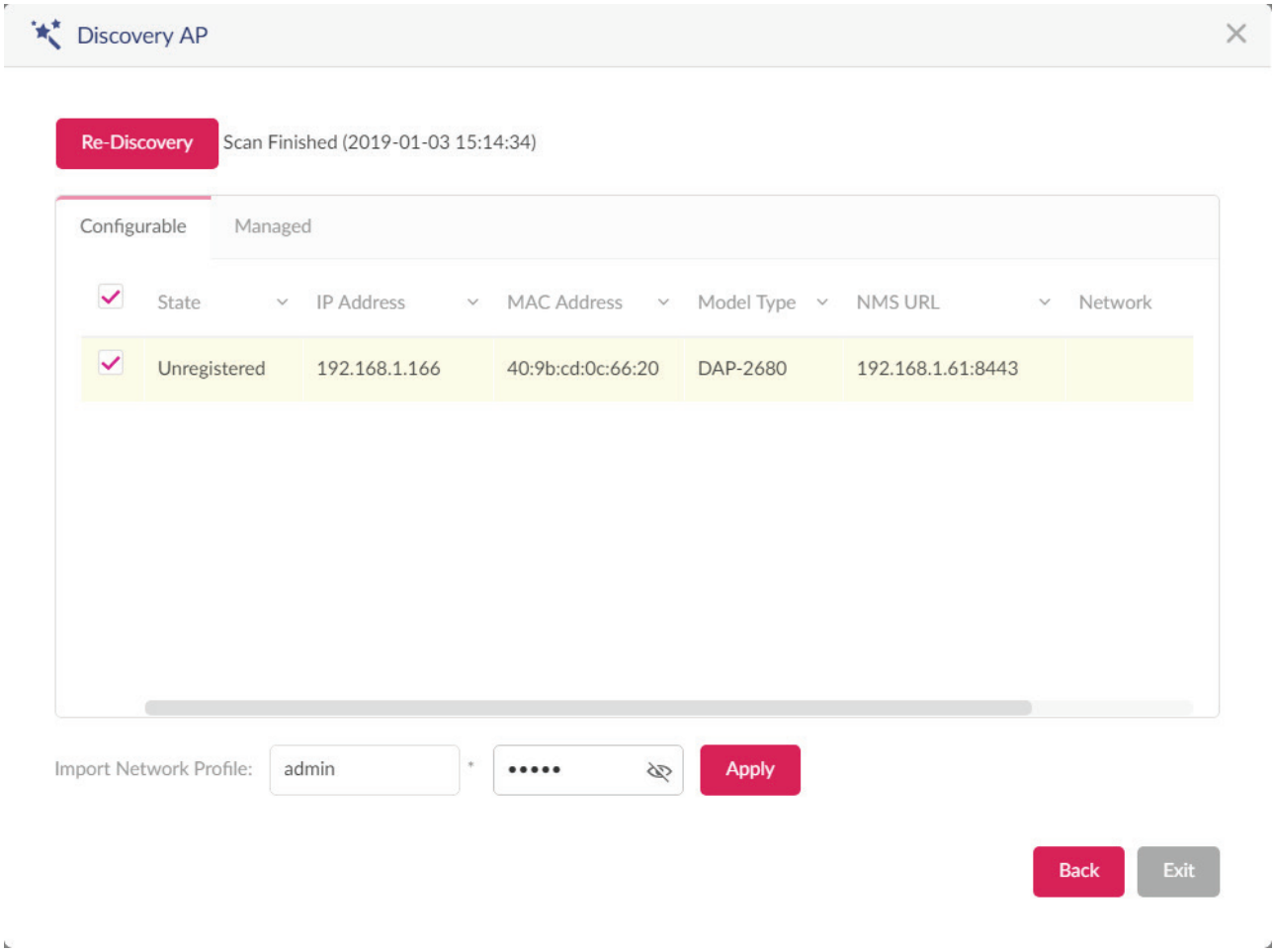



# Nuclias Connect Configuration Create Profile Add Network

The Discover Network Settings page wil appear. Select the data link layer (layer 2 or layer 3) to define the type of network to run Discover Network 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.




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



# Nuclias Connect Configuration Profile Settings

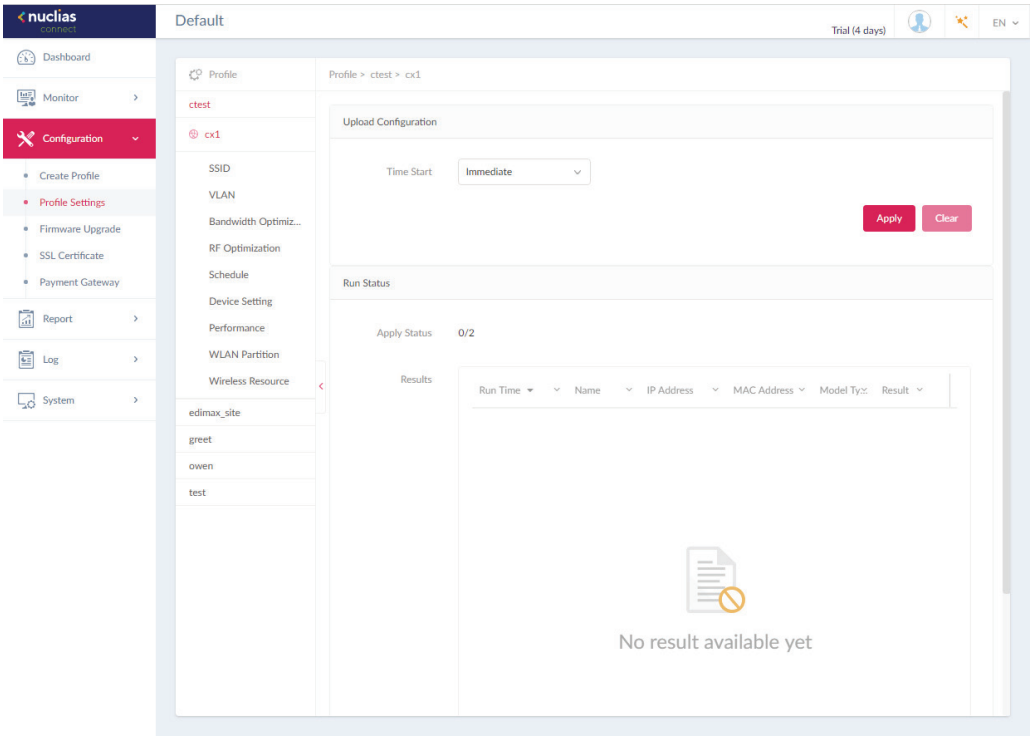
The Profile Settings function allows for the management of existing networks. Navigate to **Configuration > Profile Settings** to view existing sites. Select a site followed by an available network to view all settings that are available for editing: **SSID**, **VLAN**, **Bandwidth Optimization**, **RF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

Once a network is selected the following screen will appear. The upload configuration function is available on the **Profile Settings > [Site] > [Network]** page.

For any updates to site or network configuration to take effect, the configuration must be uploaded to the access point. Under the **Upload Configuration** frame, click the **Time Start** drop-down menu and select the time (Immediate or Select Time) to update the configuration to the access point.

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 frame, the status of the upload configuration function will be reported. Once an update is complete, the results will be displayed in the **Results** frame.



# Nuclias Connect Configuration Profile Settings SSID

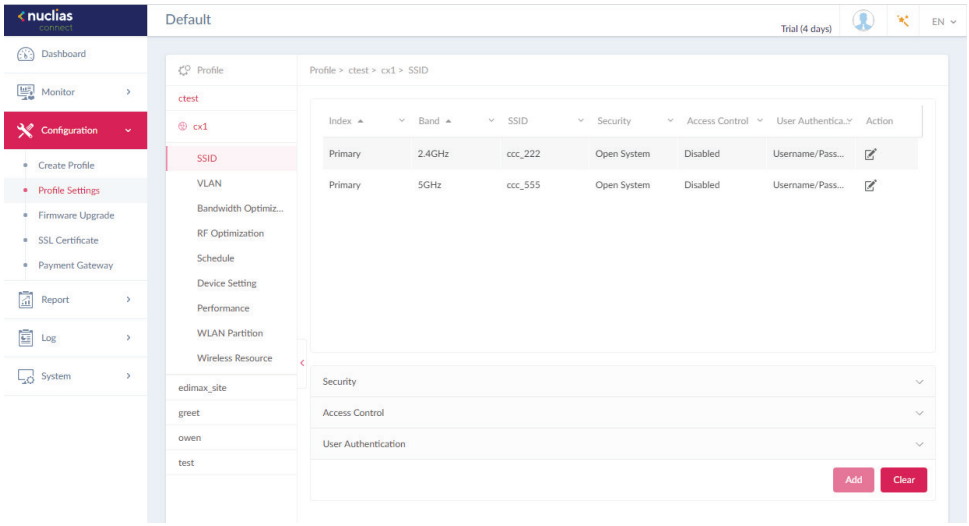
The SSID page displays the configurable parameters of a network's wireless settings. Navigate to **Configuration > Profile Settings > [Site] > [Network] > SSID** to view existing settings.

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

| Block | 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 the Nuclias Connect. For further information, see the 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 the 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.(Only APs support this function are activated.) |
| **Encryption** | Click the drop-down menu to enable or disable WEP Open System encryption. The function is only available when **Security** is set as **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. |
| **Encryption Type** | Click the drop-down menu to select the encryption type: Auto, AES, or TKIP. |
| **Group Key Update Interval** | Enter the WPA group key update interval value. |
| **Passphrase** | Enter the secret pass phrase used. The function is only available when **Security** is **WPA-Personal**, **WPA2-Personal** or **WPA-Auto-Personal**. |
| **RADIUS Server** | Enter the RADIUS server's IP address. The function is only available when **Security** is **WPA-Enterprise**, **WPA2-Enterprise** or **WPA-Auto-Enterprise**. |
| **Port** | Enter the RADIUS server's port number. The function is only available when **Security** is **WPA-Enterprise**, **WPA2-Enterprise** or **WPA-Auto-Enterprise**. |

Once the settings are updated, the configuration must be uploaded to the access points. See "Profile Settings" on page 50 for further information.

# Nuclias Connect Configuration Profile Settings SSID




| Block | Description |
|---|---|
| **RADIUS Secret** | Enter the RADIUS server's secret pass phrase. The function is only available when **Security** is **WPA-Enterprise**, **WPA2-Enterprise** or **WPA-Auto-Enterprise**. |

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 the MAC address file, located on the local computer, that will be uploaded. Click **Upload** to update the MAC address list. Click **Download** to download the current MAC 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. Interval |
| **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 whitelisted and click **Add** to add the address to the white list table. This function is only available when **Authentication Type** is **Username/Password**. |

| Block | Description |
|---|---|
| **Upload Whitelist File** | Click **Browser...** to select the white list file, located on the local computer, that will be uploaded. Click **Upload** to update the white list. Click **Download** to download the current white list. The function is only available when **Authentication Type** is **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**. |
| **Password** | Enter the password and click **Add**. Click **Clear** to clear the entered fields. This function is only available when **Authentication Type** is **Username/Password**. |
| **RADIUS Server** | Enter the RADIUS server's IP address. This function is only available when **Authentication Type** is **Remote RADIUS** or **MAC Address**. |
| **RADIUS Port** | Enter the RADIUS server's port number. This function is only available when **Authentication Type** is **Remote RADIUS** or **MAC Address**. |
| **RADIUS Secret** | Enter the RADIUS server's secret. This function is only available when **Authentication Type** is **Remote RADIUS** or **MAC Address**. |
| **Remote RADIUS Type** | Enter the RADIUS server's type. This function is only available when **Authentication Type** is **Remote RADIUS** or **MAC Address**. |
| **Server** | Enter the LDAP server's IP address. This function is only available when **Authentication Type** is **LDAP**. |
| **Port** | Enter the LDAP server's port number. This function is only available when **Authentication Type** is **LDAP**. |
| **Authentication Mode** | Click on the drop-down menu to select the authentication mode. This function is only available when **Authentication Type** is **LDAP**. |
| **Username** | Enter the administrator's username that will be able to access and search the LDAP database. This function is only available when **Authentication Type** is **LDAP**. |
| **Password** | Enter the administrator's password that will be able to access and search the LDAP database. This function is only available when **Authentication Type** is **LDAP**. |
| **Base DN** | Enter the base domain name of the LDAP database. This function is only available when **Authentication Type** is **LDAP**. |
| **Account Attribute** | Enter attribute for the account. This function is only available when **Authentication Type** is **LDAP**. |
| **Identity** | Enter the name of the administrator. This function is only available when **Authentication Type** is **LDAP**. |
| **Server** | Enter the POP3 server's IP address. This function is only available when **Authentication Type** is **POP3**. |
| **Port** | Enter the POP3 server's port number. This function is only available when **Authentication Type** is **POP3**. |

| Block | Description |
|---|---|
| **Connection Type** | Click the drop-down menu to select the connection type. This function is only available when **Authentication Type** is **POP3**. |
| **Passcode List** | Display the configured front desk user accounts that have been assigned to this network and have already 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 **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. |
| **Choose Template** | Click the drop-down menu to select the used login style. This function is only not available when **Authentication Type** is **Web Redirection Only**.<br>• Click **Preview** to preview the selected style.<br>• Click **Upload Login File** to upload a new style.<br>• Click to delete the selected style.<br>• 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.

# Nuclias Connect Configuration Profile Settings VLAN

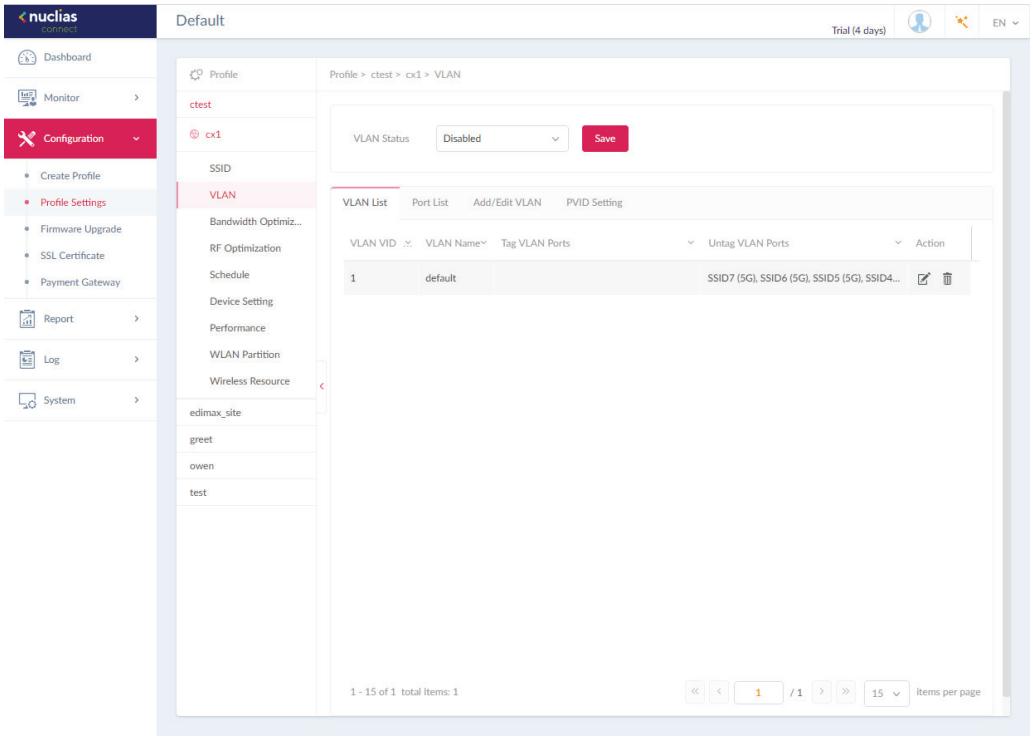
The VLAN page will show the configurable settings of a network's virtual LAN subnetwork settings. Navigate to **Configuration > Profile Settings > [Site] > [Network] > VLAN** to view existing settings.

| 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 will appear. The list indicates the available 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 will 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 will show the connected virtual LAN segment.

In the **Add/Edit VLAN** tab, we can create a new VLAN and assign untagged ports in that VLAN. After clicking the Modify icon in the VLAN List tab, you will be re-directed to this 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.

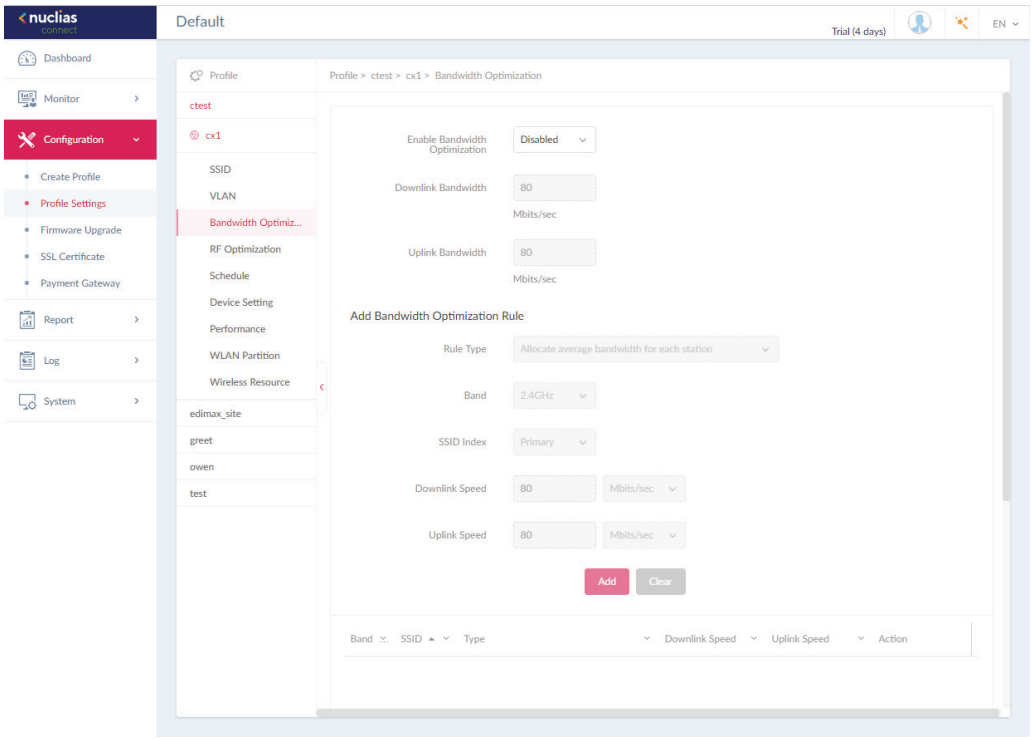
Once the settings are updated, the configuration must be uploaded to the access points. See "Profile Settings" on page 50 for further information.

# Nuclias Connect Configuration Profile Settings 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.<br>• Allocate an average BW for each station: Optimize bandwidth by averaging the allocated bandwidth for each client.<br>• Allocate a maximum BW for each station: Specify the maximum bandwidth for each connected client, while reserving available bandwidth for additional clients.<br>• 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.<br>• 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.



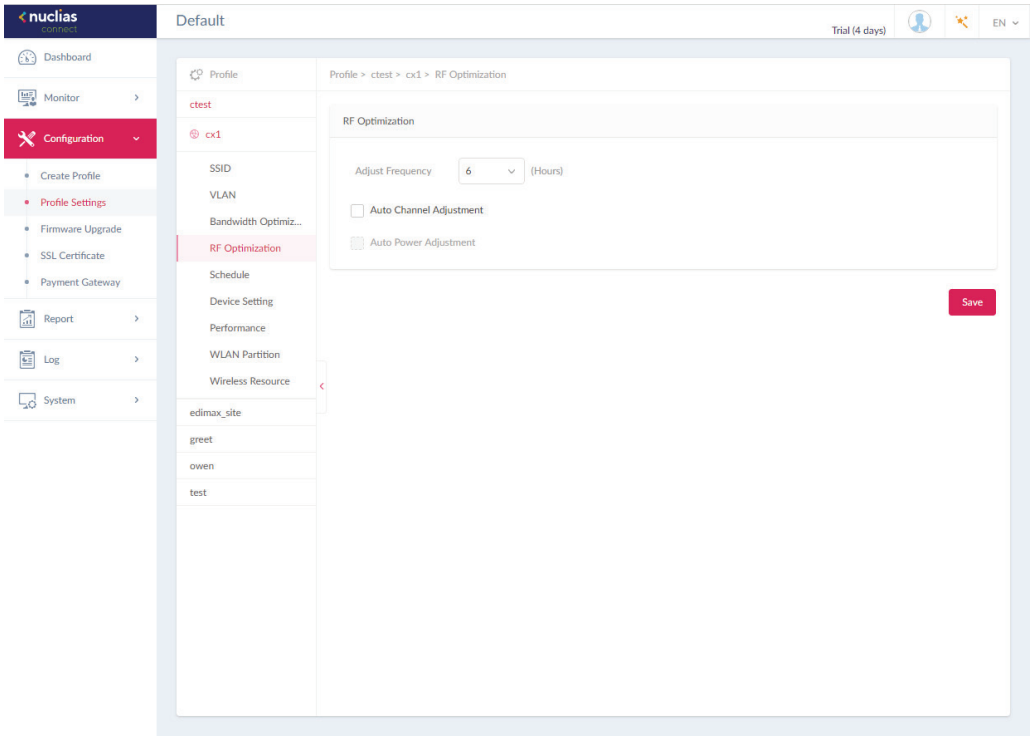

Once the settings are updated, the configuration must be uploaded to the access points. See "Profile Settings" on page 50 for further information.

# Nuclias Connect Configuration Profile Settings 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 50 for further information.

# Nuclias Connect Configuration Profile Settings Schedule

The Schedule page displays the wireless schedule settings describing how to specify a schedule to maintain an SSD active within a specified time. Navigate to **Configuration > Profile Settings > [Site] > [Network] > Schedule** to view existing settings.

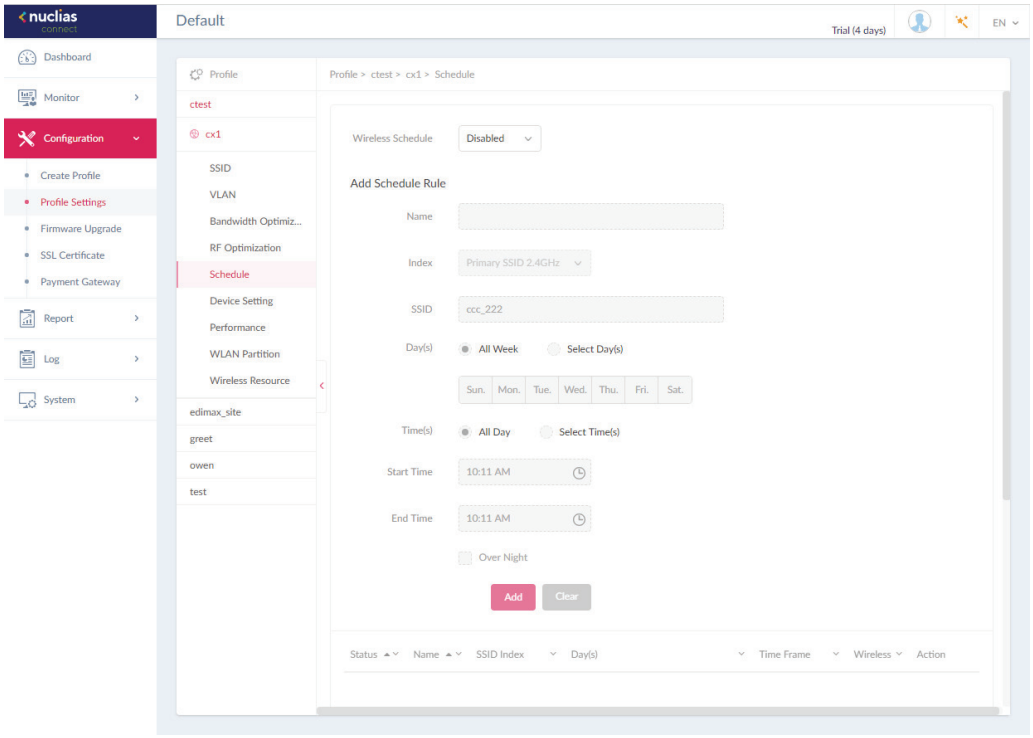
| Parameter | Description |
|---|---|
| **Wireless Schedule** | Click the drop-down menu to enable or disable the wireless schedule function. |
| **Name** | Enter the name of the schedule rule. |
| **Index** | Click the drop-down menu to select SSID on which the schedule setting is applied. |
| **SSID** | Display the SSID name. |
| **Day(s)** | Click the radio button to select the active days for the schedule.<br>• All Week: Enable the rule for the whole week.<br>• Select Day(s): Specifies particular day(s) to activate the rule. |
| **Time(s)** | Click the radio button to select the active times for the schedule.<br>• All Day: Enable the rule for the whole day.<br>• Select Time(s): Specifies a starting and ending time for the rule. |
| **Start Time** | Enter the hours and minutes of the day. This function is only available when **Time(s)** is **Select Time(s)**. |
| **End Time** | Enter the hours and minutes of the day. This function is only available when **Time(s)** is **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 50 for further information.



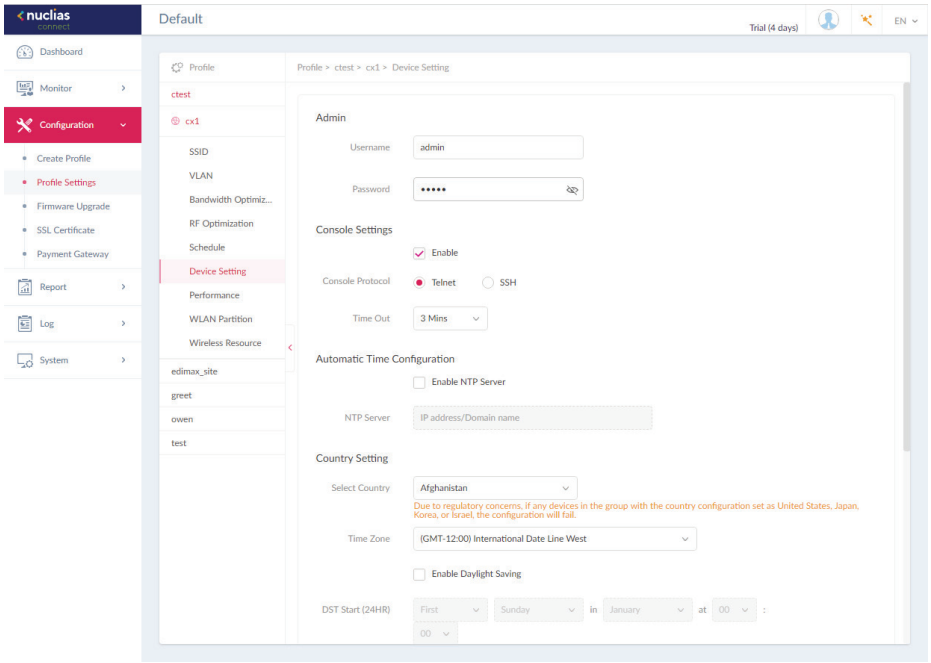
# Nuclias Connect Configuration Profile Settings Device Setting

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 on this page 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 50 for further information.

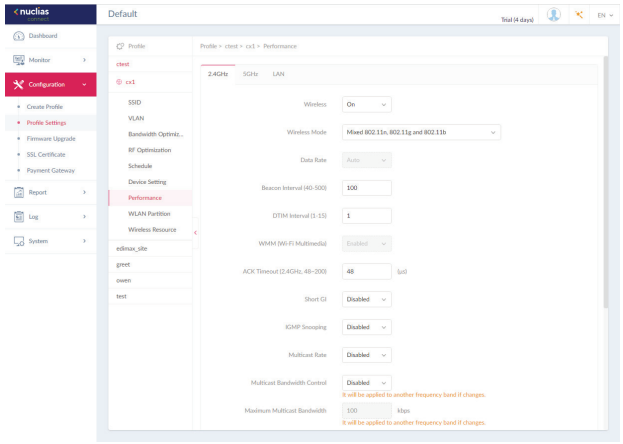


# Nuclias Connect Configuration Profile Settings Performance 2.4GHz/5GHz

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] > Device Setting** 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 **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 intterval 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 DHCPOFFER 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 50 for further information.

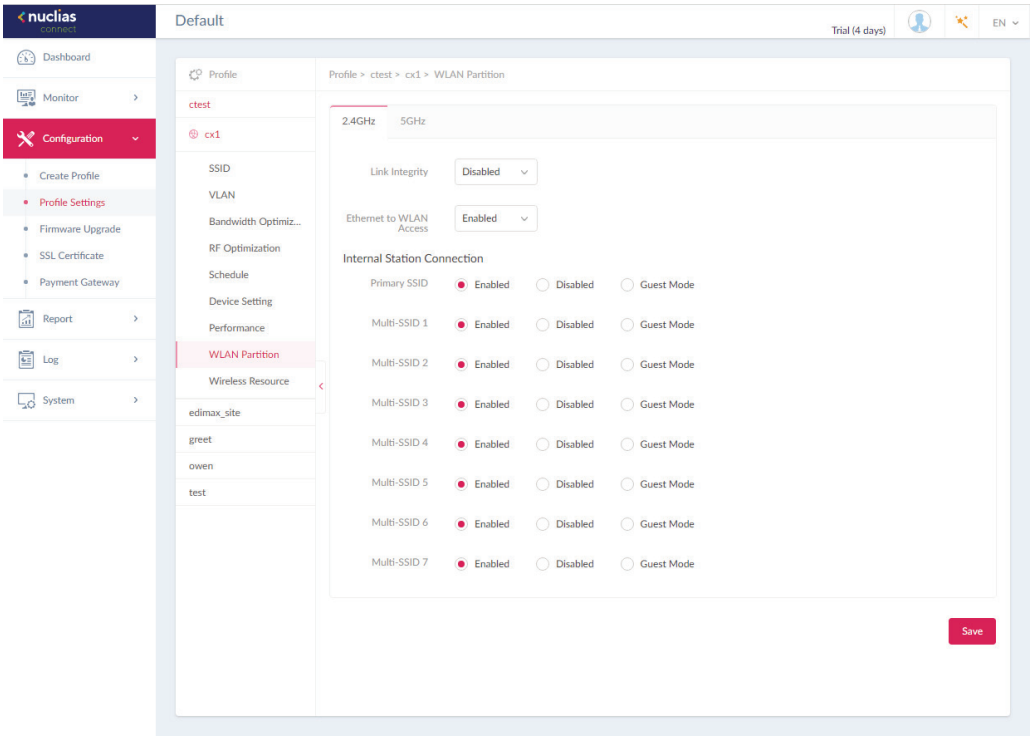
# Nuclias Connect Configuration Profile Settings WLAN Partition

## 2.4GHz/5GHz

The WLAN Partition page displays the wireless partitioning settings that allows 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.

| Parameter | Description |
|---|---|
| **Link Integrity** | Click the drop-down menu to enable or disable the wireless link integrity function. |
| **Ethernet to WLAN Access** | Click the drop-down menu to enable or disable Ethernet to WLAN access function. |
| **Internal Station Connection** | Click the radio button to enable or disable the membership of the SSID to the WLAN partition. Select **Guest Mode** to allow this SSID to have access to this WLAN partition as a guest. |

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 50 for further information.

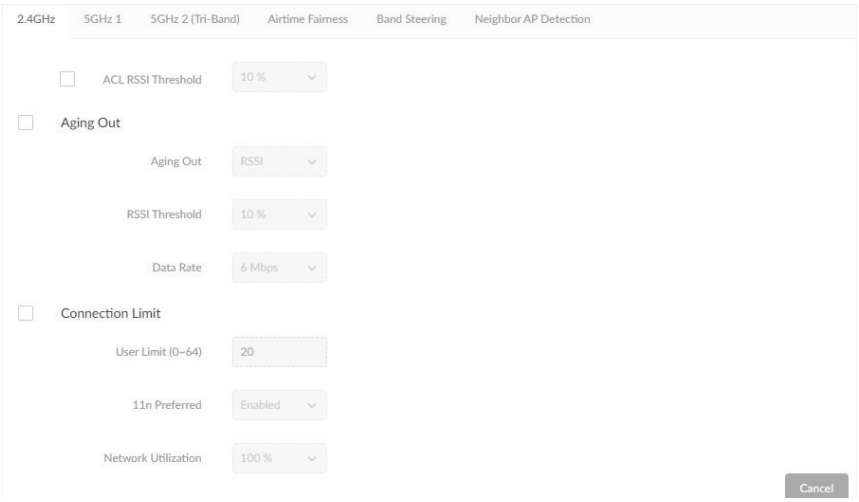
# Nuclias Connect Configuration Profile Settings Wireless Resource

## 2.4GHz/5GHz 1/5GHz 2(Tri-Band)

The Wireless Resource function in Nuclias Connect helps provides 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** | Use the drop-down menu to select criteria to disconnect a wireless clients. Available options are RSSI and Data Rate. |
| **Aging Out** | Click the drop-down menu to select the aging out mode |
| **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 RRSI 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 when the number of users exceeds 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.




Once the settings are updated, the configuration must be uploaded to the access points. See "Profile Settings" on page 50 for further information.

# Nuclias Connect Configuration Profile Settings Wireless Resource

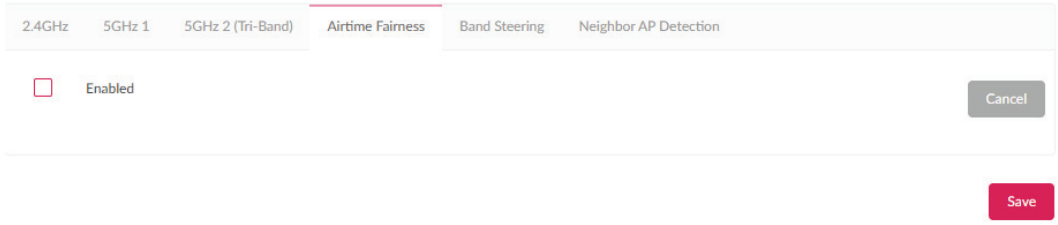
## Airtime Fairness

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 can be slow from either long physical distances, 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 setting.

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

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




Once the settings are updated, the configuration must be uploaded to the related access points. See "Profile Settings" on page 50 for further information.

# Nuclias Connect Configuration Profile Settings Wireless Resource

## Band Steering

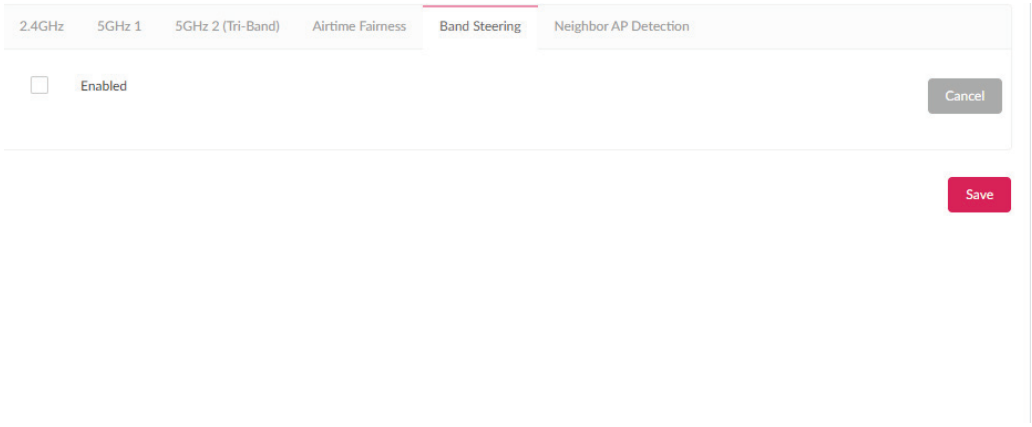
Band Steering allows dual-band-capable clients to connect to the less crowded 5GHz network, and leave the 2.4GHz network available for those clients who support 2.4GHz only

.

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.

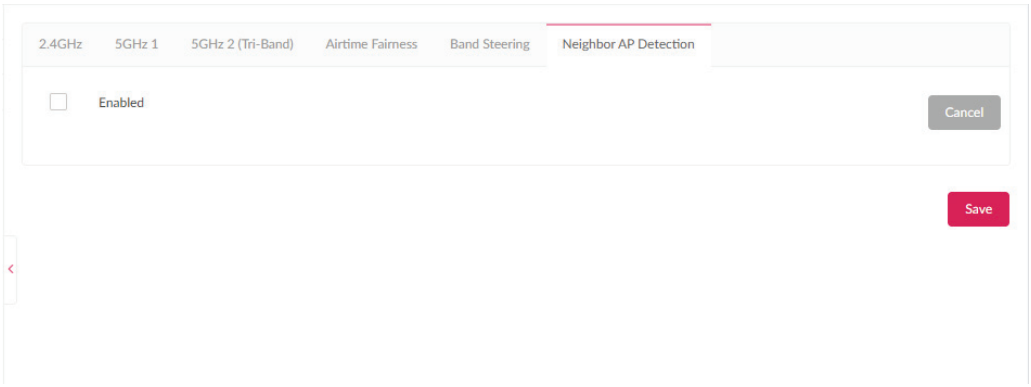


# Nuclias Connect Configuration Profile Settings Wireless Resource

## 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.



# Nuclias Connect Configuration Firmware Upgrade

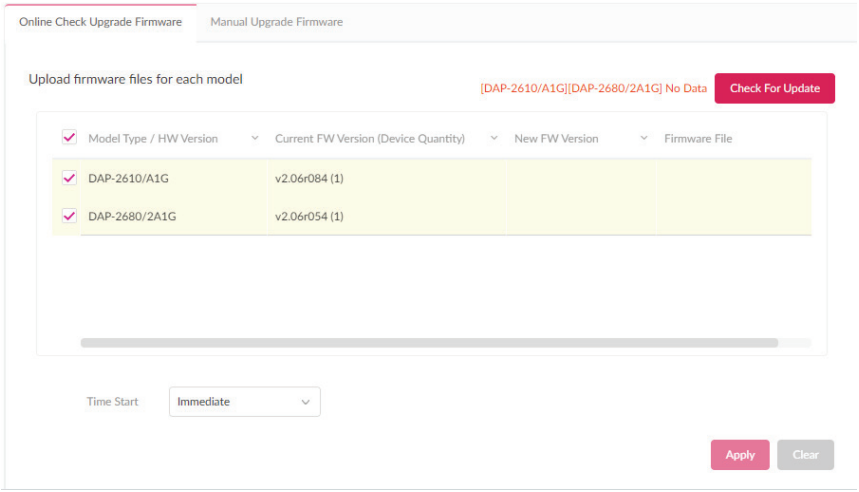
The Firmware Upgrade function allows users to perform a firmware upgrade. For on-line update, please confirm your controller is on-line first. For manual upgrade. please go to your local D-Link website to see if there is a newer version firmware available.

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

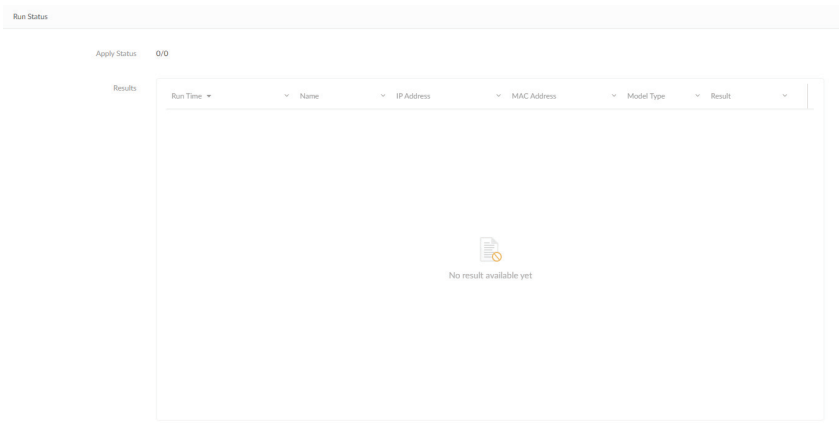
| Block | Description |
|---|---|
| **Change(Manual Upgrade Firmware)** | Click to select a firmware file to upload. Files are model specific. |
| **Check For Update(Online Check Upgrade Firmware)** | Click to check if there has new official firmware in on-line server. |
| **Time Start** | Click the drop-down menu to select a specific time or to 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 bottom of this page. The results can be sorted by Run Time, Name, IP Address, MAC Address, Model Type and Result.



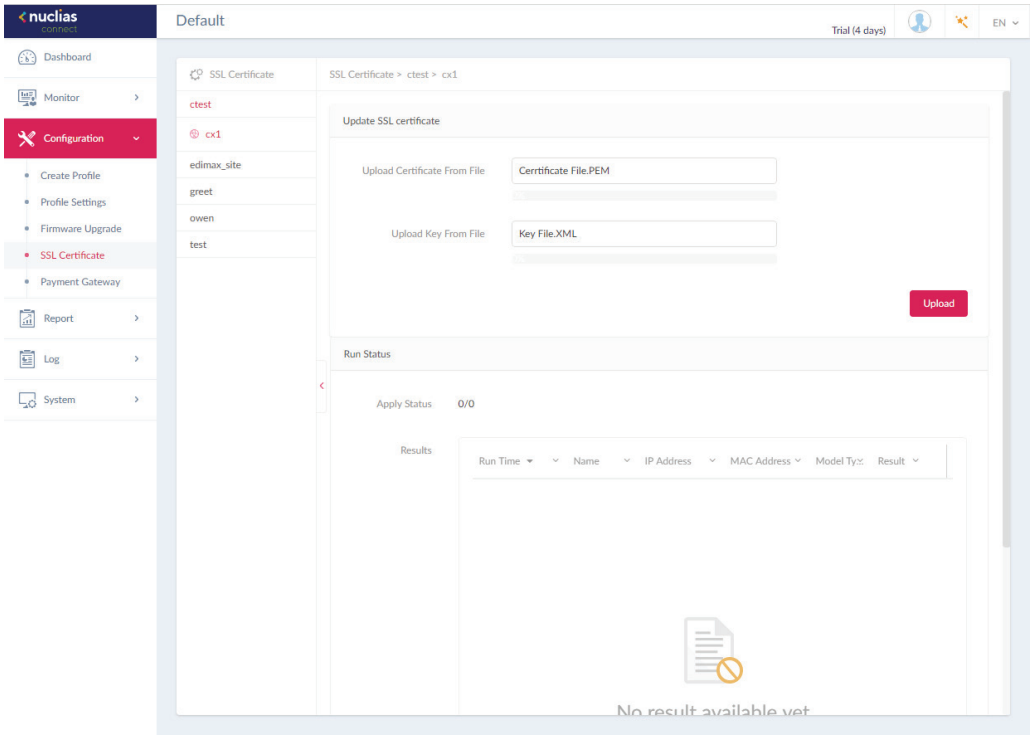
# Nuclias Connect Configuration SSL Certificate

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:

| Block | Description |
|---|---|
| **Upload Certificate From File** | Click **Browser...** to select the SSL certificate file located on the drive that will be uploaded. |
| **Upload Key From File** | Click **Browser...** to select the SSL key file located on the local drive that will be uploaded. |

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



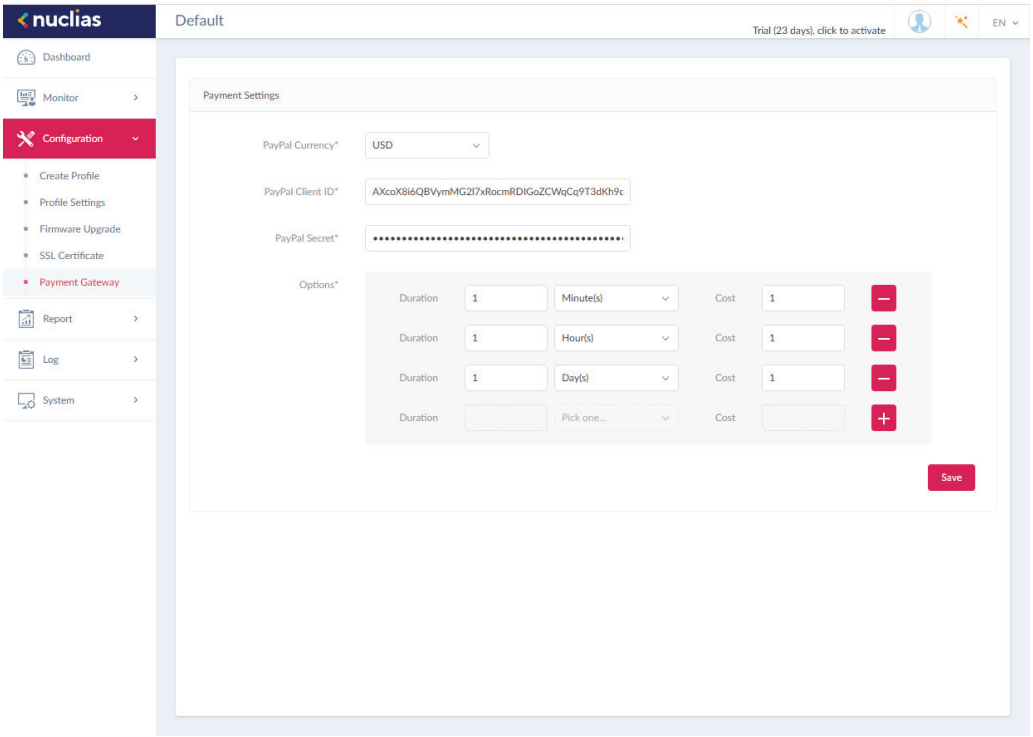
# Nuclias Connect Configuration Payment Gateway

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.



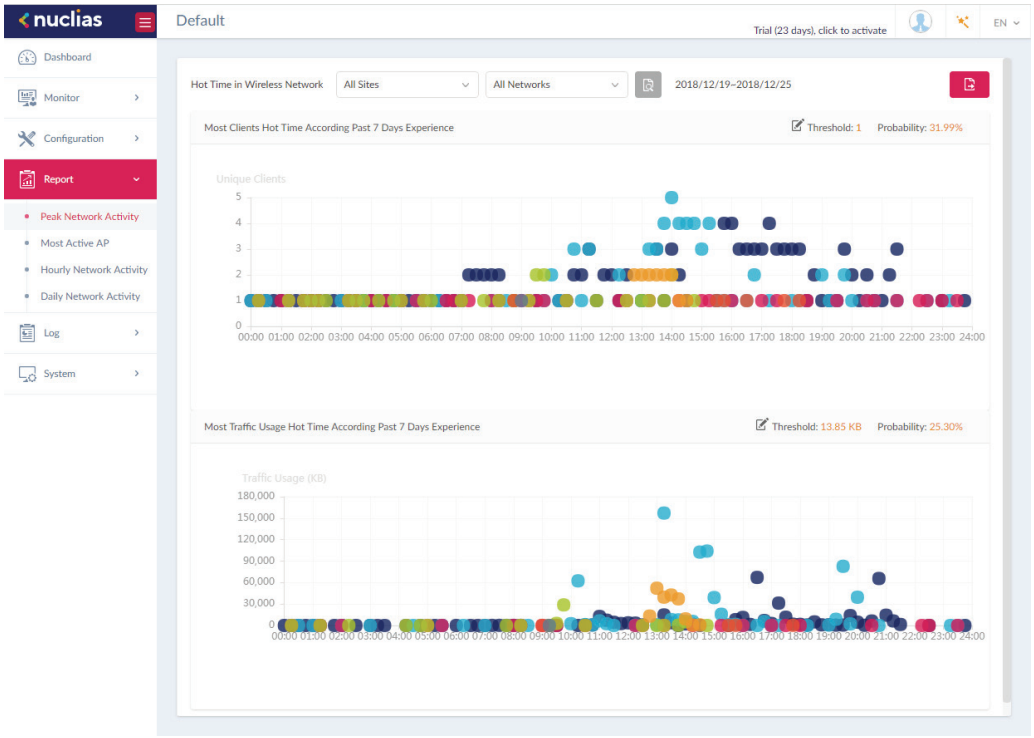
# Nuclias Connect Report Peak Network Activity

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 nformation.

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.

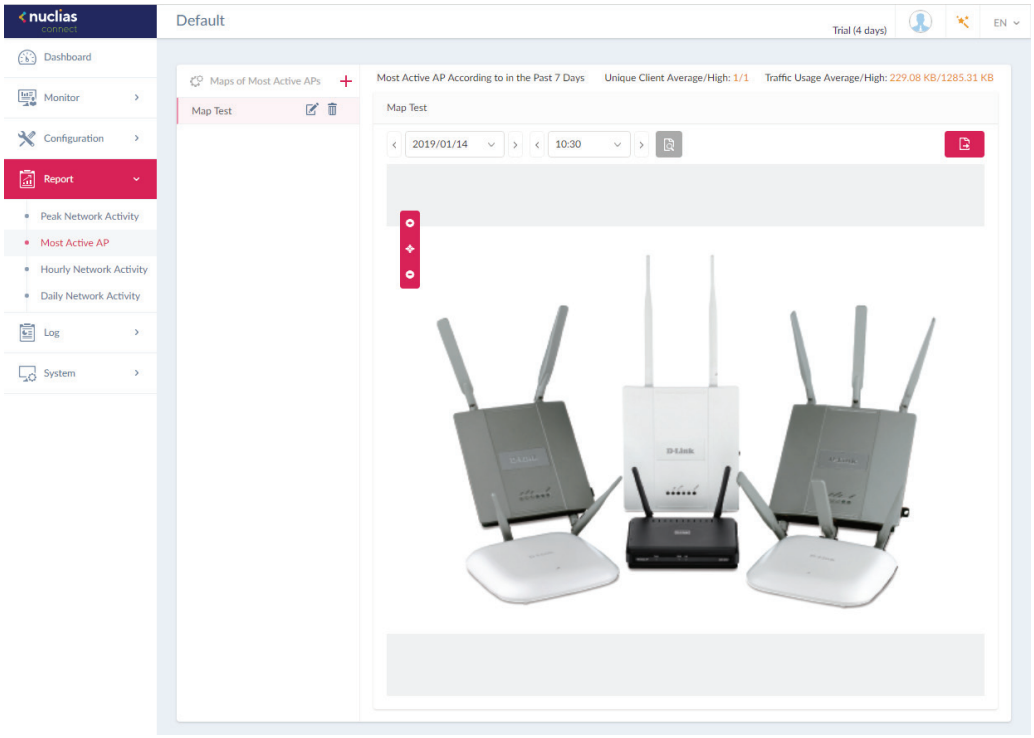


# Nuclias Connect Report Most Active AP

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 name 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 the image.

To view a network AP active map report, select the date and time then click to view the report.
Once a report has been generated, click to save the report to a local PDF file.



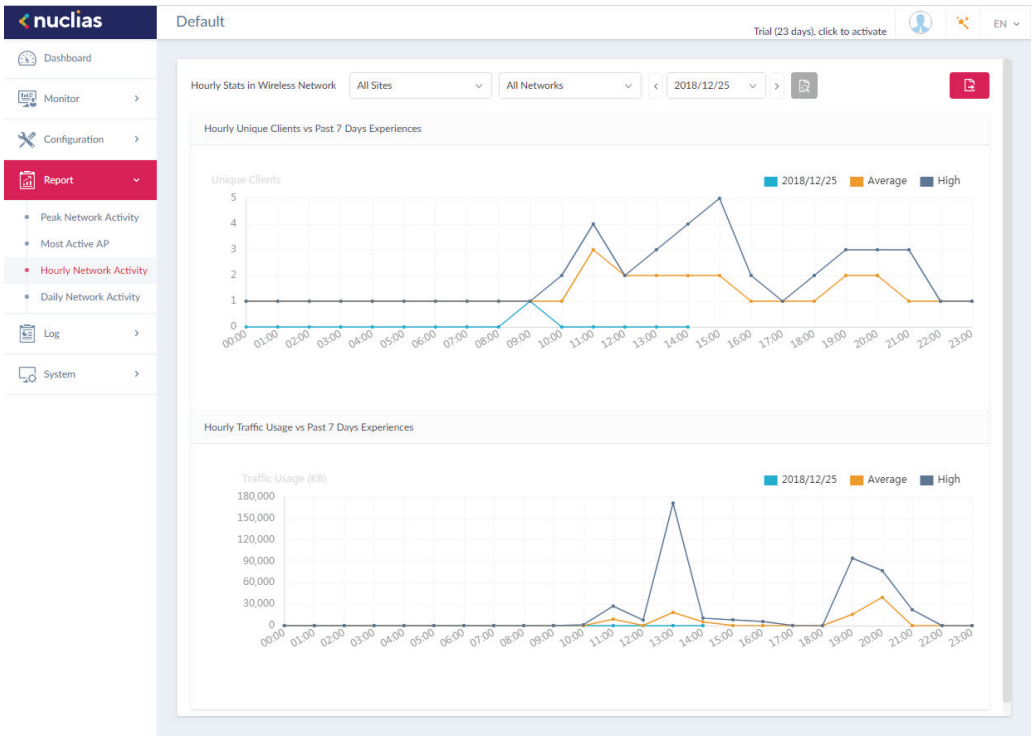
# Nuclias Connect Report Hourly Network Activity

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



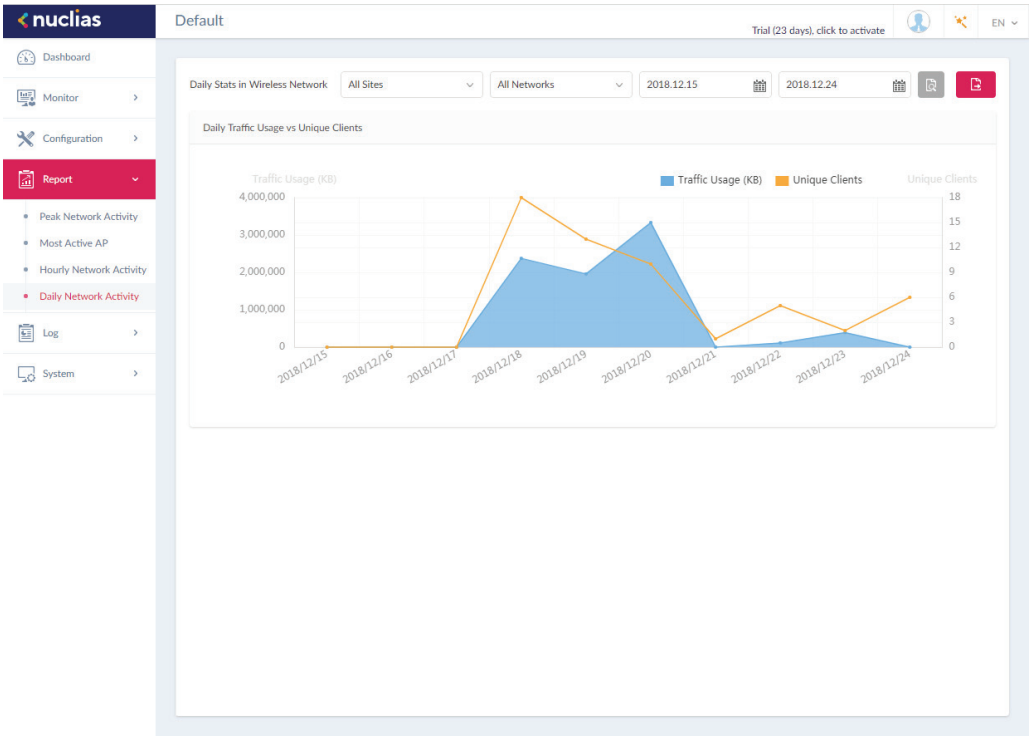
# Nuclias Connect Report Daily Network Activity

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

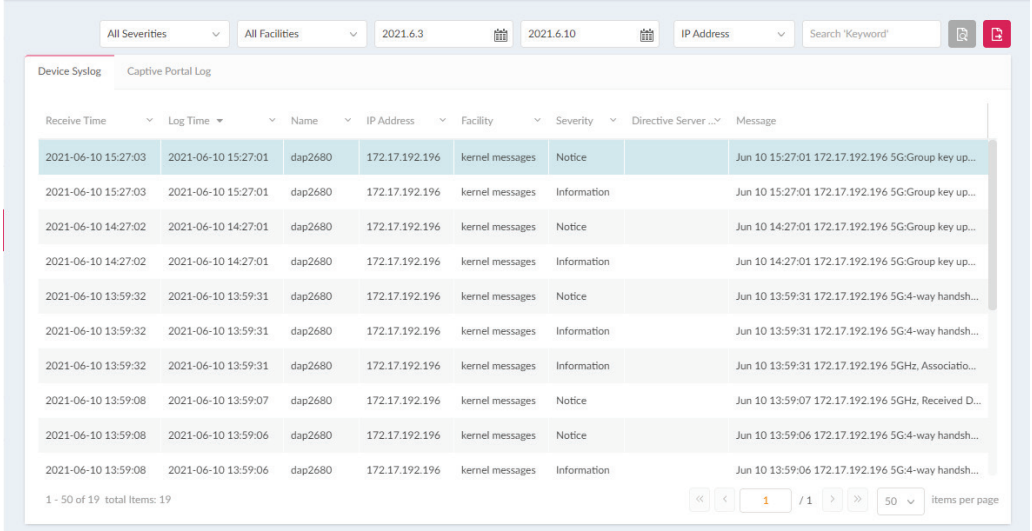


# Nuclias Connect Log Device Syslog

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 gengerated report.

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

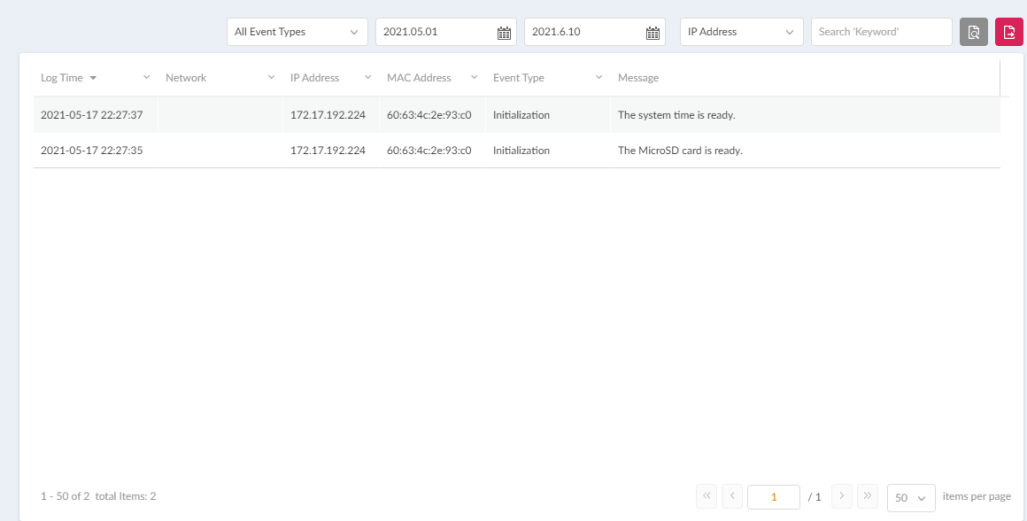


# Nuclias Connec Log System Event Log

The System Event Log function allows administrators to view alerts that may require attention and necessary action to continue smooth 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 has been generated, click to save the report to a local PDF file.



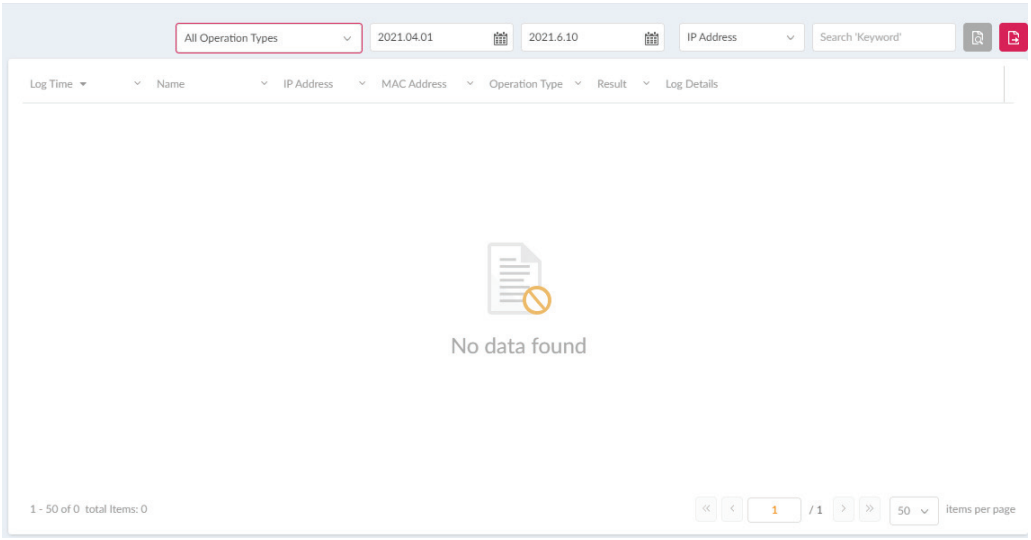
# Nuclias Connect Log Device Log

The Device Log function allows administrators to view alert messages from an AP's embedded memory. The system and network messages includes a time stamp and message type. The log information includes but is 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.

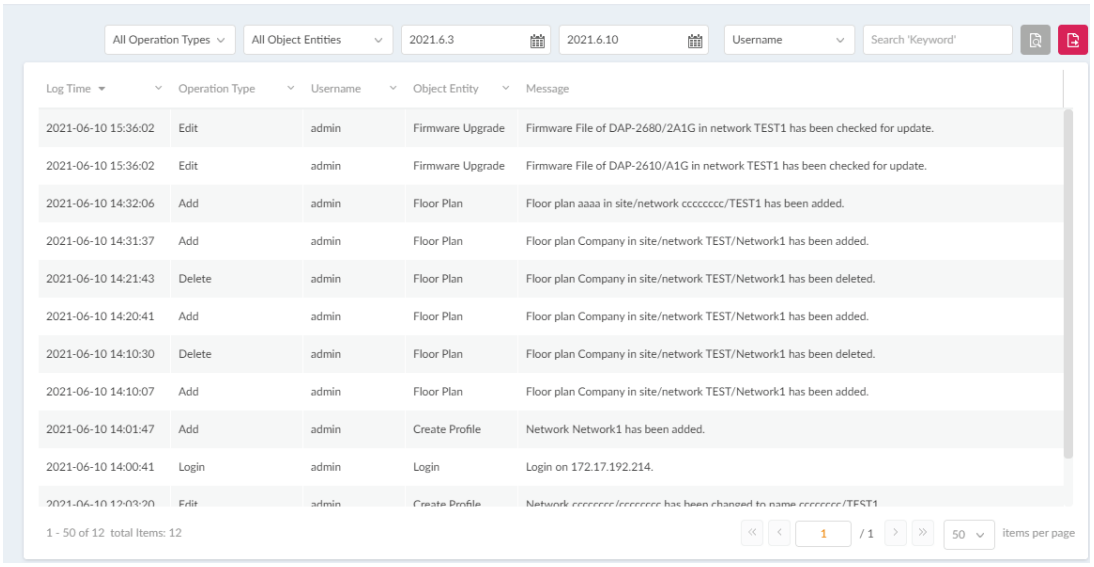
To start a Device Log, select the operation type and define the period of time to report. Click the drop-down menu to define the type of search criteria to view, IP address or Trap Details. Fill in the keyword field and click to view the generated report.

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



# 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.

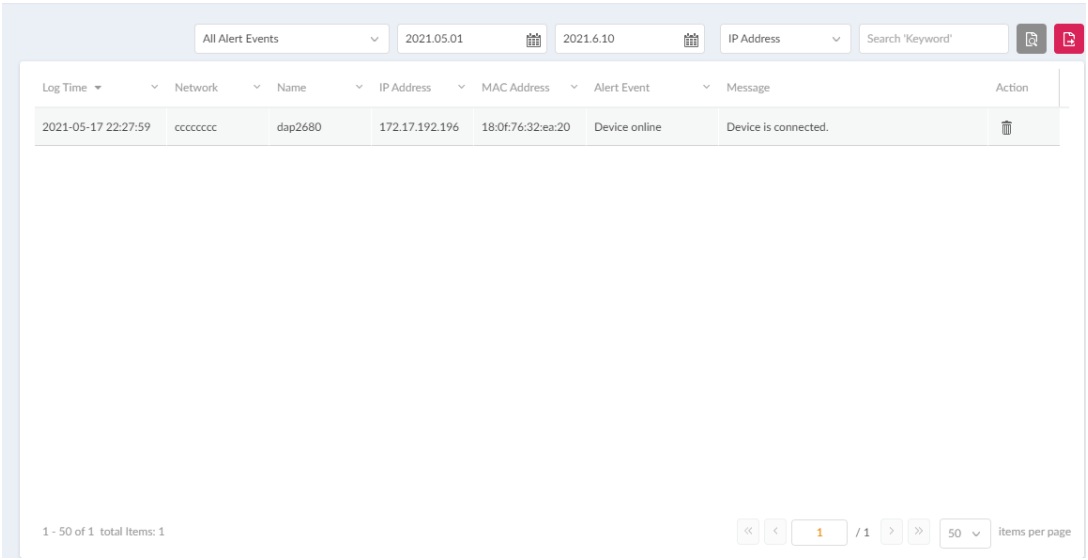



To generate an Audit Log report, select the entries by Operation Type (operations that performed on the object entities) and Object Entity (i.e. the objects associated with the functional tabs in the left pane), define the time period, and select Username or Message as the filtering criteria. Then enter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

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

# Nuclias Connect Log Alerts

This type of log records events activities for alert, e.g. new firmware release, port linked or blocked, and device online or offline.




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

# Nuclias Connect System Device Management

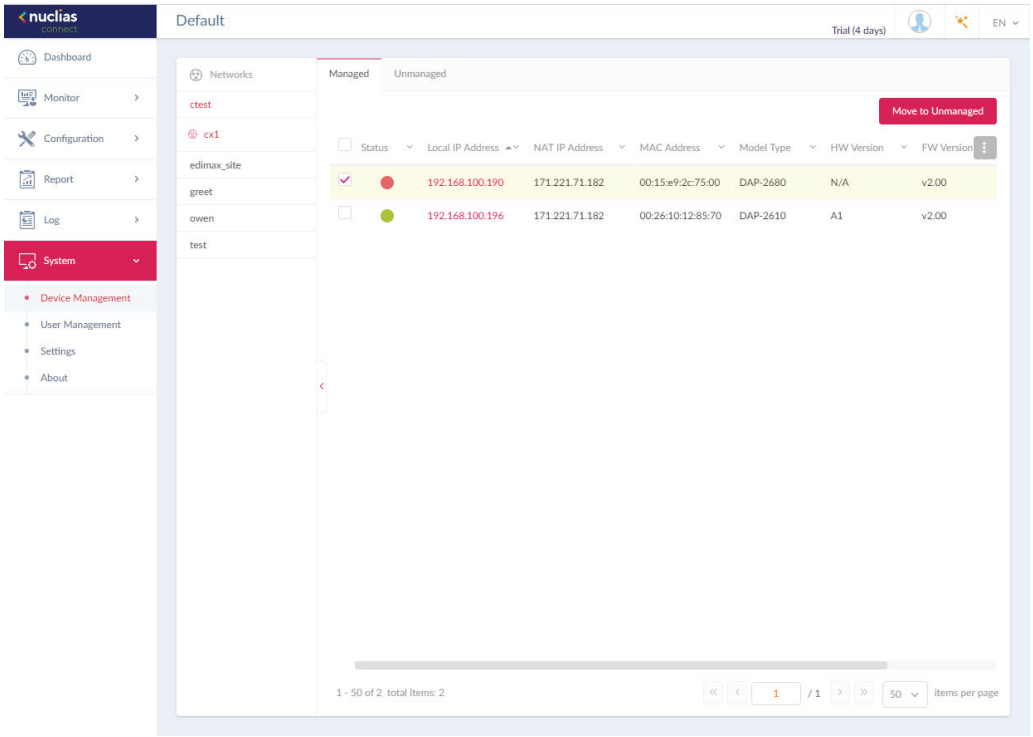
The Device Management function allows Allows user to view list of all devices on the network both managed and unmanaged devices.

Navigate to **Log > Device** Log to view the relevant information.

Click on the prospective tab to view either managed or unmanaged devices.

On the upper right hand corner of each tab is a button that you can use to move devices to Unamanaged, and vice versa. On the unmanaaged tab, next to the Move button is the Delete button that can be used to delete a device on the network.

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 criteria by which you can add to the list to view.



# Nuclias Connect System User Management User Status

The User Status function allows administrators to view the current status of all registered user profiles, edit or delete the profile. From the page, the Login Status displays the login state of the user; ● indicates a logged in state, while ● indicates the user is logged off.

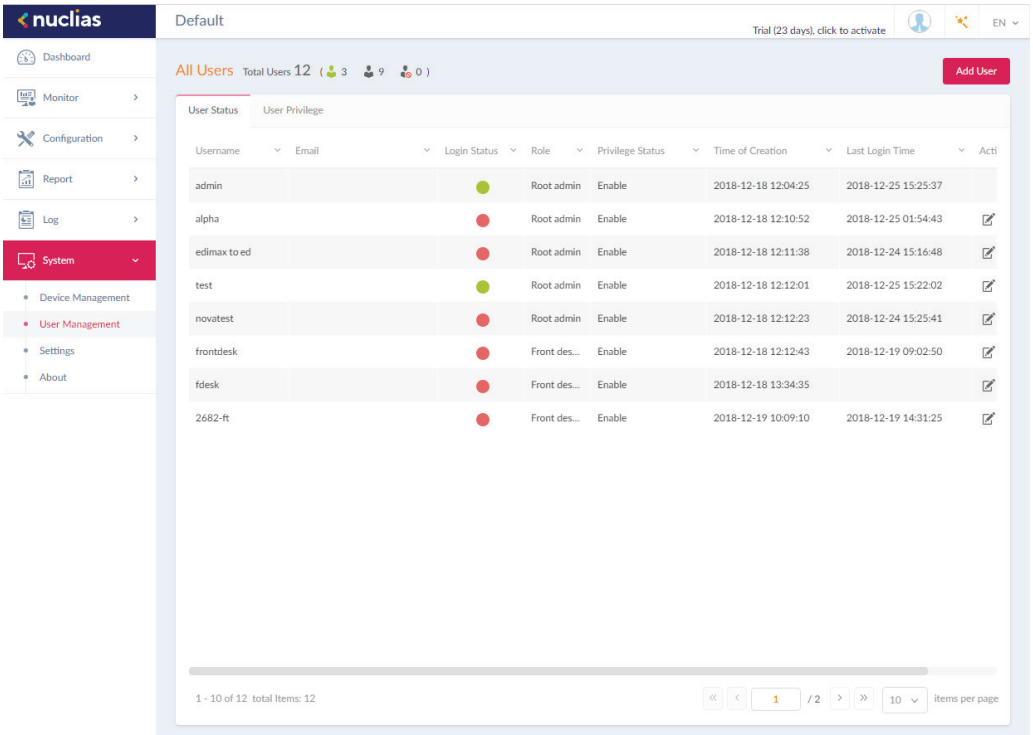
Navigate to **System > User Management** to view the relevant information.

To edit a user profile, select a user and click ✎ and the User Management page displays. The username, password, email, priviledge, priviledge status, location, contact number as well as the user description are editable from the modifications page. As a note, 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.

The following is a list of available user profiles and a description of their function.

- Admin: This is operator account and can not be deleted.
- Root admin: Can manage all sites/networks on this server.
- Local admin: Can manage his own network.
- Root user: Can view all sites/networks on this server.
- Local user: Can view his own network
- Front desk user: Can generate and manage passcodes.

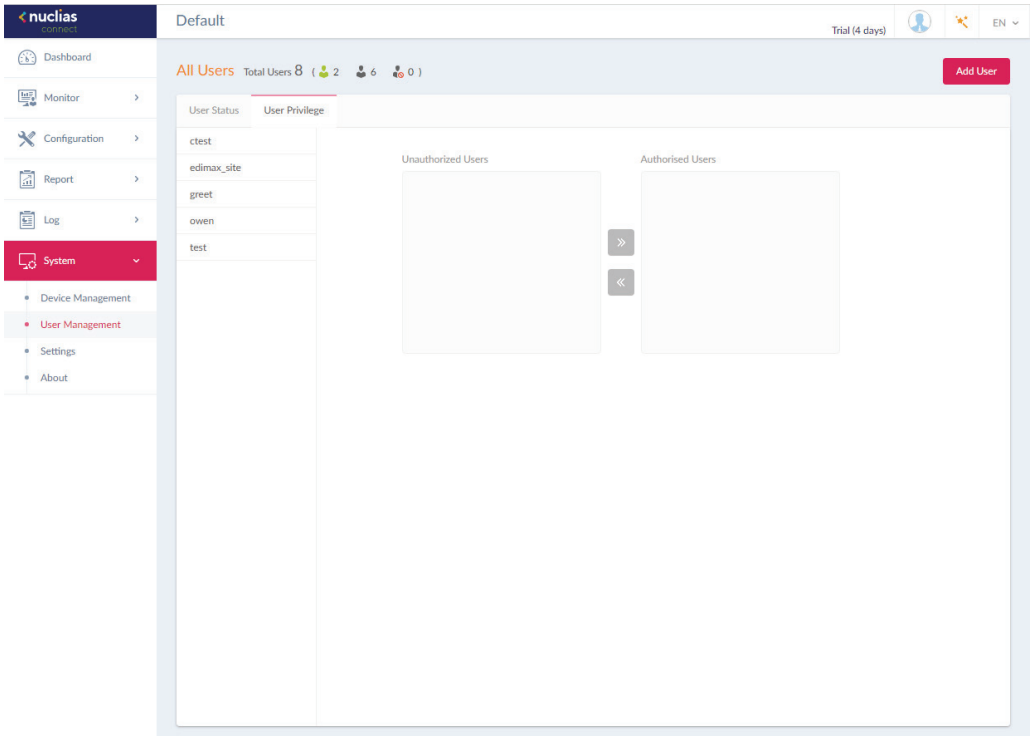


# Nuclias Connect System User Management User Privilege

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 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 to 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.

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, and SMTP information. The General tab displays customizable 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 display the function information.

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

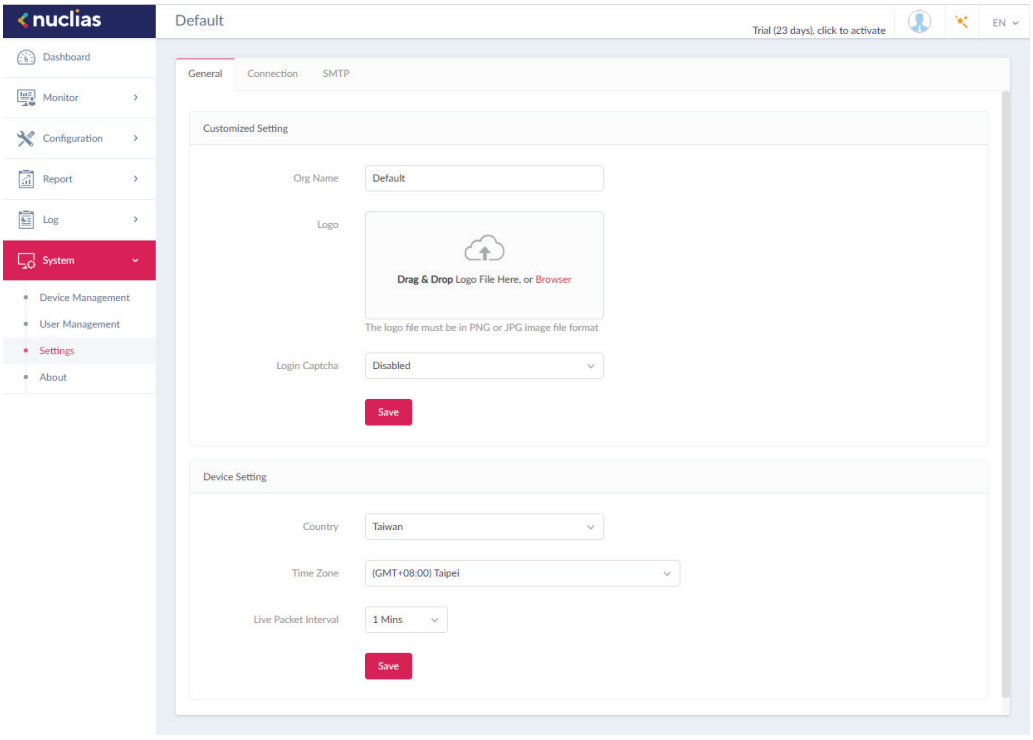
| Parameter | Description |
|---|---|
| **Org Name** | Enter a description to set the organization name |
| **Logo** | Click **Browser** to select a file to be used as the interface logo. A local file can be selected by using the browse function or by dragging and dropping a file into the frame. Supported 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 values and update the screen.

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

| Parameter | Description |
|---|---|
| **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. |
| **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.



# 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:

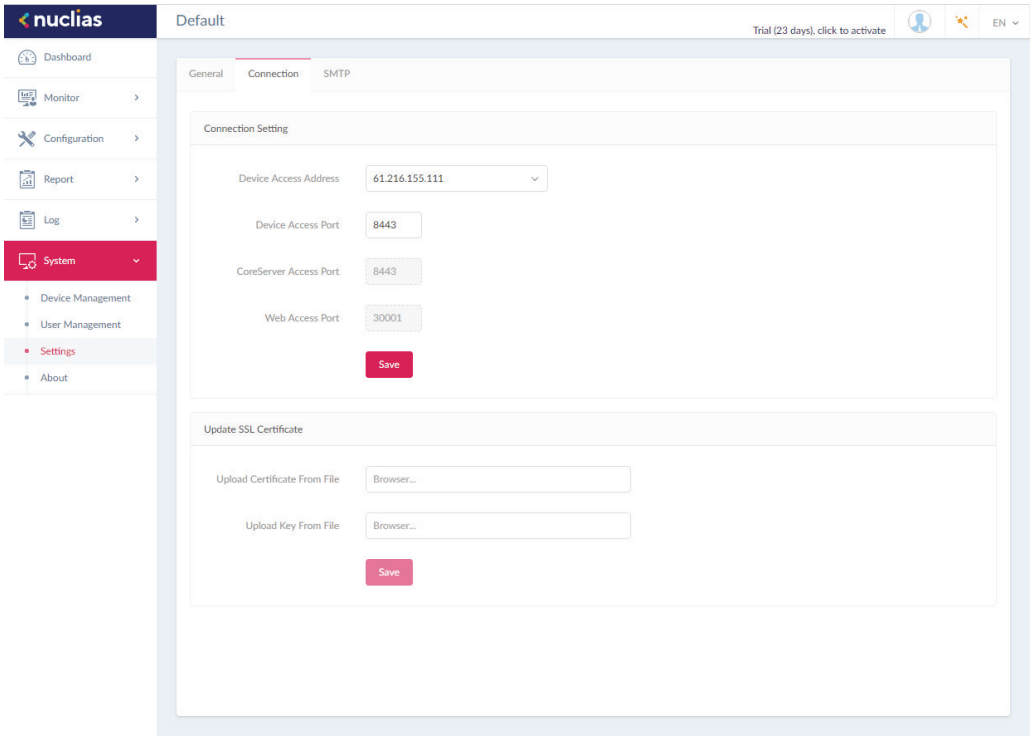
| Parameter | Description |
|---|---|
| **Device Access Address** | Enter the Nuclias Connect Server application's IP address. To manage remote APs, the IP address must be a public IP address; IP mapping is required for instances behind a firewall or router. |
| **Device Access Port** | Enter the Nuclias Connect server application's listen port number. The default value is 8443. For remote AP management behind a firewall or router, the inboud 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 **Browser...** to select the SSL certificate file located on the local drive that will be uploaded. |
| **Upload Key From File** | Click **Browser...** to select the SSL key file located on the local drive, that will be uploaded. |

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



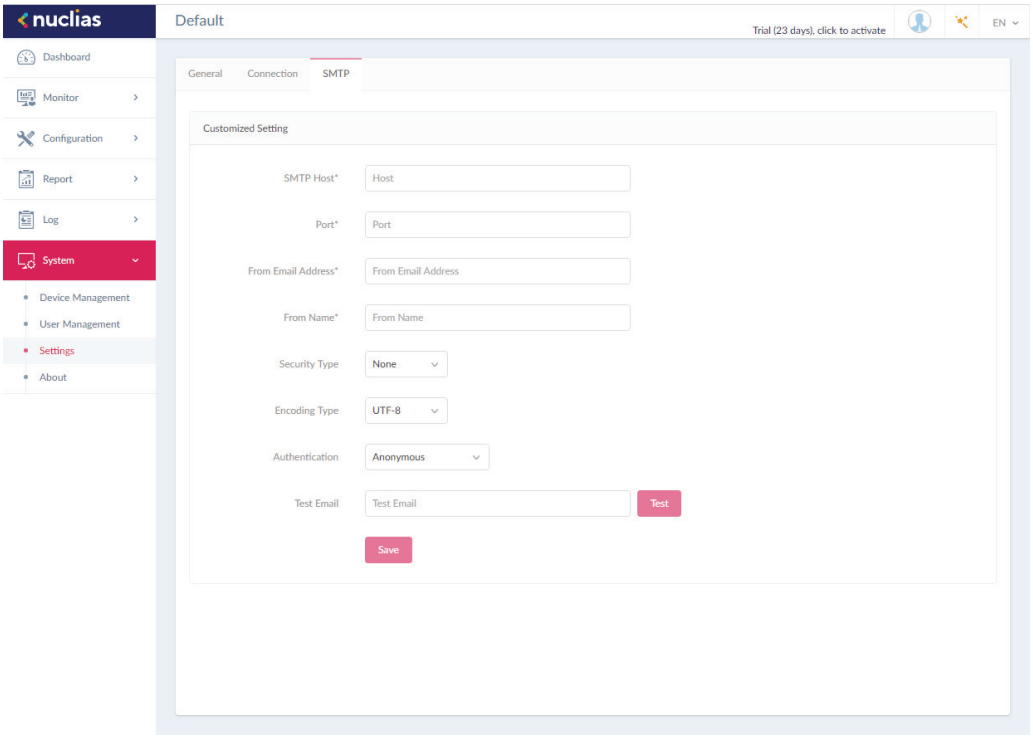
# Nuclias Connect System Settings SMTP

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 logging supported by the e-mail server. 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.

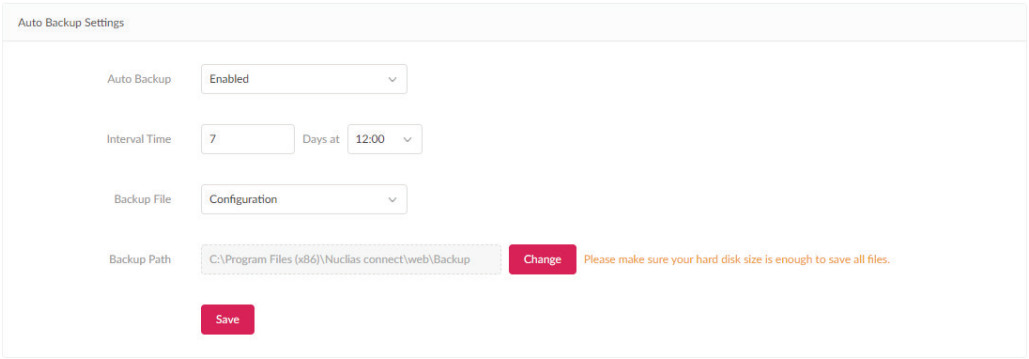


# Nuclias Connect System Settings Backup

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 |

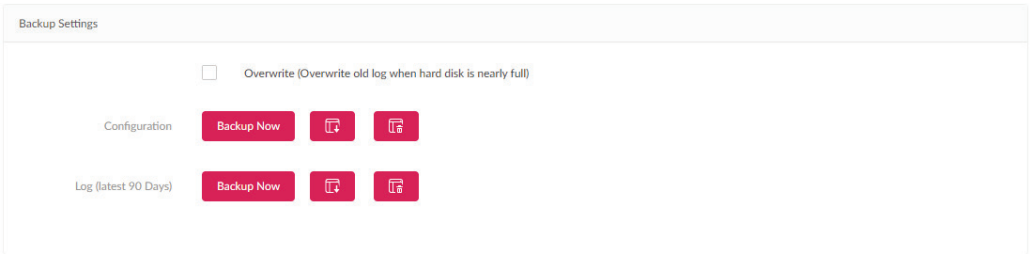



In the **Backup Settings** section, device configuration and logs can be backed up, downloaded to a local hard drive, or deleted.

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

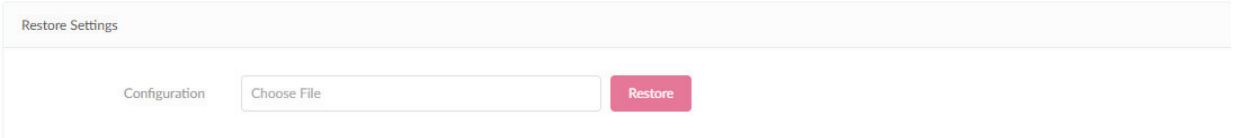
Click Download button to download the backup file to either the management computer's hard drive

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



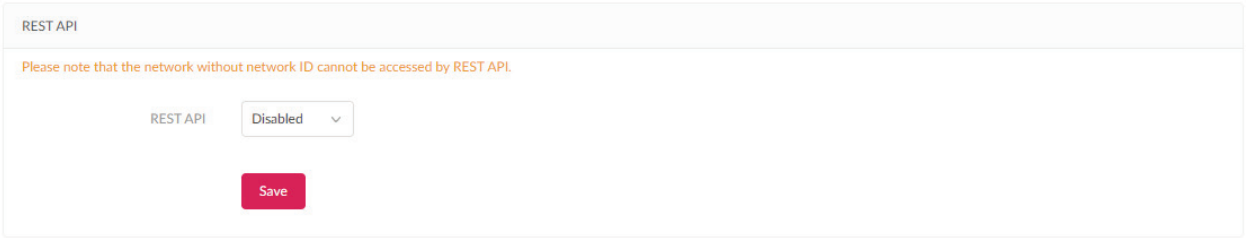

In the Restore Settings section, device configuration can be restored from local hard drive.

Specify the configuration file for configuration restore.



# 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.



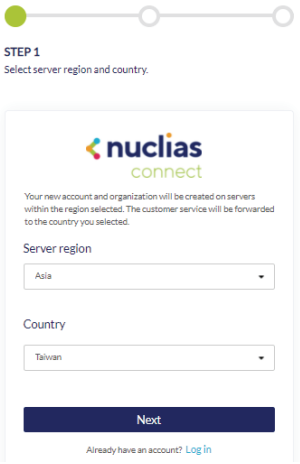
# Nuclias Connect System Settings Single Sign-On (SSO)

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, you can click on Create acount 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.



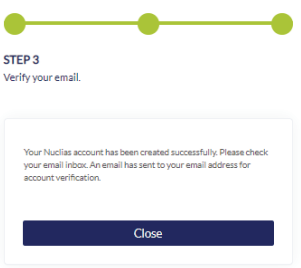

Step 2: Create organization and site.

Once the region and country have been entered, you will see the 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 3: Finish the registration.

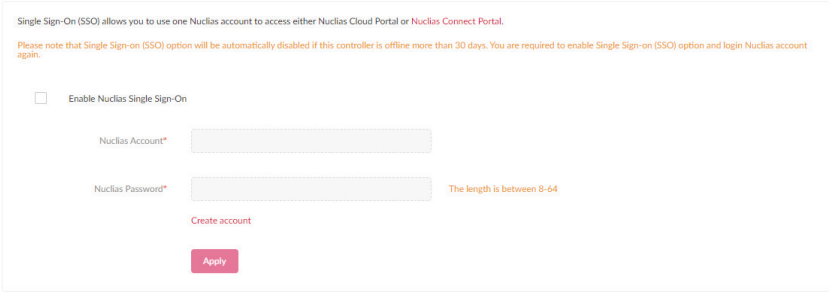
Click Close to complete the process. The registered account is now available for use. The verification information will be delivered to the registered email of the account



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. |



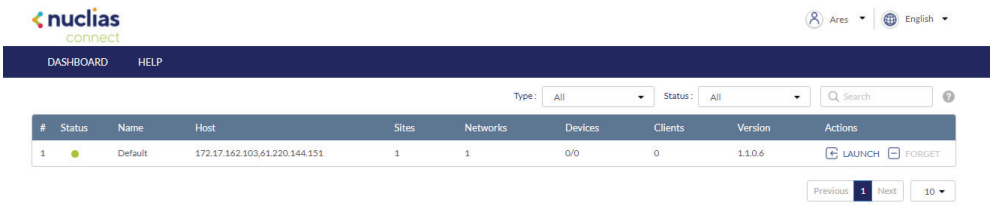

The Nuclias Connect Portal provides you with an easy way to view and connect to all your Nuclias Connect.

Requirements for use include:

• A Nuclias account

• DNC-100 with single-sign-on enabled

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



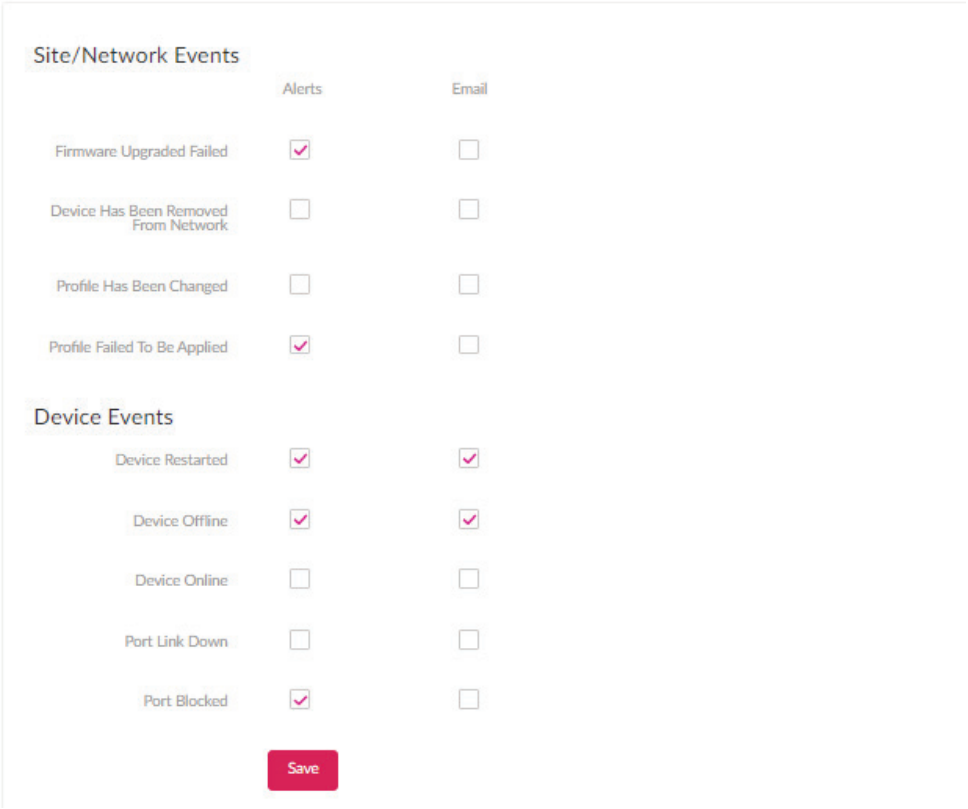

The Portal provides the following information:

| Parameter | Description |
|---|---|
| **Number** | Number of the DNC-100 on the list. |
| **Status** | Displays whether or not the Nuclias Connect portal can link.to that 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 that DNC-100. |
| **Networks** | Number of networks managed by that DNC-100. |
| **Devices** | Number of devices managed by that DNC-100. |
| **Clients** | Number of clients connected to devices managed by that DNC-100. |
| **Version** | Software version number of that 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 this DNC-100 from the Nuclias Connect portal. (Forget is only available when that 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.

Check the specific event of Email button, and go to **System**>**Settings**>**User Management**, edit the user and select "Receive Email Alert" to allow use to receive alert email from Nuclias Connect.




Click Save to save the values and update the screen.

# 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 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.