NUCLIAS CLOUD
DBA Series User Manual

V 1.01

nuclias
cloud

1 Table of Contents

1. Introduction

The manual is organized according the menu layout of the Nuclias Portal interface.

1.1 Audience

This reference manual is intended for network administrators and other IT professionals responsible for managing network devices using the Nuclias Portal. This manual is written in a way that assumes that you already have a basic knowledge of modern networking principles.

1.2 Other Documentation

The documents below are a further source of information with regards to configuring and troubleshooting Nuclias Portal. All the documents are available either from the D-Link website or the Nuclias website. Other documents related to Nuclias Portal are:

- Nuclias Switch User Manual

1.3 Conventions

Convention	Description
Boldface Font	Indicates a button, a toolbar icon, menu, or menu item. For example: Open the **File** menu and choose **Cancel**. Used for emphasis. May also indicate system messages or prompts appearing on screen. For example: **You have mail**. Bold font is also used to represent file names, program names, and commands. For example: Use the **Copy** command.
Initial capital letter	Indicates a window name. Names of keys on the keyboard have initial capitals. For example: Click Enter.
Menu Name > Menu Option	Indicates the menu structure. **Device > Port > Port Properties** means the **Port Properties** menu option under the **Port** menu option that is located under the **Device**.

Table 1-1

1.4 Notes, Notices, and Cautions

Below are examples of the three types of indicators used in this manual. When making changes to Nuclias Portal using the information in this document, you should pay special attention to these indicators. Each example below provides an explanatory remark regarding each type of indicator.

NOTE: A note indicates important information that helps you make better use of your device.

NOTICE: A notice indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

CAUTION: A caution indicates a potential for property damage, personal injury, or death.

2 Product Introduction

D-Link Nuclias is a cloud-hosted platform that removes the cost and complexity involved with owning and maintaining your own wireless infrastructure.

Access to the D-Link Nuclias Portal platform is via a web browser. The Nuclias Portal is divided into organizations, allowing devices to be grouped in Site Tags and Sites for their physical location and be configured as a group using Profiles. Users can also be given access to the Nuclias Portal based on roles and privileges, allowing access to only the parts of the interface that are required.

The Nuclias Portal simplifies the management of your wireless and wired network, reducing the need for dedicated support staff, and allowing large numbers of devices to be managed from a single interface. Devices can be pre-registered, allowing them to be installed on site without requiring dedicated IT personnel. This reduces installation costs and simplifies network management, making the Nuclias Cloud an ideal solution for expanding and managing your new or existing wireless network.

2.1 Terms and Concepts

The following section provides a brief introduction and description of the terms and concepts used in this product.

Service Provider (SP): A Service Provider is an instance that sells the D-Link Nuclias service to customers and is responsible for providing user accounts (through invitation), and provision devices and licenses to subscribed organizations. A Service Provider can also assist in configuring an organization on request. Structurally, an SP operates at the highest level, one level higher than an MSP.

Managed Service Provider (MSP): A Managed Service Provider (MSP) or Systems Integrator (SI) is an instance that sells the Nuclias service to client organizations. A Managed Service Provider can provision multiple organizations and can manage all organizations under it. A MSP cannot manage another MSP or its affiliated organizations. Structurally, an MSP operates one level higher than an organization.

Organization (Org.): An organization is a business entity that subscribes to the D-Link Nuclias Cloud through a SP or MSP to provide wireless access to its branches. An organization may manage itself or can request the Service Provider or MSP to manage the organization. An organization cannot manage other organizations on the same level. Within the Nuclias structure, organizations are considered clients. Examples of organizations include, branch offices, restaurants, medium-sized offices.

Site Tag: A Site Tag is a label for structurally organizing and visualizing an organization. Site Tags act as branches, with each Site Tag being able to carry one or more Sites. For example, an organization with activities in multiple geographical areas can use Site Tags to easily identify and manage regional branches.

Site: A Site is a label representing a physical location. Sites are used to group devices together for easier management. Sites can also be associated with a Site Tag, in which case the Site will branch of from the Site Tag. Examples of Sites include cities, branch offices, and work floors, depending on the size and scope of the organization.

Profile: Profiles are a set of general configuration settings that can be applied to all devices associated with the Profile so all devices are configured identically as a group. Profiles can be set up to cater to specific purposes and can be applied across different Sites and Site Tags. Examples of Profiles include customer Wi-Fi with limited access, a secure office network, and public Wi-Fi with captive portal login.

Privileges: Privileges determines to what extent the user can actively manage, ranging from full access to viewing only. Some elements of the Portal interface may be locked depending on the selected privilege. Refer to the overview below for a list of all available privileges.

Admin	An administrator has full access to all elements of the Portal interface and has full management capabilities.
Editor	An editor shares similar rights as an administrator, but cannot add or delete devices, users, or organizations.
Monitor	A monitor is limited to read-only access to configurations and analysis, and cannot configure or edit devices, users, or organizations.
Viewer	A viewer is restricted to read-only access to analysis only and cannot configure or edit devices, users, or organizations. This is primarily for on-site managers who only require organization statistics.

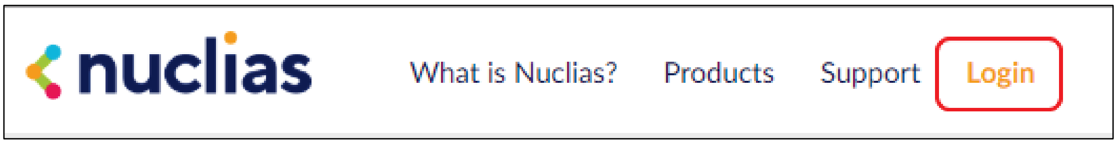
3 Getting Started with Nuclias

This section is designed to provide new users with instructions on how to get started with the D-Link Nuclias Cloud. This covers the basic requirements for using the Nuclias including how to create an account, and adding a new device using the provided Default Profile template which sets up a Wi-Fi network with recommended settings.

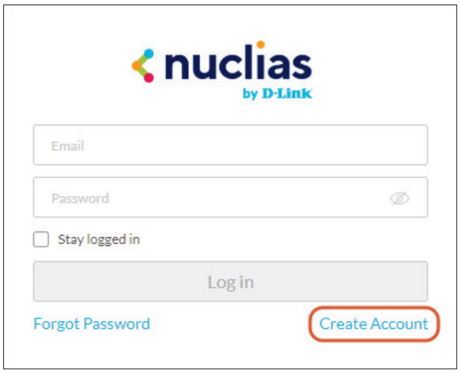
3.1 Creating an Account

Access to the D-Link Nuclias Cloud can be obtained by signing up for a free Nuclias account.

1. Go to **www.nuclias.com** and click **Login.**



2. Click **Create Account.**



3. Select a server region and customer service country and click **Next**.

Server Region	Select which server region to store your data on.
Country	Select a country for local support. If your country is not listed, choose the country closest to your area.

4. Fill out the required information:

Email	Enter your email address. This is also your user name to log into the Nuclias Portal interface.
Full Name	Enter your full name.

Password	Enter your account password.
Confirm Password	Confirm your password.
Organization Name	Enter your organization name. This will automatically create an organization with this name.
Region	Select a region. This will automatically create a Site using this region.
Timezone	Select a time zone.
Address	Enter your address.

3. Click **Create Account**.
4. You will receive an email containing a verification link. Once verified, you can now log into the Nuclias Portal interface using your account email address and password.

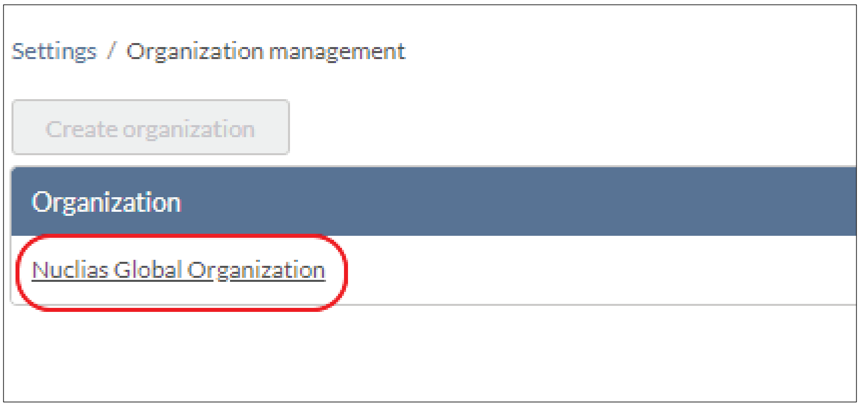
3.2 Logging In To Nuclias

1. In a web browser, go to login.nuclias.com.
2. Enter your registration email address and password.
3. Click **Log In**.

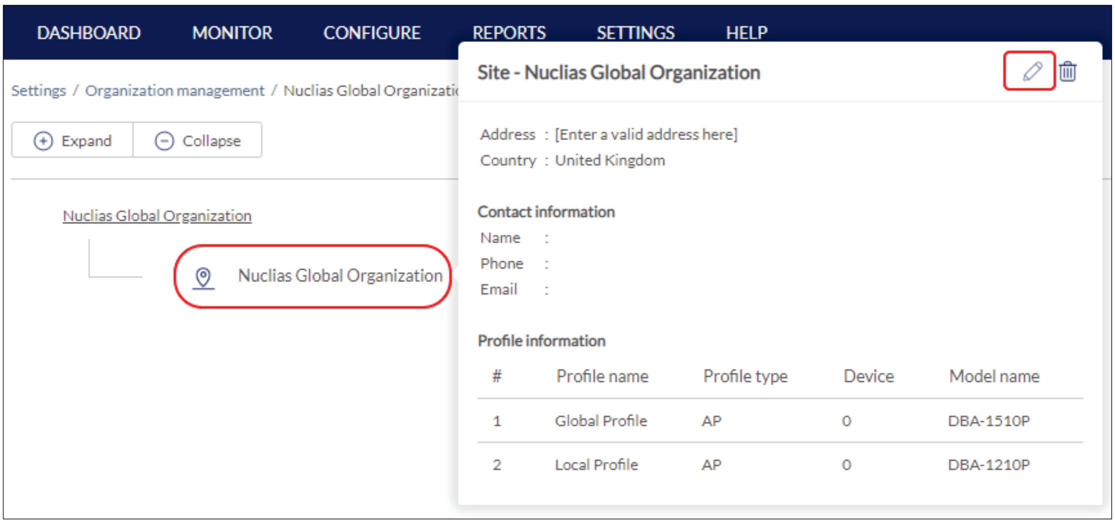
3.3 Creating a Profile

A Profile is a set of configuration settings that can be easily applied to all devices using this Profile. Multiple Profiles can be created to accommodate different requirements. When creating a new user account, the system will automatically create a set of default Profiles with recommended settings. The instructions below will explain how to create a custom Profile.

1. Navigate to the **Settings > Organization Management** page.
2. Click on the organization name to open the Site overview page.


Settings / Organization management
Create organization
Organization
Nuclias Global Organization

3. On the Site overview page, hover the cursor over the Site name and click the Pencil icon in the top-right to edit the site.


DASHBOARD
MONITOR
CONFIGURE
REPORTS
SETTINGS
HELP
Settings / Organization management / Nuclias Global Organizati
Expand
Collapse
Nuclias Global Organization
Nuclias Global Organization

Site - Nuclias Global Organization

Address : [Enter a valid address here]
Country : United Kingdom

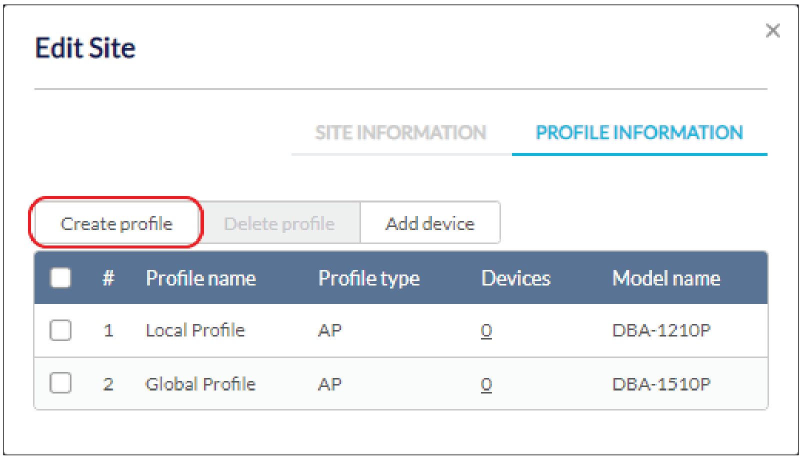
Contact information

Name :
Phone :
Email :

Profile information

#	Profile name	Profile type	Device	Model name
1	Global Profile	AP	0	DBA-1510P
2	Local Profile	AP	0	DBA-1210P

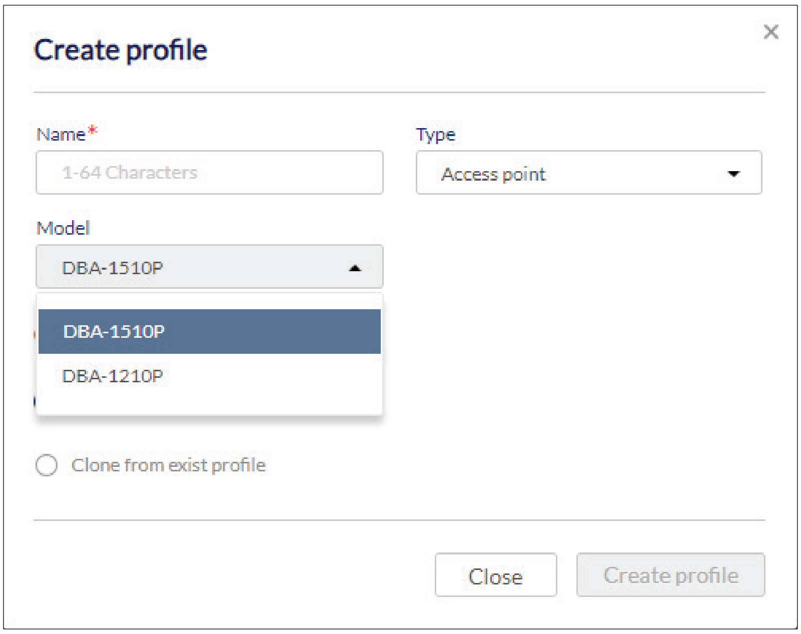
4. In the Edit Site window, click the **Profile Information** tab and click **Create Profile**.



□	#	Profile name	Profile type	Devices	Model name
□	1	Local Profile	AP	0	DBA-1210P
□	2	Global Profile	AP	0	DBA-1510P

5. Enter a name for the Profile and choose the device model.

Note: The Profile can only be used for the selected device model type.



Create profile

Name* 1-64 Characters

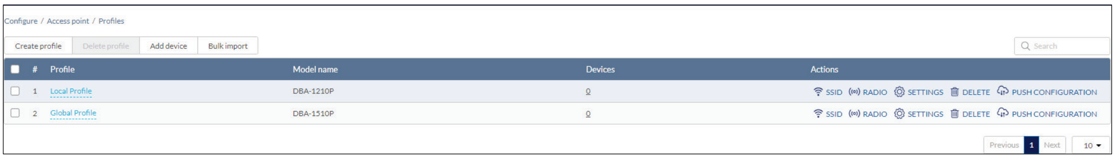
Type: Access point

Model: DBA-1510P

5. Click **Create Profile**.

3.4 Configuring a Profile

Once the Profile is created, you can start configuring a variety of settings for the Profile including setting up and customizing SSIDs, configure wireless band settings, and advanced settings.



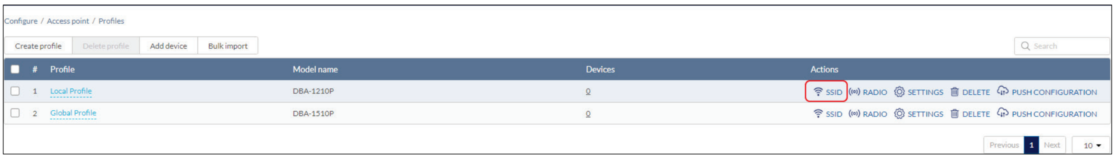
Configure / Access point / Profiles

□	#	Profile	Model name	Devices	Actions
□	1	Local Profile	DBA-1210P	0	SSID RADIO SETTINGS DELETE PUSH CONFIGURATION
□	2	Global Profile	DBA-1510P	0	SSID RADIO SETTINGS DELETE PUSH CONFIGURATION

3.4.1 Creating SSIDs

Multiple SSIDs can be created per Profile. Each SSID can be configured with unique settings to accommodate different scenarios.

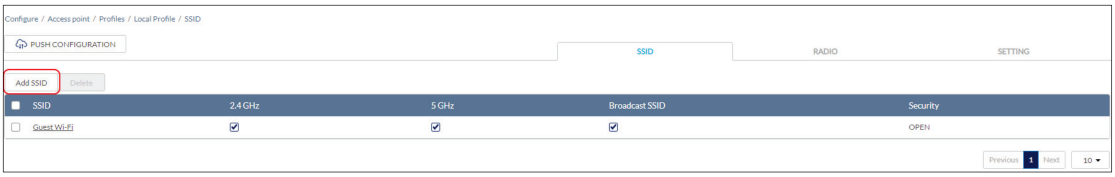
1. Navigate to the **Configure > Access Point > Profiles** page and click **SSID**.



Configure / Access point / Profiles

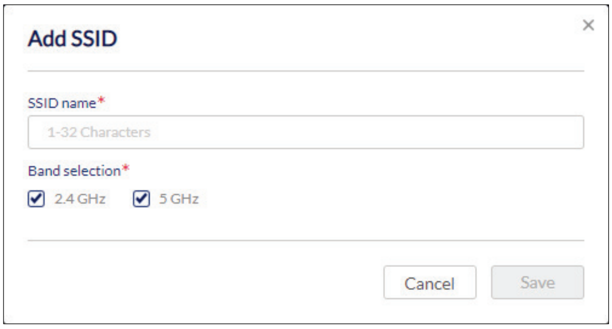
□	#	Profile	Model name	Devices	Actions
□	1	Local Profile	DBA-1210P	0	SSID RADIO SETTINGS DELETE PUSH CONFIGURATION
□	2	Global Profile	DBA-1510P	0	SSID RADIO SETTINGS DELETE PUSH CONFIGURATION

2. On the SSID page, click **Add SSID.**



☐ SSID	2.4 GHz	5 GHz	Broadcast SSID	Security
☐ Guest Wi-Fi	☑	☑	☑	OPEN

3. Enter a name for the SSID and choose which wireless bands to enable.



SSID name*

1-32 Characters

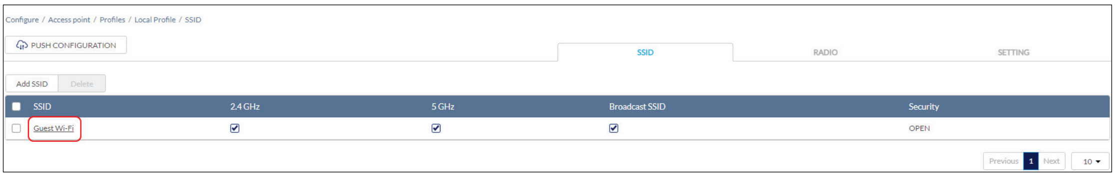
Band selection*

☑ 2.4 GHz ☑ 5 GHz

4. Click **Save.**
5. [**Optional**] Repeat steps **1** to **4** to create additional SSIDs.

3.4.1.1 Configuring SSIDs

1. Navigate to the **Configure > Access Point > Profiles** page.
2. Click on the SSID name.

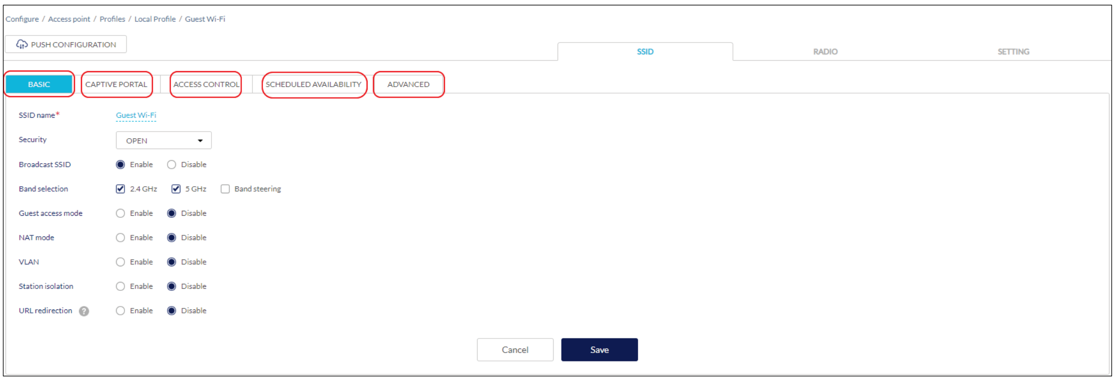


☐ SSID	2.4 GHz	5 GHz	Broadcast SSID	Security
☐ Guest Wi-Fi	☑	☑	☑	OPEN

3. From the SSID configuration window, click the **Basic, Captive Portal, Access Control, Scheduled Availability**, and **Advanced** tabs to configure the respective settings. Refer to the relevant SSID configuration sections in the User Manual for more detailed information about these settings.

Basic	Configure basic SSID settings including SSID name, security method, enabling or disabling wireless bands, and configuring VLAN settings.
Captive Portal	Configure a captive portal page for the SSID using click-through, sign-in, third party sign-in, or local and third-party sign-in.

Access Control	Configure MAC and IP-based Access Control Lists and RADIUS authentication for the SSID.
Scheduled Availability	Configure a schedule for when to enable or disable the SSID.
Advanced	Configure advanced settings including client and bandwidth limits, IGMP and multicast settings, and enabling or disabling force roaming.

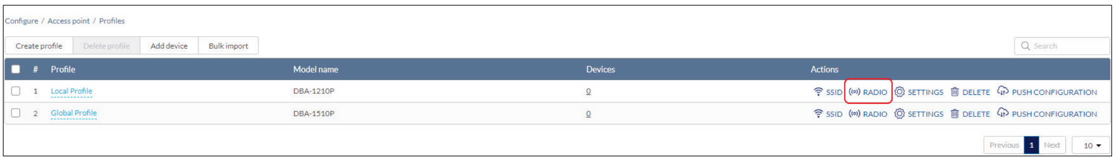


SSID name*	Guest Wi-Fi
Security	OPEN
Broadcast SSID	● Enable ○ Disable
Band selection	☑ 2.4 GHz ☑ 5 GHz □ Band steering
Guest access mode	○ Enable ● Disable
NAT mode	○ Enable ● Disable
VLAN	○ Enable ● Disable
Station isolation	○ Enable ● Disable
URL redirection	○ Enable ● Disable

4. Click **Save**.

3.4.2 Configuring Radio Settings

1. Navigate to the **Configure > Access Point > Profiles** page and click **Radio**.

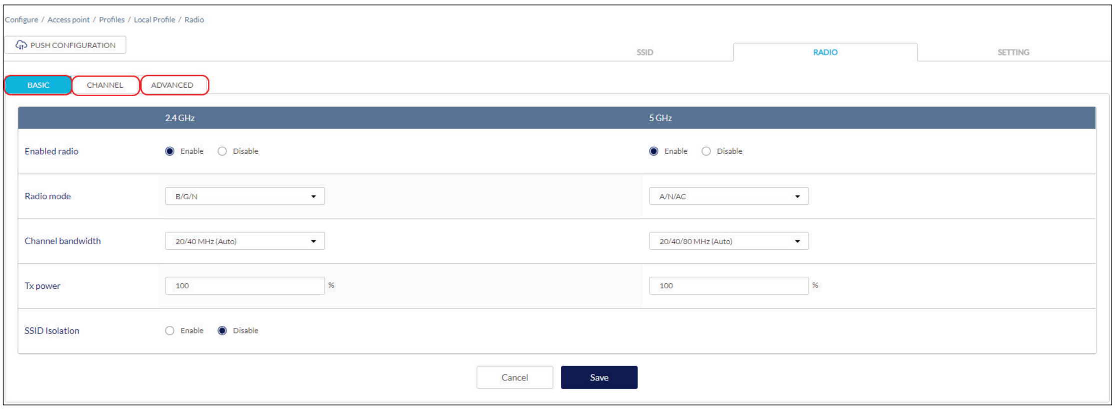


#	Profile	Model name	Devices	Actions
1	Local Profile	DBA-1210P	0	SSID RADIO SETTINGS DELETE PUSH CONFIGURATION
2	Global Profile	DBA-1510P	0	SSID RADIO SETTINGS DELETE PUSH CONFIGURATION

2. Click the **Basic, Channel**, and **Advanced** tabs to configure the respective settings. Refer to the relevant SSID configuration sections in the User Manual for more detailed information about these settings.

Basic	Configure basic wireless radio settings including enabling or disabling wireless bands, supported wireless standards, and radio transmitting power.
Channel	Configure wireless channel settings including selecting eligible channels and configuring auto-channel scanning.

Advanced	Configure advanced radio settings for performance and compatibility including multicast rate, protection mode, and UAPSD.



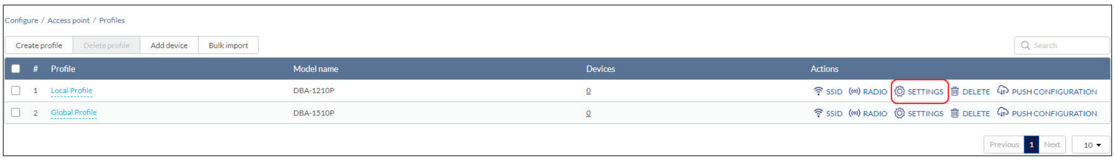
Configure / Access point / Profiles / Local Profile / Radio

	2.4 GHz	5 GHz
Enabled radio	● Enable ○ Disable	● Enable ○ Disable
Radio mode	B/G/N	A/N/AC
Channel bandwidth	20/40 MHz (Auto)	20/40/80 MHz (Auto)
Tx power	100 %	100 %
SSID Isolation	○ Enable ● Disable	

3. Click **Save**.

3.4.3 Configuring General Settings

1. Navigate to the **Configure > Access Point > Profiles** page and click **Settings**.

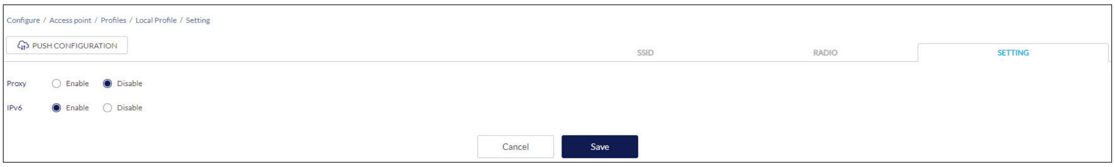


Configure / Access point / Profiles

□	#	Profile	Model name	Devices	Actions
□	1	Local Profile	DBA-1210P	0	SSID RADIO SETTINGS DELETE PUSH CONFIGURATION
□	2	Global Profile	DBA-1510P	0	SSID RADIO SETTINGS DELETE PUSH CONFIGURATION

2. Refer to the respective SSID configuration sections in the User Manual for more detailed information about these settings.

Settings	Configure a proxy server and enable or disable IPv6 support.



Configure / Access point / Profiles / Local Profile / Setting

Proxy ○ Enable ● Disable

IPv6 ● Enable ○ Disable

3. Click **Save**.

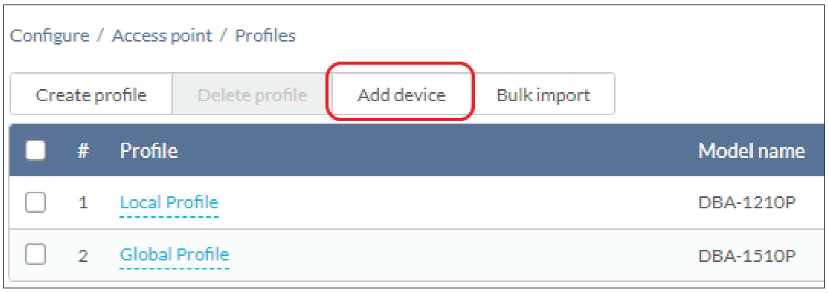
3.5 Adding a Device

In order to be able to manage the network, devices have to be added to the organization and assigned to Sites. There are multiple ways of adding devices to an organization.

3.5.1 Adding a Single Device

With all the configuration settings done, devices can be added to the organization. Devices are linked to a Site and a Profile to automatically retrieve their configuration settings.

1. Navigate to the **Configure > Access Point > Profiles** page.
2. Click **Add device**.



Configure / Access point / Profiles

□	#	Profile	Model name
□	1	Local Profile	DBA-1210P
□	2	Global Profile	DBA-1510P

3. Fill out the required information.

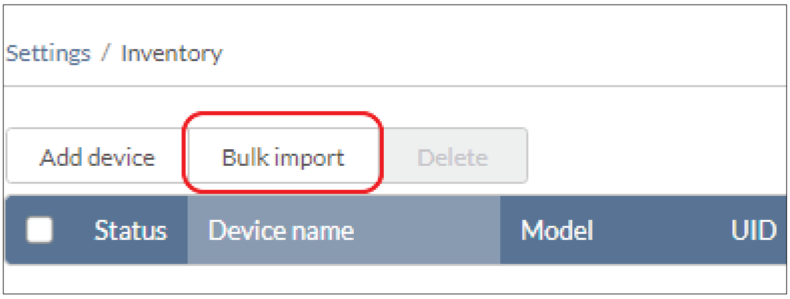
Device UID	Enter the device’s Unique Identifier (UID) found on the label printed on the device. The UID may be listed in the format **XXXX-XXXX-XXXX** or **XXXXXXXXXXXX**. When entering the UID, do not include dashes.
Device name	Enter a name for the device.
Site	Select a Site to link this device to.
Profile	Select a Profile for this device. The device will use the settings configured in that profile.
License Key	[**Optional**] Enter the device license key. **Note**: Every new device will be issued a one year free license key. Once expired, an additional license must be purchased to continue using the device.

3. Click **Save** when you are done.

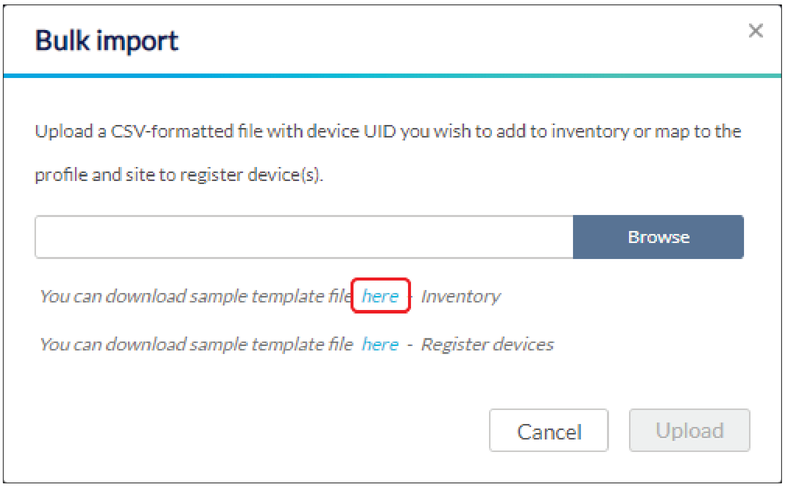
3.5.2 Bulk Adding Devices to Inventory

Devices can be bulk imported and added to Inventory to be assigned to a Site later.

1. Navigate to the **Configure > Access Point > Profiles** page.
2. Click **Bulk import**.



3. [**Optional**] Download the reference sample template.


Bulk import

Upload a CSV-formatted file with device UID you wish to add to inventory or map to the profile and site to register device(s).

You can download sample template file here - Inventory

You can download sample template file here - Register devices

4. Click **Browse**.
5. Locate the CSV-formatted file containing the UIDs of the devices.

   Note: To add devices to the inventory, use the following format:

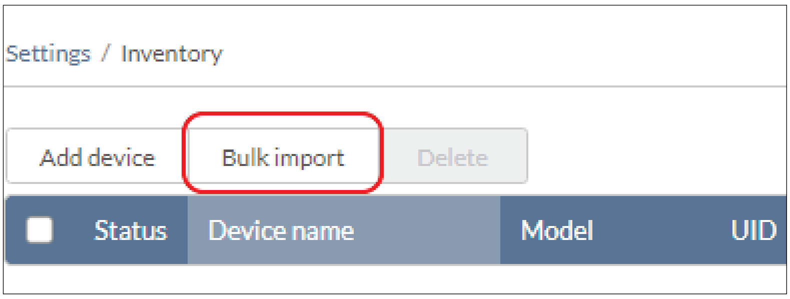
   [UID]
6. Click **Upload**.

3.5.3 Bulk Assigning Devices to Sites

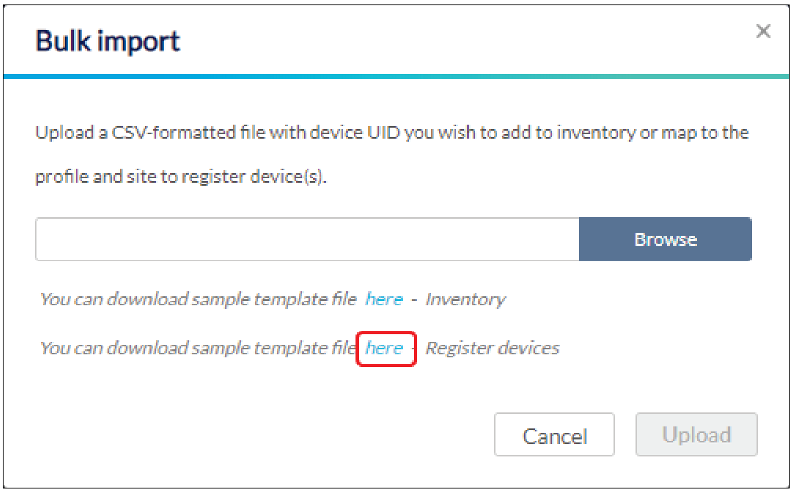
Devices can be bulk imported and immediately registered to a Site.

1. Navigate to the **Configure > Access Point > Profiles** page.

2. Click **Bulk import**.



3. [**Optional**] Download the reference sample template.



Upload a CSV-formatted file with device UID you wish to add to inventory or map to the profile and site to register device(s).

You can download sample template file here - Inventory

You can download sample template file here - Register devices

4. Click **Browse**.
5. Locate the CSV-formatted file containing the UIDs of the devices.

   Note: To directly register devices to a Site, use the following format:

   [UID][Device Name][Profile Name][Site][License Key]
6. Click **Upload**.

3.6 Managing Your Network With Nuclias

With the everything now set up, you can now start expanding and managing your network using Nuclias. There are several ways you can manage your network, refer to the following overview for more information.

- To view the real-time status of the network and at-a-glance information, refer to the **Dashboard section on page 22**.
- To monitor the organization and device activity, refer to the **Monitor section on page 26**.
- To visually structure organizations and manage devices using maps and floor plans, refer to the **Map and Floor Plans sections on pages 29 and 32**.
- To create, edit, and manage Profiles for device group configuration, refer to the **Profiles section on page 39**.
- To manage devices and perform device-specific configurations, refer to the **Devices section on page 61**.
- To create, edit, and manage user accounts, refer to the **Account** Management **section on page 88**.
- To edit and manage the organization, Site Tags, and Sites, refer to the **Organization Management section on page 92**.

4 Accessing the Nuclias Portal

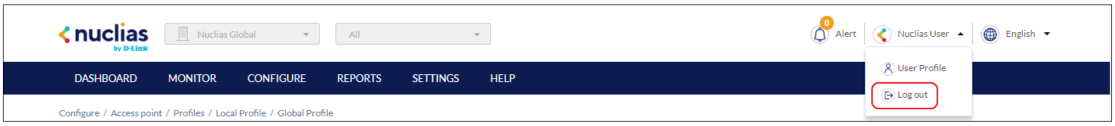
4.1 Logging in to Nuclias

1. In a web browser, go to login.nuclias.com.
2. Enter your registration email address and password.
3. Click **Log In**.

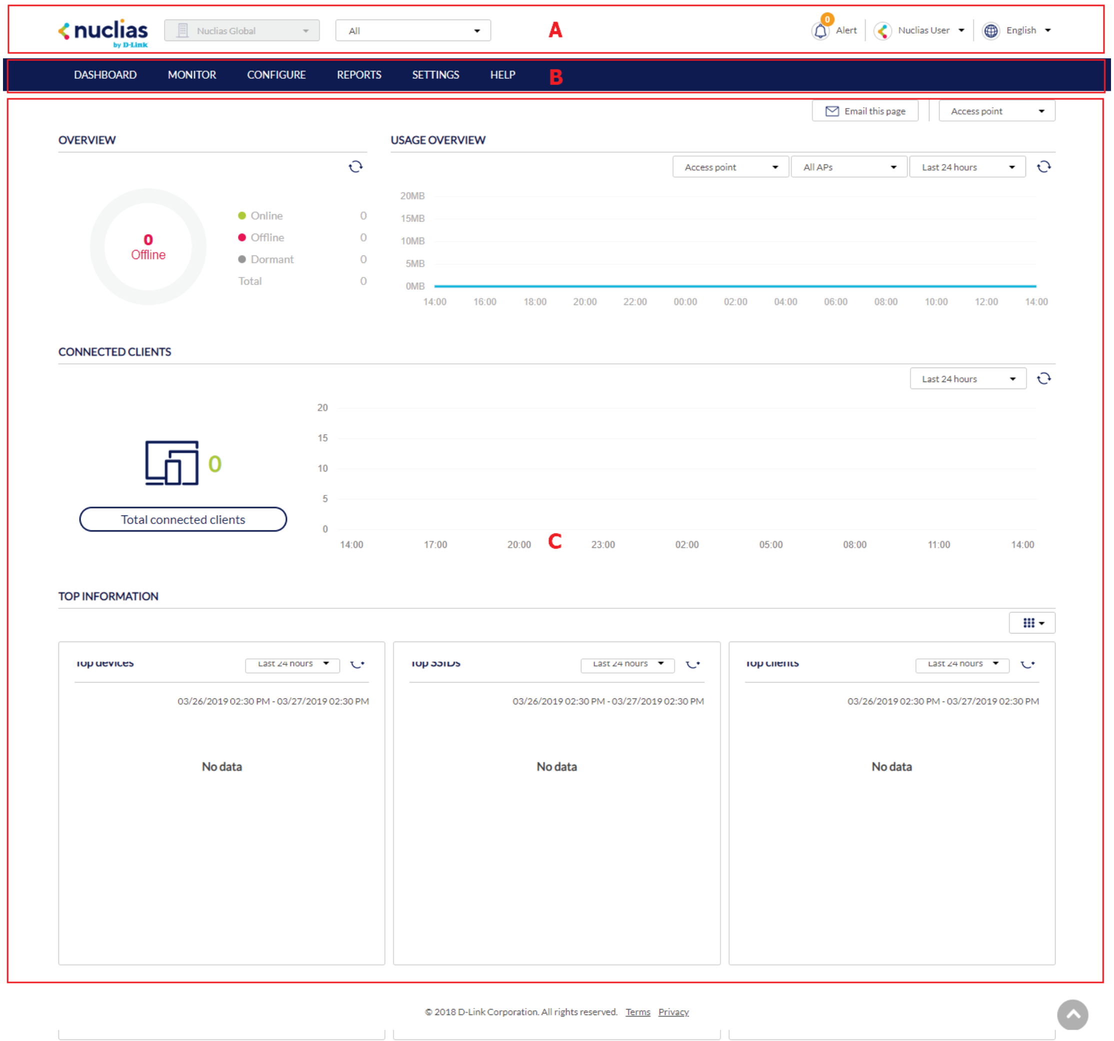
4.2 Logging Out of Nuclias

1. Click the user name in the top-right corner.
2. Click **Logout**.

   Note: Clicking **Logout** will immediately send the user back to the login page and will not prompt for confirmation.



5 Interface Overview



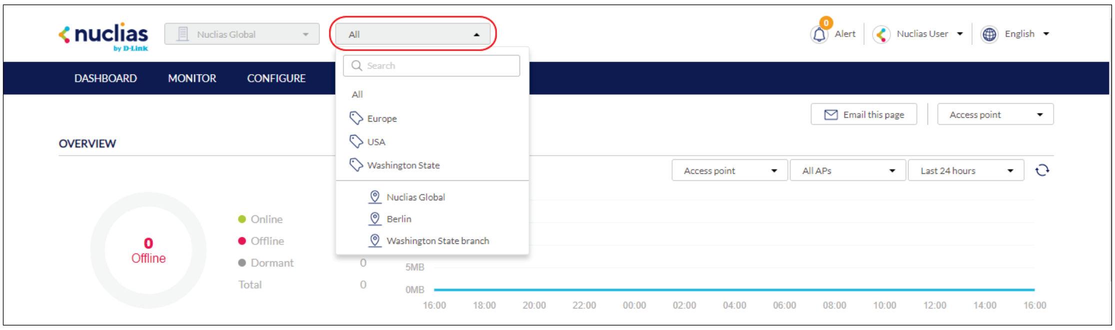
Section	Item	Description
A	**Global Toolbar**	Provides access to the organization and site selection menu as well as alerts, user account, and language menus.
B	**Management Toolbar**	Provides access to the various device management, report, and inventory sections.
C	**Workspace**	The interactive workspace to manage and configure through the Nuclias Portal. Information and options displayed in the workspace depend on the currently active management section.

5.1 Global Toolbar

5.1.1 Site Menu

The Site menu is used to select a Site or Site Tag within the selected organization, and may only contain selected sites, depending on the privilege of the account that you have logged in with. Site Tags and Sites are an easy way of grouping devices within an organization and allow for multiple devices to be configured more easily. Site Tags are marked by a tag icon, while Sites are marked by a single pin icon.

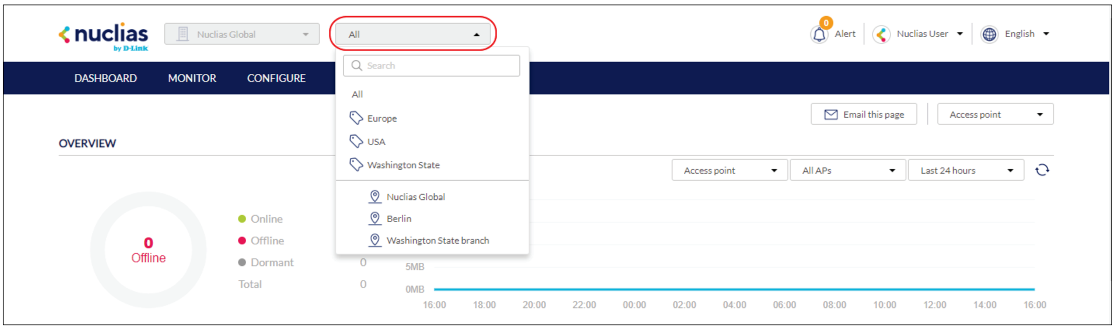
Note: For most configuration options, it is necessary to select a Site first.



5.1.1.1 Selecting a Site

By selecting a specific Site, users can view network activity, client information, and at-a-glances for the selected Site. Certain management features are also handled on the Site-level.

1. From the Global Toolbar, click the Site menu.



2. [**Optional**] Click a Site Tag to only show Sites associated with that Site Tag or click **All** to show all Sites.
3. Click the Site name.

   Note: Only information for that Site will be shown in the dashboard and management sections.

5.1.2 Account Menu

The account menu contains the User Profile and Logout options and can be reached by clicking the user name you have logged in with.

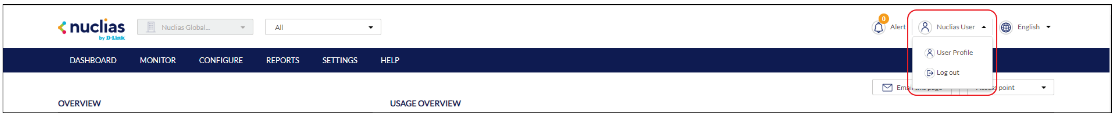
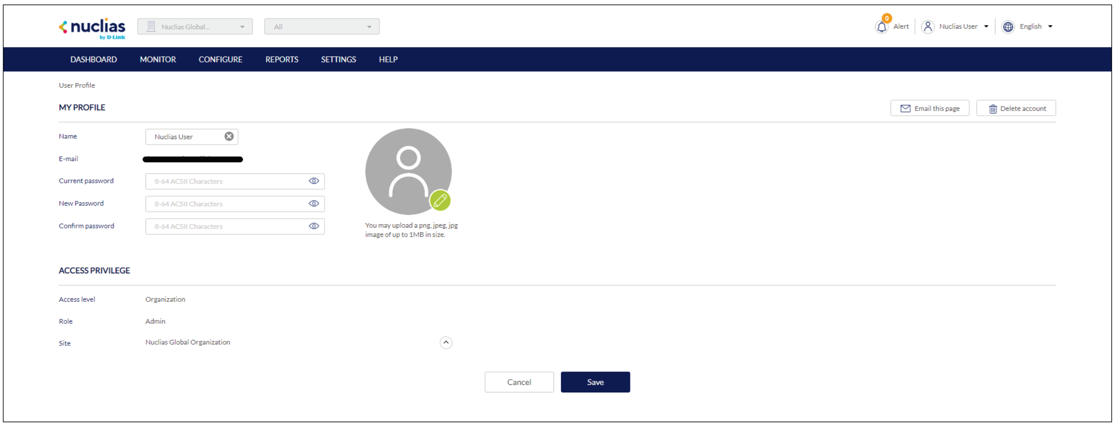


Figure 5-1

5.1.2.1 Editing a User Profile

The User Profile page is used to view the current user's profile and access privilege information. It can also be used to change the user's password and profile image.



MY PROFILE

Name: Nuclias User

E-mail: [redacted]

Current password: 8-64 ACSII Characters

New Password: 8-64 ACSII Characters

Confirm password: 8-64 ACSII Characters

You may upload a png, jpeg, jpg image of up to 1MB in size.

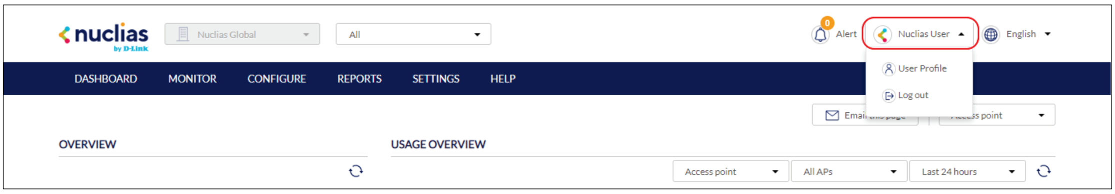
ACCESS PRIVILEGE

Access level: Organization

Role: Admin

Site: Nuclias Global Organization

1. From the Global Toolbar, click the Account menu.



2. Select **User Profile**.
3. Edit the user profile using one of the following actions:
    a. **Change user name**
        i. Click the user name in the **Name** field.
        ii. Enter a new name and press **Enter** or click outside of the field.
    b. **Change password**
        i. Enter your current password in the **Current Password** field.
        ii. Enter a new password in the **New Password** field.
        iii. Enter the new password again in the **Confirm Password** field.

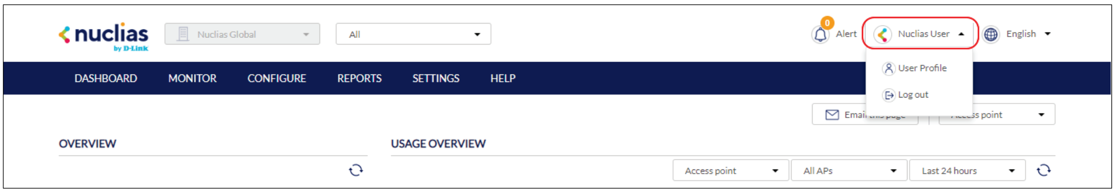
c. **Edit profile image**
    i. Click on the green **pencil icon** in the bottom-right corner of the profile image.
    ii. In the Upload Image window click **Browse** and navigate to the image you want to use.
    iii. Click **Save**.

d. **Email user information**
    i. Click the **Email this page** button to send your user information to your registered email address.

4. Click **Save**.

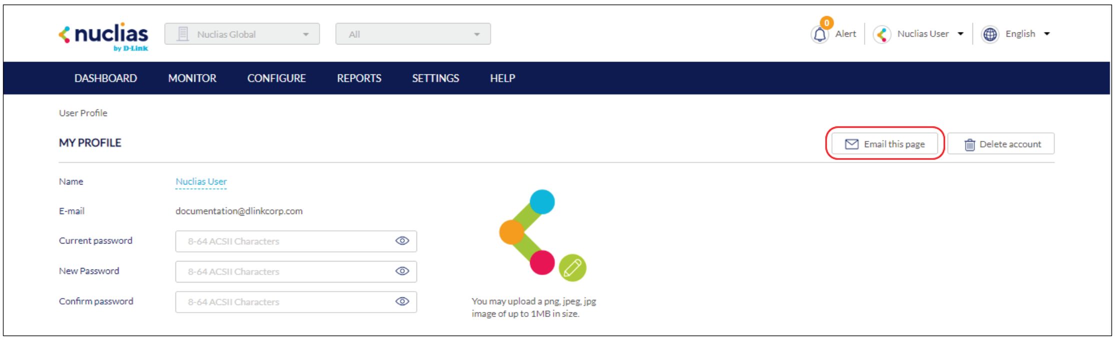
5.1.2.2 Sending A User Profile Snapshot by Email

1. From the Global Toolbar, click the Account menu.



2. Select **User Profile**.
3. Click **Email this page**.

   Note: This will immediately send a snapshot of the user profile page to the email address registered to this user account.



User Profile

MY PROFILE

Name Nuclias User

E-mail documentation@dlinkcorp.com

Current password 8-64 ACSII Characters

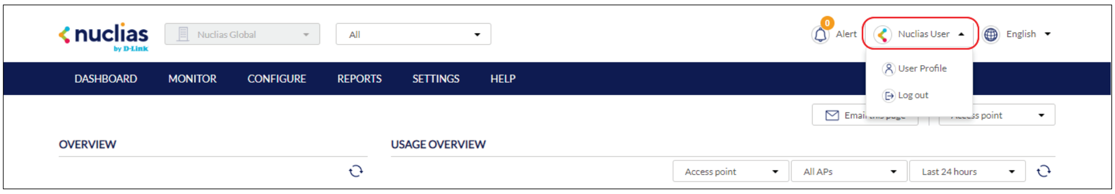
New Password 8-64 ACSII Characters

Confirm password 8-64 ACSII Characters

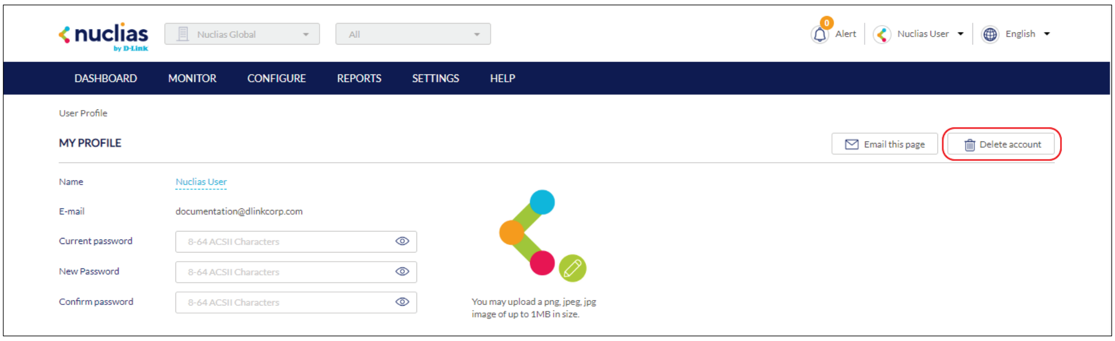
You may upload a png, jpeg, jpg image of up to 1MB in size.

5.1.2.3 Deleting a User Account

1. From the Global Toolbar, click the Account menu.



2. Select **User Profile**.
3. Click **Delete Account**.



User Profile

MY PROFILE

Name Nuclias User

E-mail documentation@dlinkcorp.com

Current password 8-64 ACSII Characters

New Password 8-64 ACSII Characters

Confirm password 8-64 ACSII Characters

You may upload a png, jpeg, jpg image of up to 1MB in size.

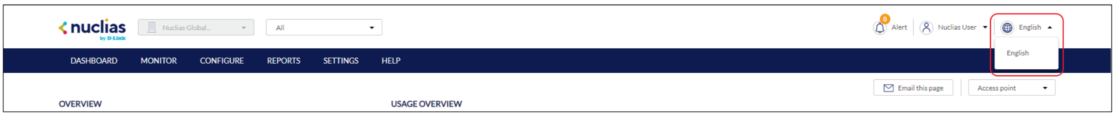
4. Enter your account password and click **Save**.

   Note: Deleting an account will remove all data associated with this user. This is permanent and cannot be undone.

5.1.3 Language Menu

5.1.3.1 Changing the Portal Language

The language menu allows users to change the display language of the Portal interface.



1. From the dashboard, click the **display language** in the top-right.
2. Select a language from the drop-down menu.

   Note: Selecting another language will immediately change the portal display language into the selected language. Currently only English is supported.

5.2 Management Toolbar

From the Management toolbar, users can access the various management features of the Nuclias Cloud platform, including Profiles and device management, device and network reports, account management, and the device and license inventory.

Dashboard	The Dashboard offers users a real time overview of the status of the network including device and user activity and performance. Refer to the **Dashboard section on page 22** for more information.
Monitor	The Monitor section grants access to detailed device, client, and event logs as well as the interactive map and floor plan tools. Refer to the **Monitor section on page 26** for more information.
Configure	The Configure section grants access to the main configuration section including Profiles and individual device settings. Refer to the **Configure section on page 38** for more information.
Reports	The Reports section grants access to detailed reports for changes on the platform, access point and client activity,

	network alerts, and license reports. Refer to the **Reports section on page 82** for more information.
Settings	The Settings section grants access to organization and user management, the device and license inventory, and firmware management. Refer to the **Settings section on page 87** for more information.
Help	The Help section offers users a platform to submit support tickets and provide feedback. Refer to the **Help section on page 107** for more information.

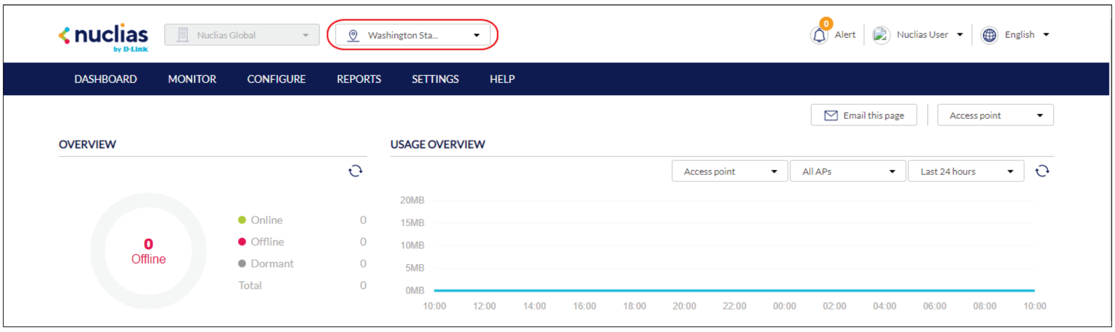
6 Dashboard

The Dashboard page is the default window that is displayed after logging into the Nuclias Portal interface. It can also be reached by clicking the **Dashboard** tab in the tool bar. It provides an overview of the devices, connected clients, and SSID activity for the selected organization and Site. It is also possible to email a dashboard report, access the map and organization view from this window by clicking the corresponding icons in the top right of the page.

6.1 Customizing the Overview For Access Points

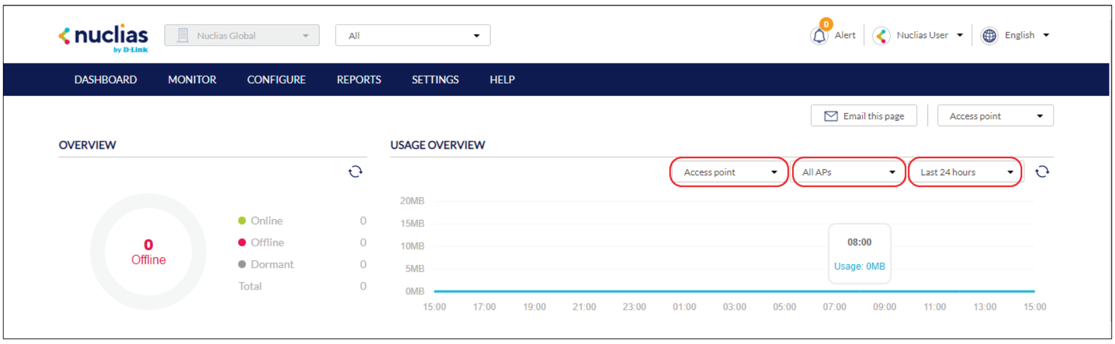
1. Navigate to the **Dashboard** page
2. Select a Site from the Site menu.

   Note: Selecting a Site will only show network and device information for the selected Site. Select **All** to show network, client, and device information for all Sites.

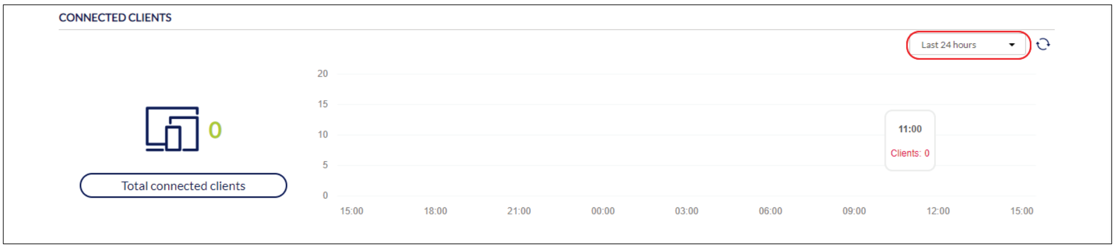


3. In the **Usage Overview** section, select Access Point or SSID, the access point(s) or

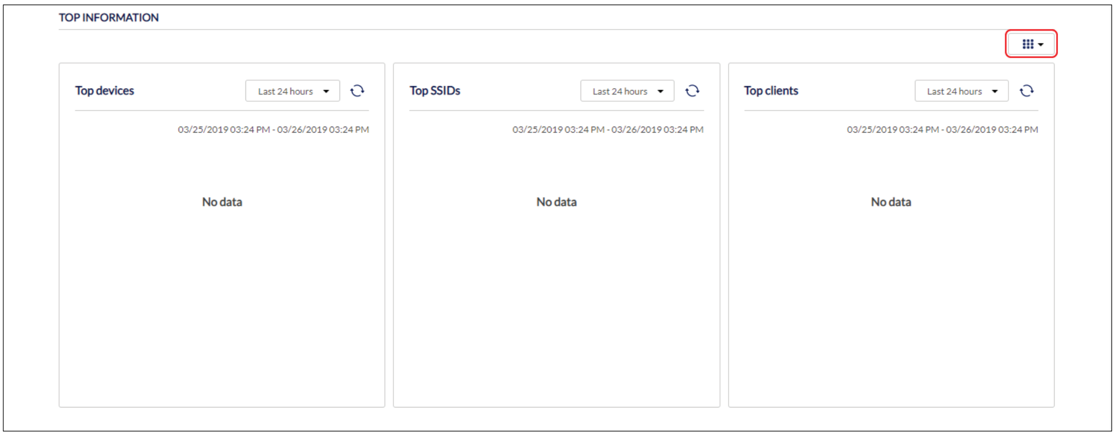
SSID(s), and the time frame from the drop-down menus.



4. In the **Connected Clients** section, select a time frame from the drop-down menu.

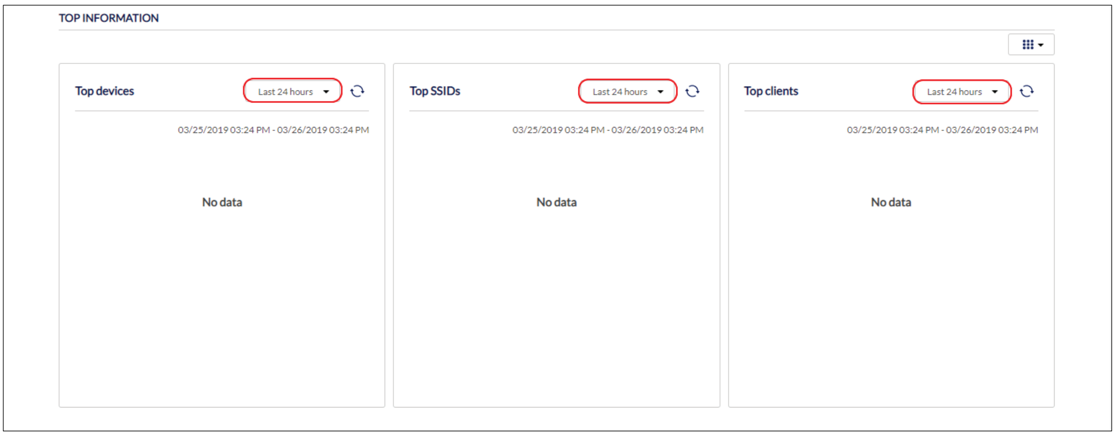


5. In the **Top Information section**, click the filter selection in the top-right.


TOP INFORMATION
Top devices
Last 24 hours
03/25/2019 03:24 PM - 03/26/2019 03:24 PM
No data
Top SSIDs
Last 24 hours
03/25/2019 03:24 PM - 03/26/2019 03:24 PM
No data
Top clients
Last 24 hours
03/25/2019 03:24 PM - 03/26/2019 03:24 PM
No data

6. Check the information parameters to display the corresponding top information in the overview window.

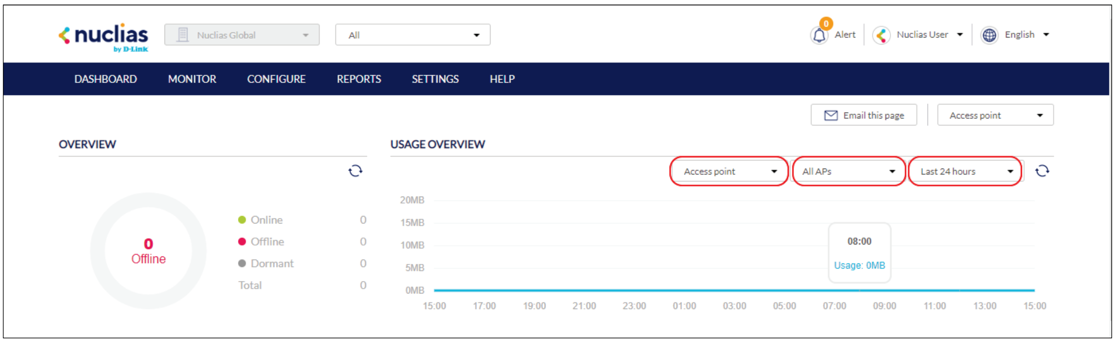
7. In the **Top Information** section, select a time frame from the drop-down menu for each enabled section.


TOP INFORMATION
Top devices
Last 24 hours
03/25/2019 03:24 PM - 03/26/2019 03:24 PM
No data
Top SSIDs
Last 24 hours
03/25/2019 03:24 PM - 03/26/2019 03:24 PM
No data
Top clients
Last 24 hours
03/25/2019 03:24 PM - 03/26/2019 03:24 PM
No data

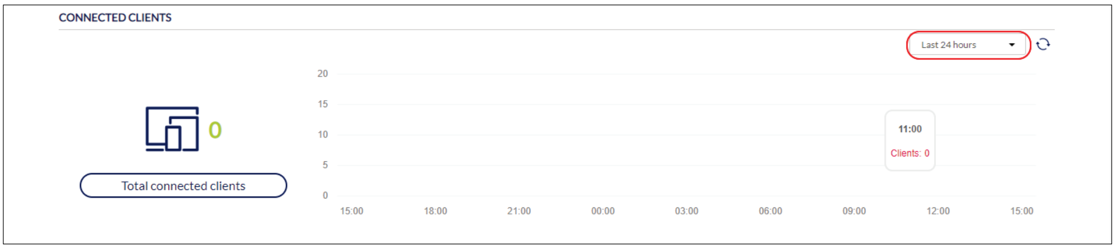
6.2 Sending A Dashboard Snapshot by Email

Users can create and send a snapshot of the dashboard window by email.

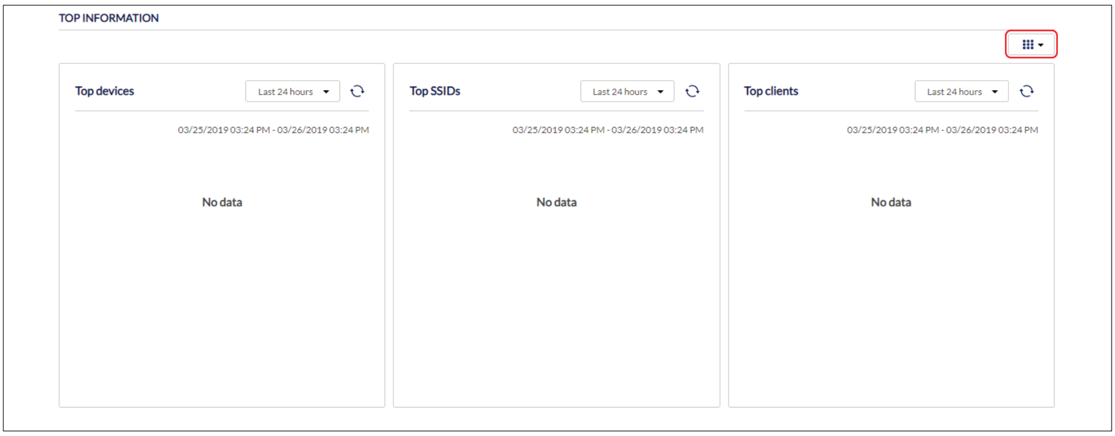
1. Navigate to the **Dashboard** page.
2. In the **Usage Overview** section, select Access Point or SSID, the access point(s) or SSID(s), and the time frame from the corresponding drop-down menus.



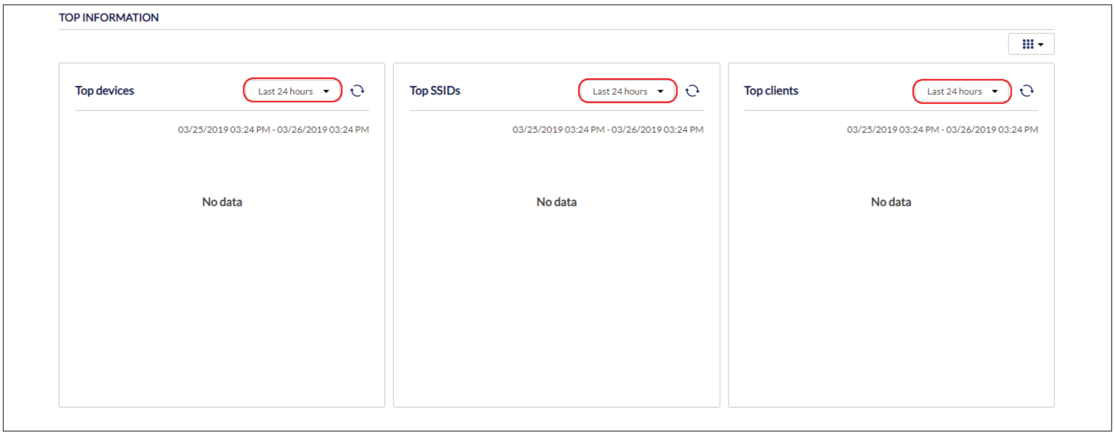
3. In the **Connected Clients** section, select a time frame from the drop-down menu.



4. In the **Top Information section**, click the filter selection in the top-right.


TOP INFORMATION
Top devices
Last 24 hours
03/25/2019 03:24 PM - 03/26/2019 03:24 PM
No data
Top SSIDs
Last 24 hours
03/25/2019 03:24 PM - 03/26/2019 03:24 PM
No data
Top clients
Last 24 hours
03/25/2019 03:24 PM - 03/26/2019 03:24 PM
No data

5. Check the information parameters to display the corresponding top information in the overview window.
6. In the **Top Information** section, select a time frame from the drop-down menu for each enabled section.


TOP INFORMATION
Top devices
Last 24 hours
03/25/2019 03:24 PM - 03/26/2019 03:24 PM
No data
Top SSIDs
Last 24 hours
03/25/2019 03:24 PM - 03/26/2019 03:24 PM
No data
Top clients
Last 24 hours
03/25/2019 03:24 PM - 03/26/2019 03:24 PM
No data

7. Click **Email this page** in the top-right.
8. In the Email report window, enter the email address of the recipient(s).

   Note: Up to 10 recipients can be added, separated by “,”.
9. Click **Send email**.

7 Monitor

From the Monitor tab, users can view detailed device monitoring reports and access the map and floor plan windows.

Access Point	The Access Point section provides detailed logs for access point devices, connected clients, and events. Refer to the **Access Point section on page 26** for more information.
Map	The Map section provides users with an interactive map that offers a geographical overview of the organization's Sites. Refer to the **Map section on page 29** for more information.
Floor Plans	The Floor Plans section allows users to create, edit, manage, and delete floor plans. Refer to the **Floor Plans section on page 32** for more information.

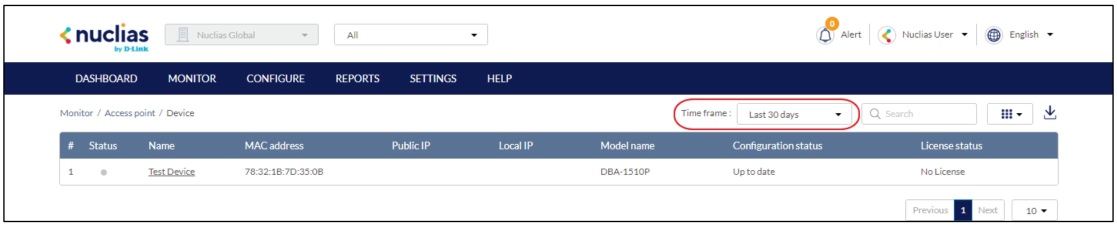
7.1 Access Point

7.1.1 Devices

From the Devices window, users can consult a detailed log of events occurring on the network. Users can also filter events using specific event filter parameters, including event type and time period.

7.1.1.1 Customizing the Device Monitor Overview

1. Navigate to the **Monitor > Access Point > Device** page.
2. Select a time frame from the time frame drop-down menu.

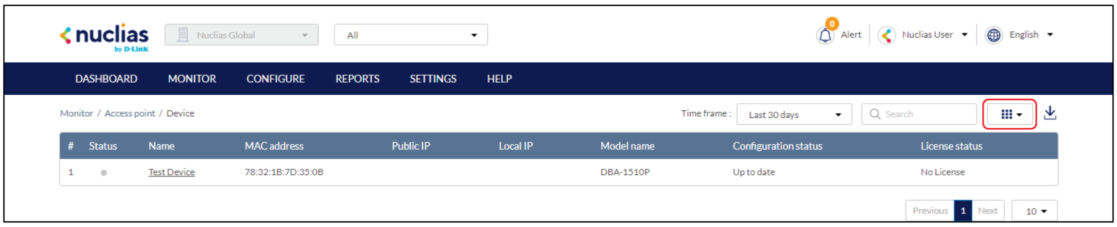


Monitor / Access point / Device

Time frame : Last 30 days

#	Status	Name	MAC address	Public IP	Local IP	Model name	Configuration status	License status
1	●	Test Device	78:32:1B:7D:35:0B			DBA-1510P	Up to date	No License

3. Click the filter parameter icon.



Monitor / Access point / Device

Time frame : Last 30 days

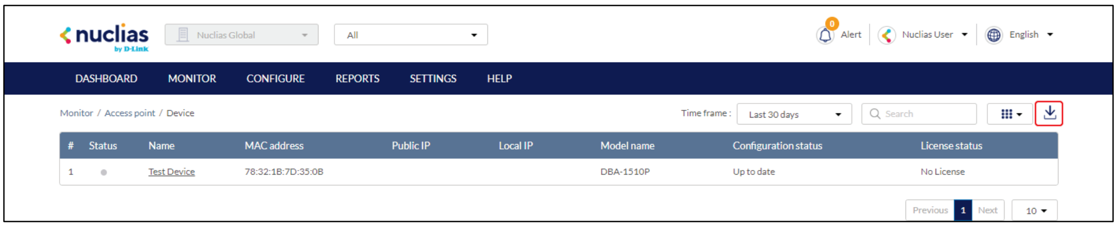
#	Status	Name	MAC address	Public IP	Local IP	Model name	Configuration status	License status
1	●	Test Device	78:32:1B:7D:35:0B			DBA-1510P	Up to date	No License

4. Click the checkbox next to the parameters to display them in the overview.

   Note: All checked parameters will automatically appear.

7.1.1.2 Downloading Device Monitoring Logs

1. Navigate to the **Monitor > Access Point > Device** page.
2. From the device list, click the **Download** icon in the top-right.



Monitor / Access point / Device

Time frame : Last 30 days

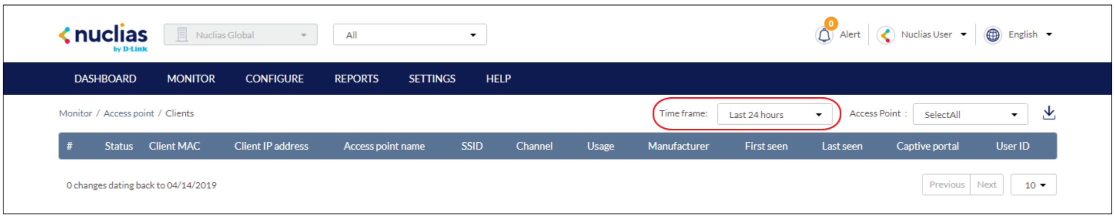
#	Status	Name	MAC address	Public IP	Local IP	Model name	Configuration status	License status
1	●	Test Device	78:32:1B:7D:35:0B			DBA-1510P	Up to date	No License

7.1.2 Clients

From the Clients window, users can consult a detailed overview of all currently registered devices with additional information including status, clients, and general settings.

7.1.2.1 Customizing the Client Monitor Overview

1. Navigate to the **Monitor > Access Point > Clients** page.
2. Select a time frame from the time frame drop-down menu.



Monitor / Access point / Clients

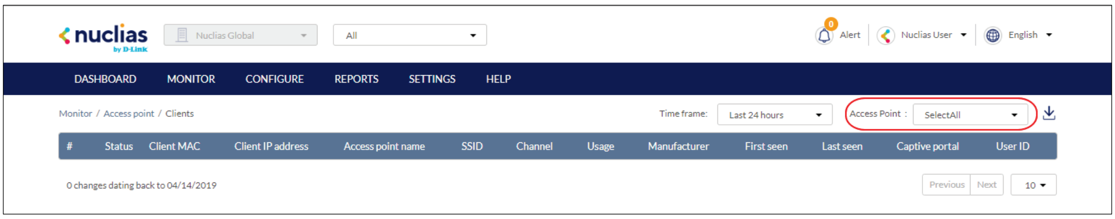
Time frame: Last 24 hours

Access Point : SelectAll

#	Status	Client MAC	Client IP address	Access point name	SSID	Channel	Usage	Manufacturer	First seen	Last seen	Captive portal	User ID

0 changes dating back to 04/14/2019

3. Select an access point from the access point drop-down menu.



Time frame: Last 24 hours

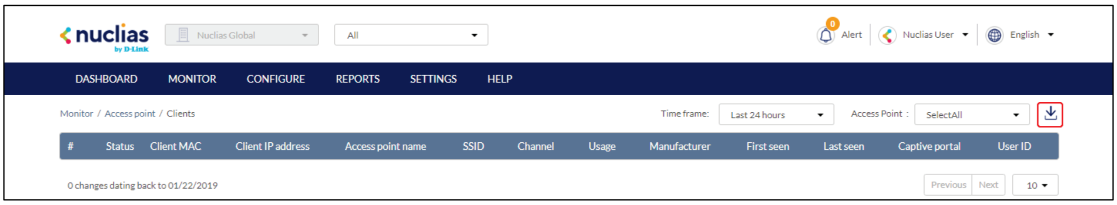
Access Point : SelectAll

#	Status	Client MAC	Client IP address	Access point name	SSID	Channel	Usage	Manufacturer	First seen	Last seen	Captive portal	User ID

0 changes dating back to 04/14/2019

7.1.2.2 Downloading Client Monitoring Logs

1. Navigate to the **Monitor > Access Point > Clients** page.
2. From the device list, click the **Download** icon in the top-right.



Time frame: Last 24 hours

Access Point : SelectAll

#	Status	Client MAC	Client IP address	Access point name	SSID	Channel	Usage	Manufacturer	First seen	Last seen	Captive portal	User ID

0 changes dating back to 01/22/2019

7.1.3 Event Logs

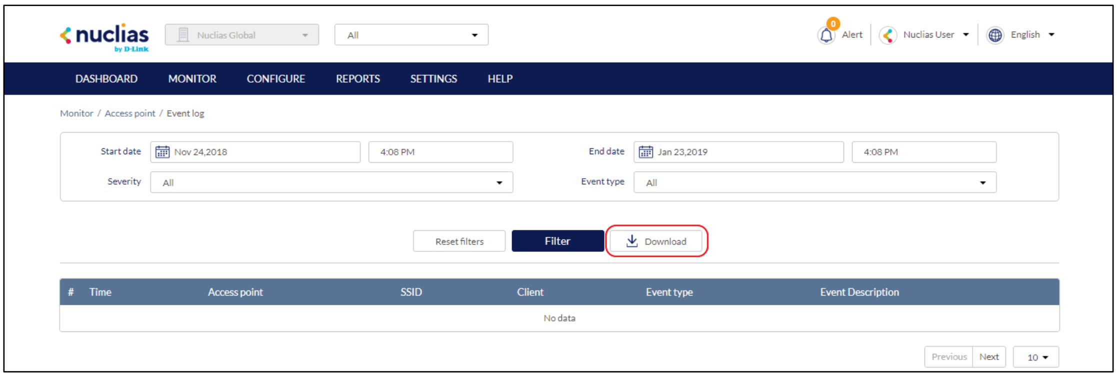
From the Events Logs window, users can consult a detailed log of events occurring on the network. Users can define event filter parameters, including event type and time period.

7.1.3.1 Filtering Event Log Parameters

1. Navigate to the **Monitor > Access Point > Event Logs** page.
2. In the Start Date field, click the calendar icon to select a date and enter a time of day to define the event log starting time.
3. In the End date field, click the calendar icon to select a date and enter a time of day to define the event log ending time.
4. Click the Severity drop-down menu and select the severity levels to display.
5. Click the Event type drop-down menu and select the event types to display.
6. Click **Filter** to display all events matching the defined parameters.
7. [**Optional**] Click **Reset filters** to reset all currently set parameters.

7.1.3.2 Downloading Event Logs

1. Navigate to the **Monitor > Access Point > Event Logs** page.
2. From the event log list, click **Download** icon in the center.



Start date Nov 24,2018 4:08 PM
End date Jan 23,2019 4:08 PM
Severity All
Event type All

#	Time	Access point	SSID	Client	Event type	Event Description
No data						

7.2 Map

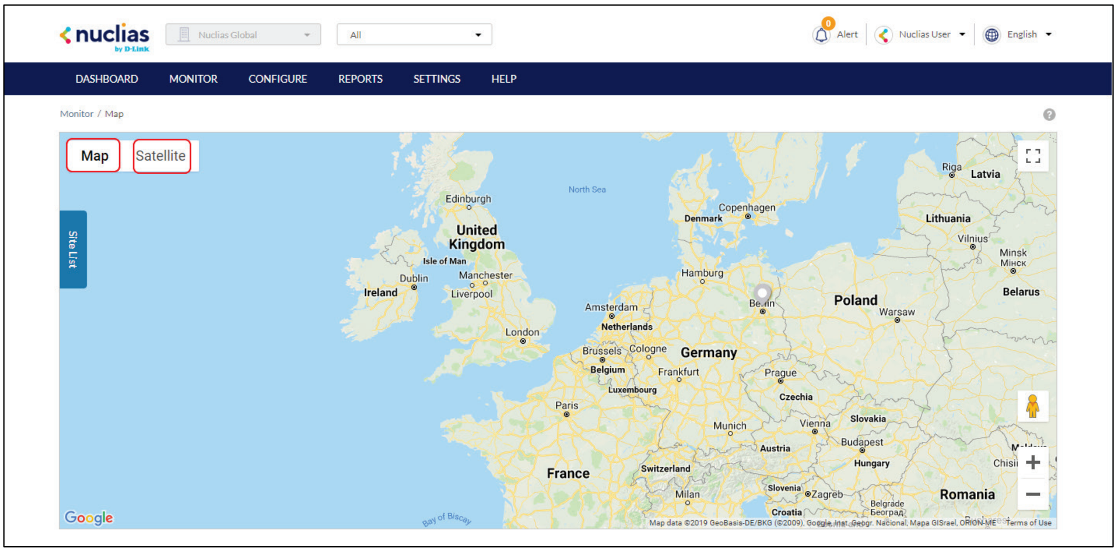
From the Map window, users can consult a geographical overview of the organization’s Sites in the form of an interactive world map.

Note: Sites must be linked to a valid address in order to show up on the map.

7.2.1 Navigating the Map

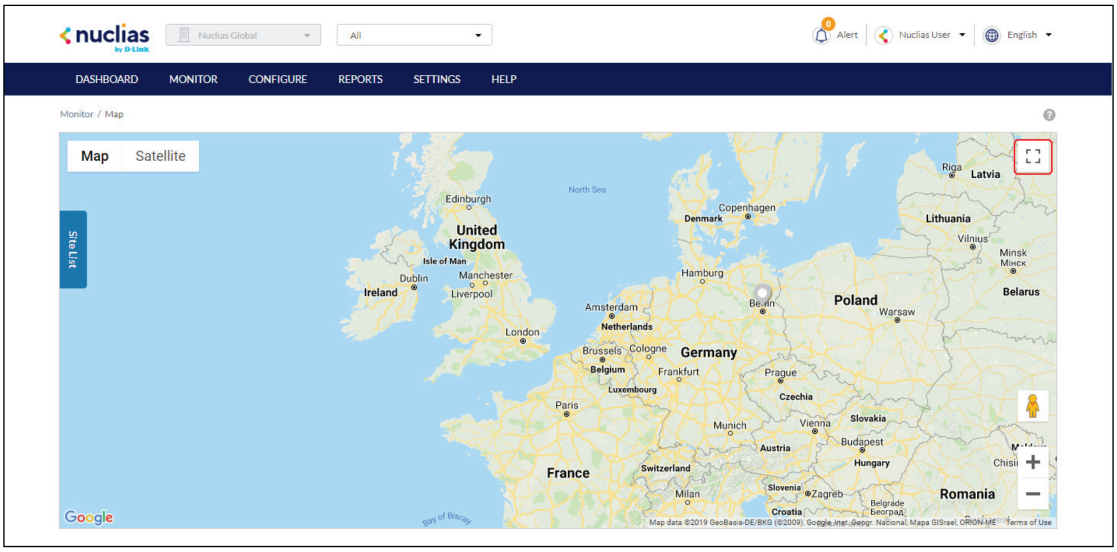
From the interactive map, users can view a geographical representation of the Site’s physical location as well as view basic information and the current status of the Site.

1. Navigate to the **Monitor > Map** page.
2. Click **Map** or **Satellite** in the top-left corner of the map to switch between the street map and satellite image map.

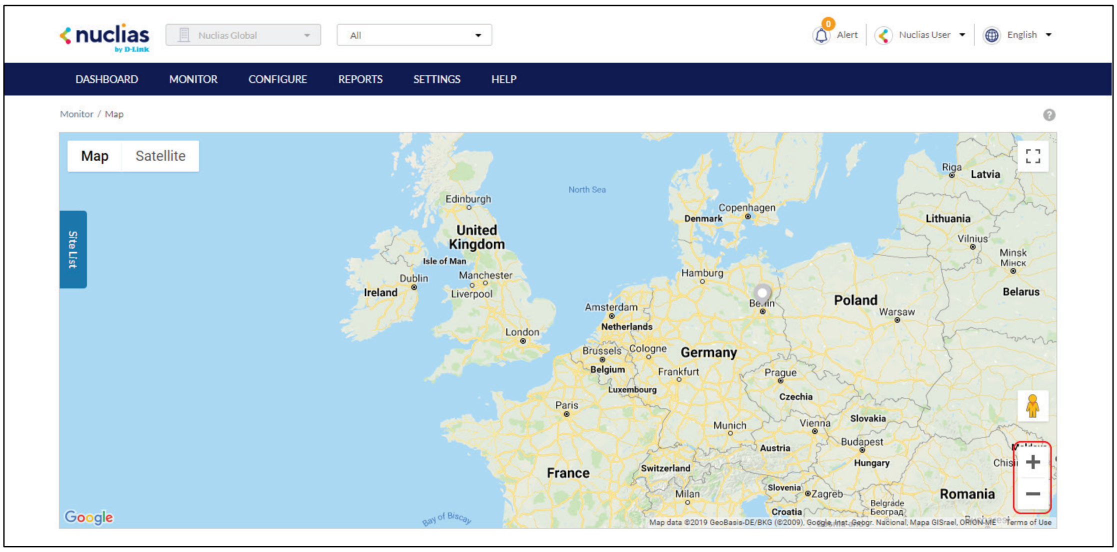


3. Click the expand icon in the top-right corner of the map to toggle full-screen mode.

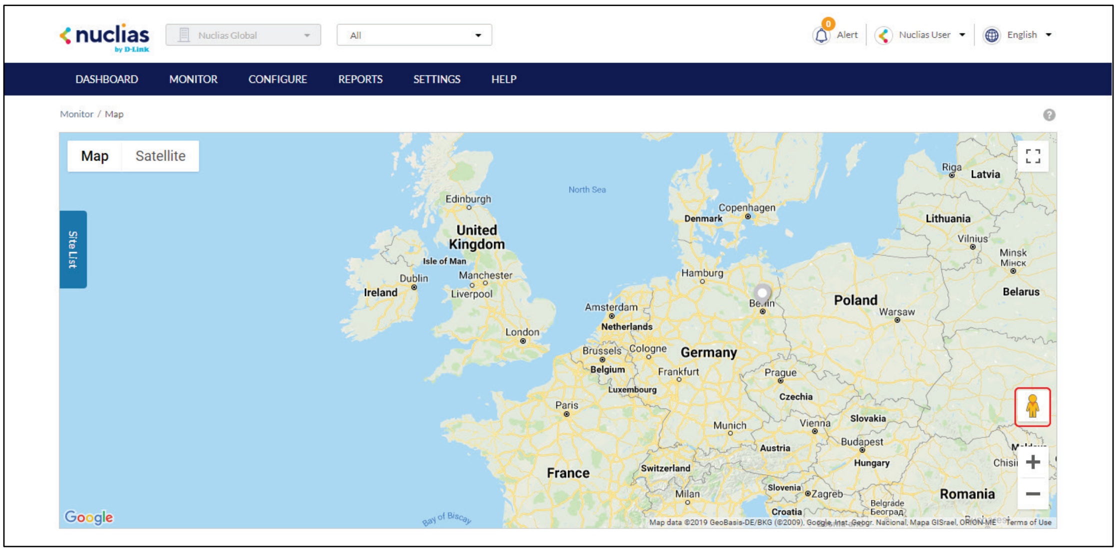
   Note: Click the expand icon again to return to windowed mode.



4. Click and drag the left-mouse button on the map surface to move around on the map.
5. Click the **+** and **–** buttons in the bottom-right corner of the map to zoom in and out on the map. Alternatively, hold **Ctrl** and scroll the mouse wheel up and down to zoom in and out.



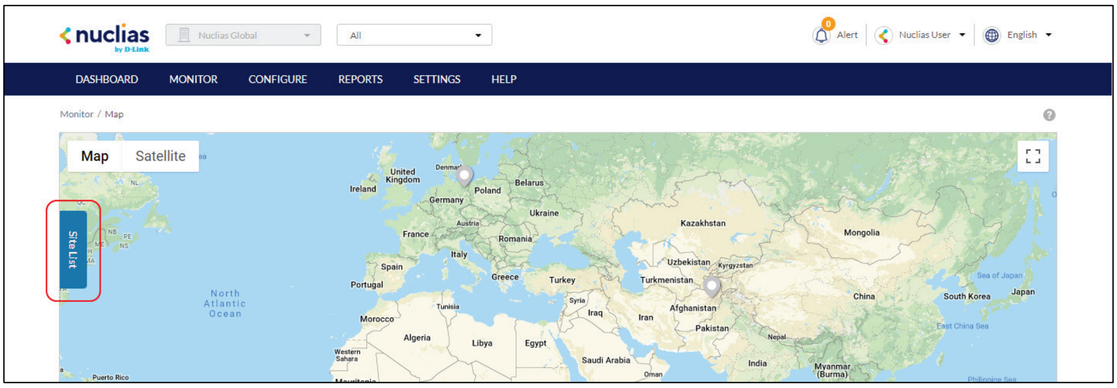
6. Drag and drop the Pegman icon anywhere on the map to open the street view of that location.
   Note: When in street view, click the return arrow to return to the map view.



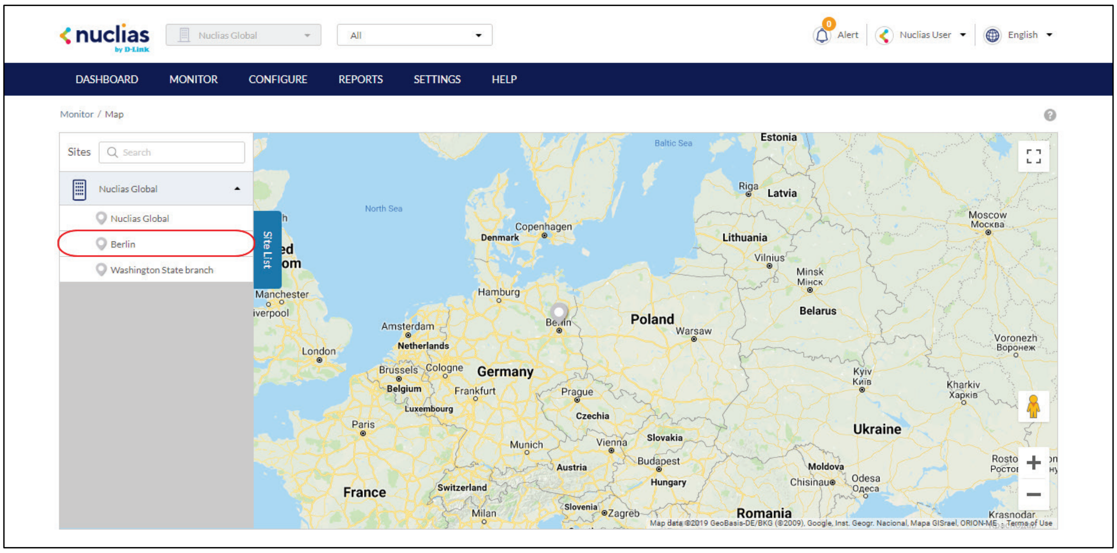
7.2.2 Navigating Sites on the Map Using the Site List

From the interactive map, users can view a geographical representation of the Site's physical location as well as view basic information and the current status of the Site.

1. Navigate to the **Monitor > Map** page.
2. Click **Site List** on the left-hand side of the map.



3. In the Site List, click the organization name to expand the list of Sites under the organization.
4. [**Optional**] Click the search field and enter the Site name.
5. From the expanded Site list, click the Site name. This will automatically navigate to the Site's location on the map.



6. Click the Site icon on the map to view basic information.
7. [**Optional**] Click the Site name in the Site window to open the Dashboard view for that Site.

7.3 Floor Plans

Floor plans offer organizations an easy way to visually represent the location of each device within the organization. Floor plans are managed per Site, and each Site can have multiple floor plans.

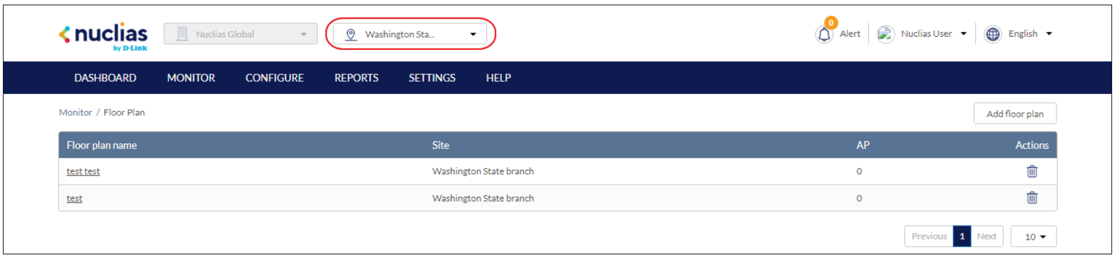
7.3.1 Adding Floor Plan

Users can create floor plans to have a visual overview of device placement.

Note: Floor plans are created for individual Sites within the organization.

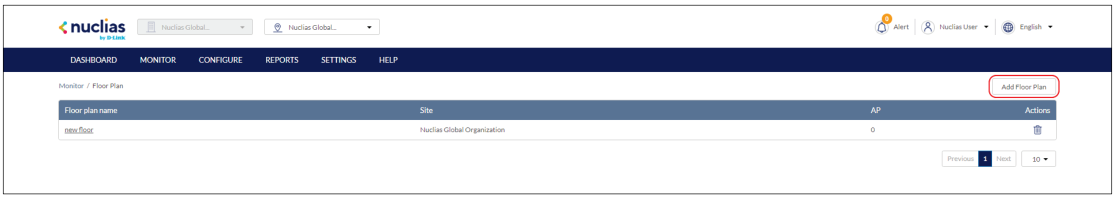
1. Navigate to the **Monitor > Floor plans** page.
2. Select a Site from the Site menu.

   Note: Selecting a Site will only show floor plans created for the selected Site. Select **All** to show all floor plans for all Sites.



Floor plan name	Site	AP	Actions
test test	Washington State branch	0	
test	Washington State branch	0	

3. From the floor plan list, click **Add Floor Plan**.



Floor plan name	Site	AP	Actions
new floor	Nuclias Global Organization	0	🗑

4. Select the Site to associate this floor plan with.
5. Click **OK**.

7.3.1 Editing Floor Plan

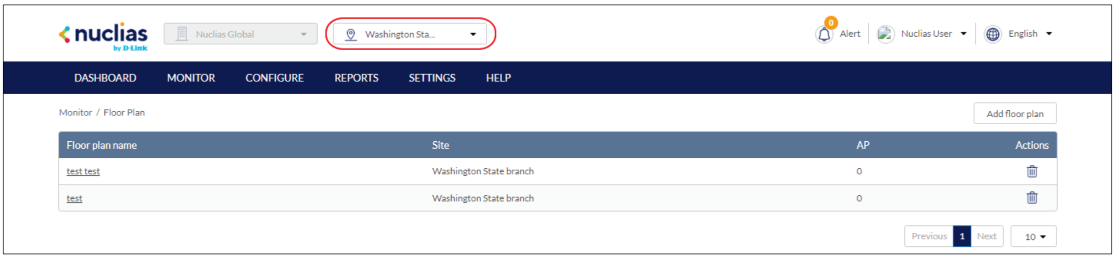
Users can add and remove device icons onto floor plans for a visual overview of the device placement, edit the floor plan name, and upload a custom floor plan image.

7.3.1.1 Adding Devices to a Floor Plan

Devices can be dragged onto the floor plan to create a visual representation of the placement of the devices within the organization.

1. Navigate to the **Monitor > Floor plans** page.
2. Select a Site from the Site menu.

   Note: Selecting a Site will only show floor plans created for the selected Site. Select **All** to show all floor plans for all Sites.



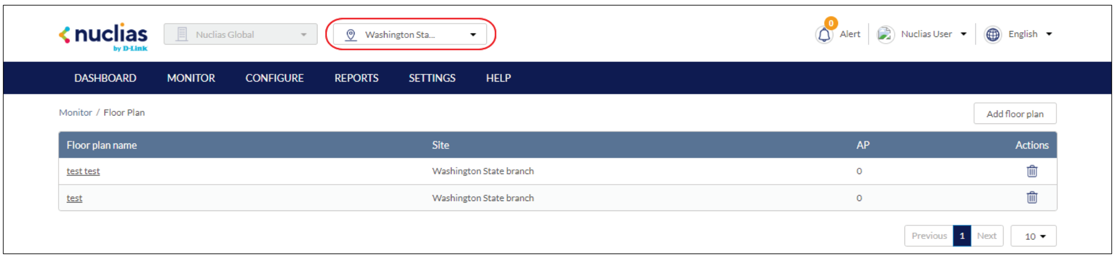
Floor plan name	Site	AP	Actions
test test	Washington State branch	0	🗑
test	Washington State branch	0	🗑

3. From the floor plan list click on the floor plan name.
4. Click and drag a device from the **Unplaced Devices** list onto the floor plan to place it on the floor plan.
5. Click **Save**.

7.3.1.2 Removing Devices from a Floor Plan

1. Navigate to the **Monitor > Floor plans** page.
2. Select a Site from the Site menu.

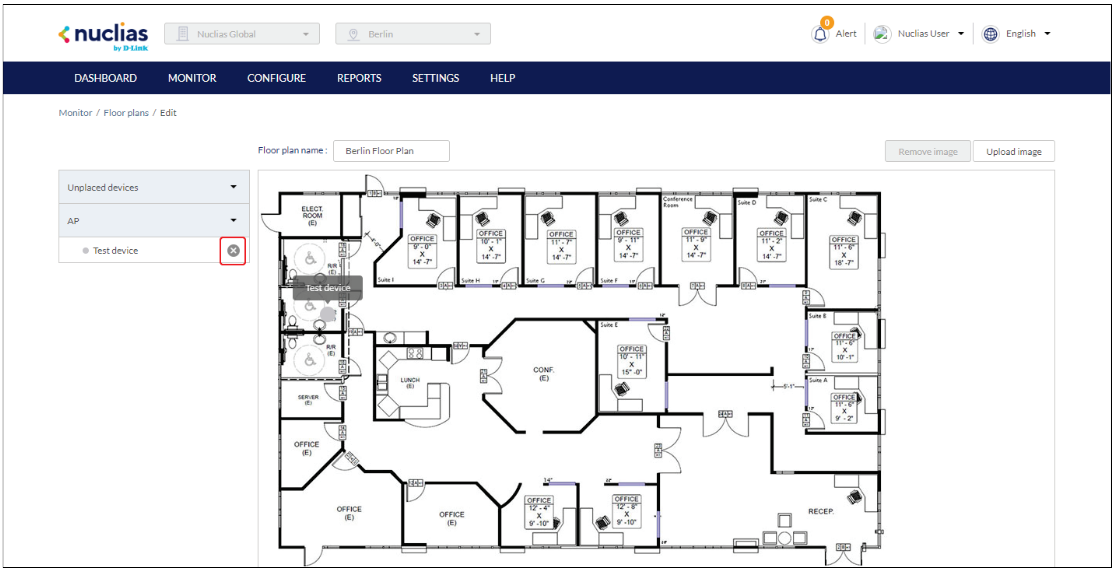
Note: Selecting a Site will only show floor plans created for the selected Site. Select **All** to show all floor plans for all Sites.



Floor plan name	Site	AP	Actions
test test	Washington State branch	0	🗑
test	Washington State branch	0	🗑

3. From the floor plan list, click on the floor plan name.
4. Click the **X** icon next to the device in the **AP** list that you wish to remove.

   Note: Devices removed from the floor plan will automatically be moved to the **Unplaced Devices** list.



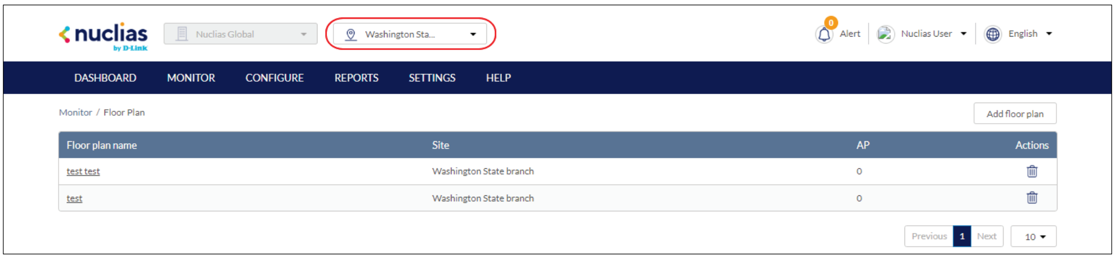
Floor plan name : Berlin Floor Plan

5. Click **Save**.

7.3.1.3 Editing a Floor Plan Name

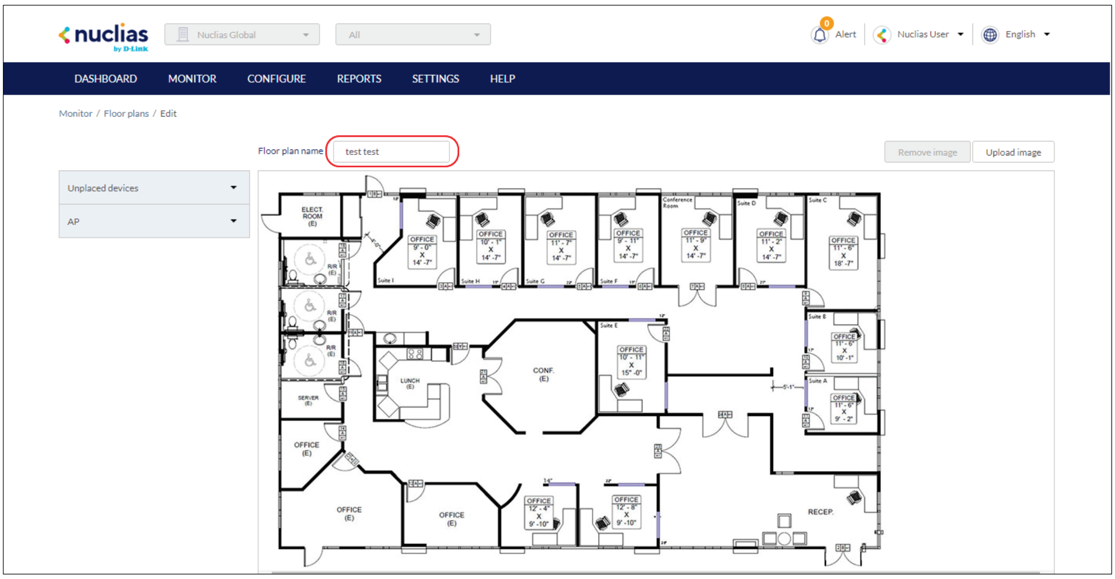
1. Navigate to the **Monitor > Floor plans** page.
2. Select a Site from the Site menu.

   Note: Selecting a Site will only show floor plans created for the selected Site. Select **All** to show all floor plans for all Sites.



Floor plan name	Site	AP	Actions
test test	Washington State branch	0	🗑
test	Washington State branch	0	🗑

3. From the floor plan list, click on the floor plan name.
4. Click the floor plan name in the Floor Plan Name field.



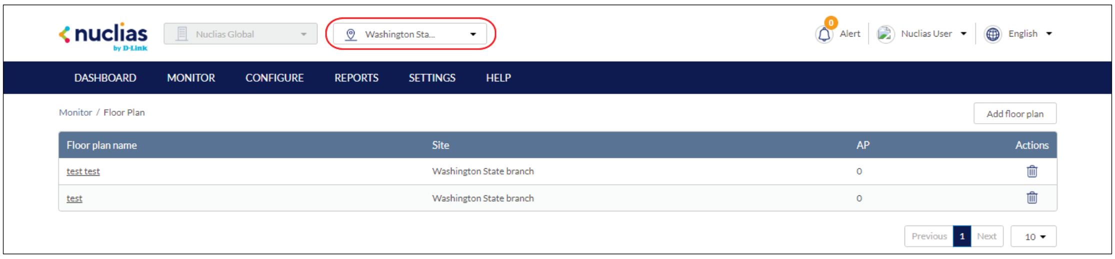
Floor plan name: test test

5. Enter a new name and press Enter or click outside of the field.
6. Click **Save**.

7.3.1.4 Adding a Custom Floor Plan Image

1. Navigate to the **Monitor > Floor plans** page.
2. Select a Site from the Site menu.

   Note: Selecting a Site will only show floor plans created for the selected Site. Select **All** to show all floor plans for all Sites.



Floor plan name	Site	AP	Actions
test test	Washington State branch	0	🗑
test	Washington State branch	0	🗑

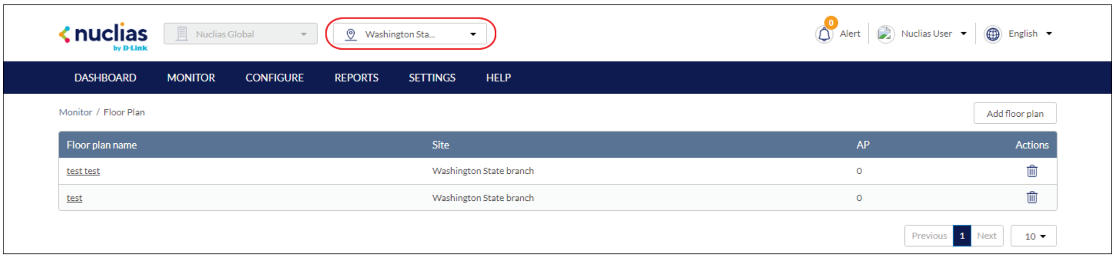
3. From the floor plan list, click on the floor plan name.
4. On the floor plan page, click **Upload image**.
5. In the Upload Image window click **Browse** and navigate to the floor plan image you want to use.
6. Click **Upload.**
7. Click **Save**.

7.3.1.5 Removing a Custom Floor Plan

Image

1. Navigate to the **Monitor > Floor plans** page.
2. Select a Site from the Site menu.

   Note: Selecting a Site will only show floor plans created for the selected Site. Select **All** to show all floor plans for all Sites.



Floor plan name	Site	AP	Actions
test test	Washington State branch	0	🗑
test	Washington State branch	0	🗑

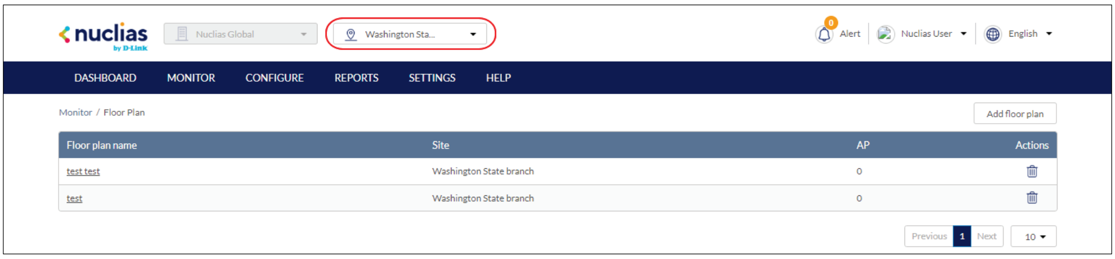
3. From the floor plan list, click on the floor plan name.
4. On the floor plan page, click **Remove image**.
5. When prompted to confirm, click **Delete**.

   Note: Deleting a custom image will restore the default floor plan image.
6. Click **Save**.

7.3.2 Deleting a Floor Plan

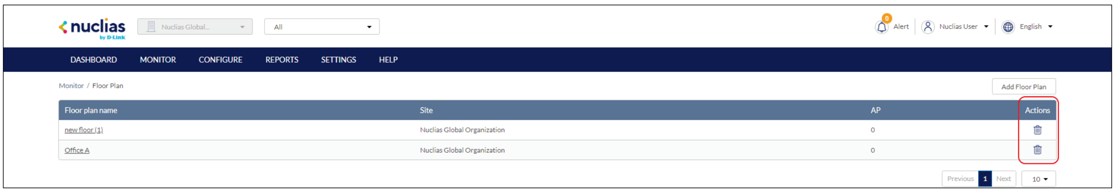
1. Navigate to the **Monitor > Floor plans** page.
2. Select a Site from the Site menu.

   Note: Selecting a Site will only show floor plans created for the selected Site. Select **All** to show all floor plans for all Sites.



Floor plan name	Site	AP	Actions
test test	Washington State branch	0	🗑
test	Washington State branch	0	🗑

3. From the floor plan list, click the trash can icon under the Actions column of the floor plan you wish to delete.



Floor plan name	Site	AP	Actions
new floor (1)	Nuclias Global Organization	0	🗑
Office A	Nuclias Global Organization	0	🗑

4. When prompted to confirm, click **Yes**.

8 Configure – Access Point

From the Configure section, users can manage Profiles and devices for the organization. The following sections provide more detailed information about Profile and device management respectively.

Profiles	From the Profiles section, users can create new and edit existing profiles, add a single device or bulk import a group of devices, and apply profile configuration settings to associated devices. Refer to the **Profiles section on page 39** for more information.
Devices	From the Devices section, users can add a single device, or bulk import a group of devices, and configure individual device settings. Refer to the **Devices section on page 61** for more information.
IP ACLs	From the IP ACL section, users can create, manage, and delete IP access control lists used to manage user network access based on their IP address. Refer to the **IP ACLs section on page 70** for more information.
MAC ACLs	From the MAC ACL section, users can create, manage, and delete MAC access control lists used to manage user network access based on their device's MAC address or through remote RADIUS server authentication. Refer to the **MAC ACLs section on page 73** for more information.
Local Authentication	From the Local Authentication section, users can create, manage, and delete local user account databases that are used as a user authentication method in Wi-Fi captive portal pages. Refer to the **Local Authentication section on page 76** for more information.

8.1 Profiles

8.1.1 Creating a Profile

Profiles are a set of general configuration settings that can be swiftly and easily applied to all devices associated with the Profile so all devices are configured identically as a group. Within each profile, users can configure SSID and wireless settings, set up landing and captive portal pages, and configure general settings.

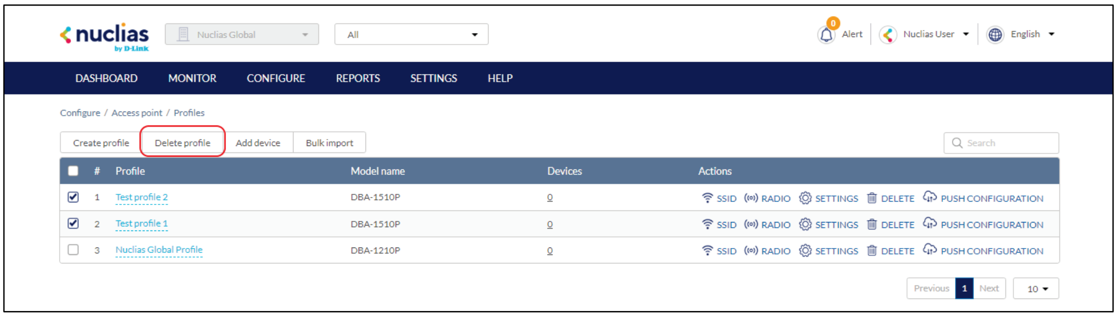
1. Navigate to the **Configure > Access Point > Profiles** page.
2. Click **Create Profile**.
3. Enter a name for the Profile and choose the device model.
   Note: The Profile can only be used for the selected device model type.
4. [**Optional**] Select **Clone from exist profile** and choose a Profile from the drop-down menu to clone an existing Profile.
5. Click **Create Profile**.

8.1.2 Deleting a Profile

1. Navigate to the **Configure > Access Point > Profiles** page.
2. From the Profile list, click **Delete** under the Actions column of the Profile you wish to delete.
3. When prompted to confirm, click **Yes**.

8.1.3 Deleting Multiple Profiles

1. Navigate to the **Configure > Access Point > Profiles** page.
2. Click the checkbox next to the Profiles you wish to delete.
3. Click **Delete profile**.



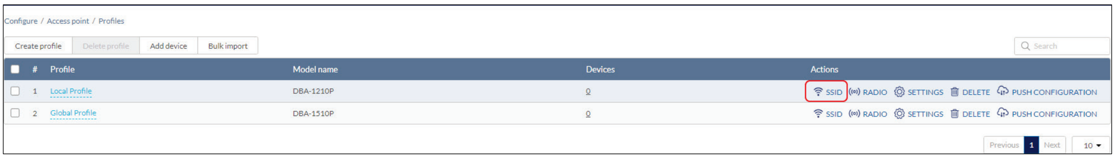
☐	#	Profile	Model name	Devices	Actions
☑	1	Test profile 2	DBA-1510P	0	SSID RADIO SETTINGS DELETE PUSH CONFIGURATION
☑	2	Test profile 1	DBA-1510P	0	SSID RADIO SETTINGS DELETE PUSH CONFIGURATION
☐	3	Nuclias Global Profile	DBA-1210P	0	SSID RADIO SETTINGS DELETE PUSH CONFIGURATION

4. When prompted to confirm, click **Yes**.

8.1.4 Creating an SSID

Users can create multiple SSIDs under a single Profile and configure each SSID with unique settings to accommodate different wireless usage scenarios.

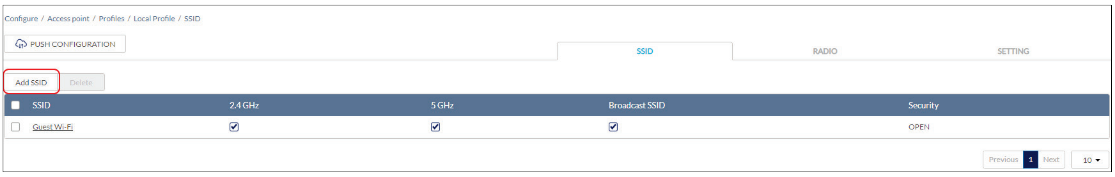
1. Navigate to the **Configure > Access Point > Profiles** page.
2. From the Profile list, click **SSID** under the Actions column of the Profile you wish to create an SSID for.



Configure / Access point / Profiles

☐	#	Profile	Model name	Devices	Actions
☐	1	Local Profile	DBA-1210P	0	SSID RADIO SETTINGS DELETE PUSH CONFIGURATION
☐	2	Global Profile	DBA-1510P	0	SSID RADIO SETTINGS DELETE PUSH CONFIGURATION

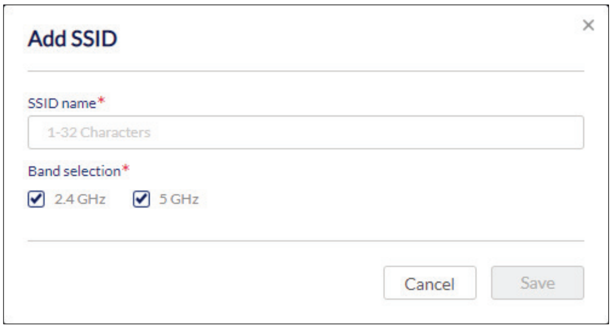
3. On the SSID page, click **Add SSID.**



Configure / Access point / Profiles / Local Profile / SSID

☐	SSID	2.4 GHz	5 GHz	Broadcast SSID	Security
☐	Guest Wi-Fi	☑	☑	☑	OPEN

4. Enter a name for the SSID and choose which wireless bands to enable.



Add SSID

SSID name*

1-32 Characters

Band selection*

☑ 2.4 GHz ☑ 5 GHz

5. Click **Save**.
6. [**Optional**] Repeat steps **1** to **5** to create additional SSIDs.

8.1.5 Configuring Basic SSID Settings

8.1.5.1 Configuring Basic SSID Settings Using No Security

From the basic SSID configuration section, users can configure general wireless and SSID settings, including SSID name, security mode, DHCP settings, broadcasting mode, and VLAN functionality.

1. Navigate to the **Configure > Access Point > Profiles** page.
2. From the Profile list, click **SSID** under the Actions column of the Profile of the SSID you wish to edit.
3. From the SSID list, click the SSID name of the SSID you wish to edit.
4. In the SSID configuration window, click the **Basic** tab.
5. From the Security drop-down menu, select **Open**.
   Note: This removes all security from the SSID and will allow all clients to associate to the SSID without requiring authentication or authorization. This is not recommended.
6. Choose to enable or disable SSID broadcasting.
   Note: If SSID broadcasting is disabled, users will not see the SSID on their device.
7. Check the wireless bands to enable. If both bands are enabled, choose to enable or disable band steering which automatically connects compatible clients to the 5 GHz band.
8. Choose to enable or disable guest access mode.
   Note: Enabling guest access will make this SSID an isolated guest network and will automatically enable NAT mode and station isolation. This prevents external clients from connecting to the internal network.
9. Choose to enable or disable Network Address Translation (NAT mode).
   Note: This is enabled by default if guest access mode is enabled.
10. If **NAT Mode** is enabled, select **Auto** to use an automatic IP pool or select a customized 2.4 GHz and 5 GHz DHCP pool from the drop-down menu.
11. [**Optional**] To create a customized DHCP pool, click **Add a DHCP Pool** and specify the following information:

DHCP name	Enter a name for the DHCP pool.
Lease time	Select a duration from the drop-down menus to specify the IP lease time. When the lease time expires, the client will be assigned a new IP address from the pool.
Start IP	Enter the starting IP address of the pool. Only IP address within the start/end range will be assigned to clients.
End IP	Enter the starting IP address of the pool. Only IP address within the start/end range will be assigned to

	clients.
Subnet mask	Enter a valid subnet mask.
Gateway	Enter a valid gateway address.
Primary	Enter a primary DNS server address.
Secondary	Enter a secondary DNS server address.

12. Choose to enable or disable VLAN.
13. If VLAN is enabled, specify the following information:

    Note: If VLAN and NAT mode are both enabled, the device's IP connection setting must be configured to use the same VLAN in order to connect to the Internet. Refer to the **Editing a Device section on page 64.**

VLAN mode	Select the VLAN type. **Tagged**: Adds an 802.1Q header to traffic. **Untagged**: Does not add a tag to traffic.
VLAN tag	If the VLAN mode is set to **Tagged**, specify a VLAN tag. This will segment traffic with the respective VLAN tag.

14. Choose to enable or disable Station Isolation. This prevents clients connected to the same SSID from communicating with each other.
15. Choose to enable URL redirection.
16. If URL redirection is enabled, specify the following information:

URL for redirection	Enter the URL clients connecting to the SSID will be redirected to.
Redirection interval	Enter the time (in minutes) clients will be periodically redirected to the URL.

17. Click **Save**.
18. Click **Push Configuration**.

8.1.5.2 Configuring Basic SSID Settings Using WPA, WPA+WPA2 With Preshared Key Authentication

1. Navigate to the **Configure > Access Point > Profiles** page.
2. From the Profile list, click **SSID** under the Actions column of the Profile of the SSID you wish to edit.
3. From the SSID list, click the SSID name of the SSID you wish to edit.
4. In the SSID configuration window, click the **Basic** tab.
5. From the Security drop-down menu, select **WPA** or **WPA+WPA2**.
6. From the Auth Method drop-down menu, select **PSK**.
7. Specify the following information:

Encryption	Select an encryption method.
Pre-shared key	Enter a pre-shared key which clients will need to enter in order to connect to the SSID.
Group key update interval	Set the interval (in seconds) at which the group key is updated for the SSID. The default is **3600** seconds.

8. Choose to enable or disable SSID broadcasting.
   Note: If SSID broadcasting is disabled, users will not see the SSID on their device.
9. Check the wireless bands to enable. If both bands are enabled, choose to enable or disable band steering which automatically connects compatible clients to the 5 GHz band.
10. Choose to enable or disable guest access mode.
    Note: Enabling guest access will make this SSID an isolated guest network and will automatically enable NAT mode and station isolation. This prevents external clients from connecting to the internal network.
11. Choose to enable or disable Network Address Translation (NAT mode).
    Note: This is enabled by default if guest access mode is enabled.
12. If **NAT Mode** is enabled, select **Auto** to use an automatic IP pool or select a customized 2.4 GHz and 5 GHz DHCP pool from the drop-down menu.
13. [**Optional**] To create a customized DHCP pool, click **Add a DHCP Pool** and specify the following information:

DHCP name	Enter a name for the DHCP pool.
Lease time	Select a duration from the drop-down menus to specify the IP lease time. When the lease time expires, the client will be assigned a new IP address from the pool.
Start IP	Enter the starting IP address of the pool. Only IP address within the start/end range will be assigned to

	clients.
End IP	Enter the starting IP address of the pool. Only IP address within the start/end range will be assigned to clients.
Subnet mask	Enter a valid subnet mask.
Gateway	Enter a valid gateway address.
Primary	Enter a primary DNS server address.
Secondary	Enter a secondary DNS server address.

14. Choose to enable or disable VLAN.
15. If VLAN is enabled, specify the following information:

    Note: If VLAN and NAT mode are both enabled, the device's IP connection setting must be configured to use the same VLAN in order to connect to the Internet. Refer to the **Editing a Device section on page 64.**

VLAN mode	Select the VLAN type. **Tagged**: Adds an 802.1Q header to traffic. **Untagged**: Does not add a tag to traffic.
VLAN tag	If the VLAN mode is set to **Tagged**, specify a VLAN tag. This will segment traffic with the respective VLAN tag.

16. Choose to enable or disable Station Isolation. This prevents clients connected to the same SSID from communicating with each other.
17. Choose to enable URL redirection.
18. If URL redirection is enabled, specify the following information:

URL for redirection	Enter the URL clients connecting to the SSID will be redirected to.
Redirection interval	Enter the time (in minutes) clients will be periodically redirected to the URL.

19. Click **Save**.
20. Click **Push Configuration**.

8.1.5.3 Configuring Basic SSID Settings

Using WPA, WPA+WPA2 With 802.1X Enterprise (RADIUS) Authentication

1. Navigate to the **Configure > Access Point > Profiles** page.
2. From the Profile list, click **SSID** under the Actions column of the Profile of the SSID you wish to edit.
3. From the SSID list, click the SSID name of the SSID you wish to edit.
4. In the SSID configuration window, click the **Basic** tab.
5. From the Security drop-down menu, select **WPA** or **WPA+WPA2**.
6. From the Auth Method drop-down menu, select **RADIUS**.
7. [**Optional**] If you have no preconfigured RADIUS servers, click **Add a RADIUS server** and specify the following information:

Host	Enter the IP address of the RADIUS server.
Port	Enter a port for the RADIUS server. The range is between **1** and **65535**.
Secret	Enter a shared secret.

8. Select a primary RADIUS server database from the drop-down menu.
9. [**Optional**] Select a secondary RADIUS server database from the drop-down menu.
10. Specify the following information:

Encryption	Select an encryption method.
Group key update interval	Set the interval (in seconds) at which the group key is updated for the SSID. The default is **3600** seconds.

11. Choose to enable or disable SSID broadcasting.

    Note: If SSID broadcasting is disabled, users will not see the SSID on their device.
12. Check the wireless bands to enable. If both bands are enabled, choose to enable or disable band steering which automatically connects compatible clients to the 5 GHz band.
13. Choose to enable or disable guest access mode.

    Note: Enabling guest access will make this SSID an isolated guest network and will automatically enable NAT mode and station isolation. This prevents external clients from connecting to the internal network.
14. Choose to enable or disable Network Address Translation (NAT mode).

    Note: This is enabled by default if guest access mode is enabled.

15. If **NAT Mode** is enabled, select **Auto** to use an automatic IP pool or select a customized 2.4 GHz and 5 GHz DHCP pool from the drop-down menu.
16. [**Optional**] To create a customized DHCP pool, click **Add a DHCP Pool** and specify the following information:

DHCP name	Enter a name for the DHCP pool.
Lease time	Select a duration from the drop-down menus to specify the IP lease time. When the lease time expires, the client will be assigned a new IP address from the pool.
Start IP	Enter the starting IP address of the pool. Only IP address within the start/end range will be assigned to clients.
End IP	Enter the starting IP address of the pool. Only IP address within the start/end range will be assigned to clients.
Subnet mask	Enter a valid subnet mask.
Gateway	Enter a valid gateway address.
Primary	Enter a primary DNS server address.
Secondary	Enter a secondary DNS server address.

17. Choose to enable or disable VLAN.
18. If VLAN is enabled, specify the following information:

    Note: If VLAN and NAT mode are both enabled, the device's IP connection setting must be configured to use the same VLAN in order to connect to the Internet. Refer to the **Editing a Device section on page 64.**

VLAN mode	Select the VLAN type. **Tagged**: Adds an 802.1Q header to traffic. **Untagged**: Does not add a tag to traffic.
VLAN tag	If the VLAN mode is set to **Tagged**, specify a VLAN tag. This will segment traffic with the respective VLAN tag.

19. Choose to enable or disable Station Isolation. This prevents clients connected to the same SSID from communicating with each other.
20. Choose to enable URL redirection.
21. If URL redirection is enabled, specify the following information:

URL for redirection	Enter the URL clients connecting to the SSID will be redirected to.
Redirection interval	Enter the time (in minutes) clients will be periodically redirected to the URL.

22. Click **Save**.
23. Click **Push Configuration**.

8.1.6 Configuring SSID Captive Portal Settings

8.1.6.1 Configuring an SSID Click-Through Captive Portal

A click-through captive portal page requires users to click through a splash page such as a Terms of Agree page before connecting to the SSID. This requires no additional login credentials.

1. Navigate to the **Configure > Access Point > Profiles** page.
2. From the Profile list, click **SSID** under the Actions column of the Profile of the SSID you wish to edit.
3. From the SSID list, click the SSID name of the SSID you wish to edit.
4. In the SSID configuration window, click the **Captive Portal** tab.
5. Select **Click-through** as the Splash page type.
6. Select a click-through page from the drop-down menu.
7. [**Optional**] Click **Splash page editor** to open the splash page editor window. Refer to the **Splash Page Editor section on page 80** for more information.
8. Specify the following information:

Session Timeout	Enter a duration (in minutes) before the connection session automatically times out.
Idle timeout	Enter a duration (in minutes) of allowed inactivity before the captive portal page times out.

9. Click **Save**.
10. Click **Push Configuration**.

8.1.6.2 Configuring an SSID Captive Portal With Basic Login Page Using Local Authentication

A basic login captive portal page requires users to log in using a user account configured in local authentication databases. To create and manage local authentication databases, refer to the **Local Authentication** section on page **76** for more information.

1. Navigate to the **Configure > Access Point > Profiles** page.
2. From the Profile list, click **SSID** under the Actions column of the Profile of the SSID you wish to edit.
3. From the SSID list, click the SSID name of the SSID you wish to edit.
4. In the SSID configuration window, click the **Captive Portal** tab.
5. Select **Sign-on with basic login page** as the Splash page type.
6. Select a basic login page from the drop-down menu.
7. [**Optional**] Click **Splash page editor** to open the splash page editor window. Refer to the **Splash Page Editor section on page 80** for more information.
8. Select **Local authentication** as the Basic Login Page type.
9. [**Optional**] Choose to enable or disable simultaneous logins.
10. Select a local authentication database from the drop-down menu.
    Note: Local authentication databases can be configured separately. Refer to the **Local Authentication section on page 76** for more information.
11. [**Optional**] Click **Add authentication users** to create a new local authentication database.
12. Specify the following information:

Session Timeout	Enter a duration (in minutes) before the connection session automatically times out.
Idle timeout	Enter a duration (in minutes) of allowed inactivity before the captive portal page times out.

13. Click **Save**.
14. Click **Push Configuration**.

8.1.6.3 Configuring an SSID Captive Portal

With Basic Login Page Using a RADIUS Server

1. Navigate to the **Configure > Access Point > Profiles** page.
2. From the Profile list, click **SSID** under the Actions column of the Profile of the SSID you wish to edit.
3. From the SSID list, click the SSID name of the SSID you wish to edit.
4. In the SSID configuration window, click the **Captive Portal** tab.
5. Select **Sign-on with basic login page** as the Splash page type.
6. Select a basic login page from the drop-down menu.
7. [**Optional**] Click **Splash page editor** to open the splash page editor window. Refer to the **Splash Page Editor section on page 80** for more information.
8. Select **RADIUS** as the Basic Login Page type.
9. [**Optional**] If you have no preconfigured RADIUS servers, click **Add a RADIUS server** and specify the following information:

Host	Enter the IP address of the RADIUS server.
Port	Enter a port for the RADIUS server. The range is between **1** and **65535**.
Secret	Enter a shared secret.

10. Select a primary RADIUS server database from the drop-down menu.
11. [**Optional**] Select a secondary RADIUS server database from the drop-down menu.
12. Specify the following information:

Session Timeout	Enter a duration (in minutes) before the connection session automatically times out.
Idle timeout	Enter a duration (in minutes) of allowed inactivity before the captive portal page times out.

13. Click **Save**.
14. Click **Push Configuration**.

8.1.6.4 Configuring an SSID Captive Portal With Third Party Login

1. Navigate to the **Configure > Access Point > Profiles** page.

2. From the Profile list, click **SSID** under the Actions column of the Profile of the SSID you wish to edit.
3. From the SSID list, click the SSID name of the SSID you wish to edit.
4. In the SSID configuration window, click the **Captive Portal** tab.
5. Select **Sign-on with third party credentials** as the Splash page type.
6. Select a social login page from the drop-down menu.
7. [**Optional**] Click **Splash page editor** to open the splash page editor window. Refer to the **Splash Page Editor section on page 80** for more information.
8. Select the required information:

3rd party credentials	Check to the box next to Facebook and Google to enable logging in using Facebook and Google account credentials.
Session Timeout	Enter a duration (in minutes) before the connection session automatically times out.
Idle timeout	Enter a duration (in minutes) of allowed inactivity before the captive portal page times out.

9. Click **Save**.
10. Click **Push Configuration**.

8.1.6.5 Configuring an SSID Captive Portal With Basic and Third Party Login Using Local Authentication

1. Navigate to the **Configure > Access Point > Profiles** page.
2. From the Profile list, click **SSID** under the Actions column of the Profile of the SSID you wish to edit.
3. From the SSID list, click the SSID name of the SSID you wish to edit.
4. In the SSID configuration window, click the **Captive Portal** tab.
5. Select **Sign-on with basic login page and third party credentials** as the Splash page type.
6. Select a third party sign-on page from the drop-down menu.
7. [**Optional**] Click **Splash page editor** to open the splash page editor window. Refer to the **Splash Page Editor section on page 80** for more information.
8. Select **Local authentication** as the Basic Login Page type.
9. [**Optional**] Choose to enable or disable simultaneous logins.
10. Select a local authentication database from the drop-down menu.

Note: Local authentication databases can be configured separately. Refer to the **Local Authentication section on page 76** for more information.

11. [**Optional**] Click **Add authentication users** to create a new local authentication database.
12. Specify the following information:

3rd party credentials	Check to the box next to Facebook and Google to enable logging in using Facebook and Google account credentials.
Session Timeout	Enter a duration (in minutes) before the connection session automatically times out.
Idle timeout	Enter a duration (in minutes) of allowed inactivity before the captive portal page times out.

13. Click **Save**.
14. Click **Push Configuration**.

8.1.6.6 Configuring an SSID Captive Portal With Basic and Third Party Login Using a RADIUS Server

1. Navigate to the **Configure > Access Point > Profiles** page.
2. From the Profile list, click **SSID** under the Actions column of the Profile of the SSID you wish to edit.
3. From the SSID list, click the SSID name of the SSID you wish to edit.
4. In the SSID configuration window, click the **Captive Portal** tab.
5. Select **Sign-on with basic login page and third party credentials** as the Splash page type.
6. Select a basic login page from the drop-down menu.
7. [**Optional**] Click **Splash page editor** to open the splash page editor window. Refer to the **Splash Page Editor section on page 80** for more information.
8. Select **RADIUS** as the Basic Login Page type.
9. [**Optional**] If you have no preconfigured RADIUS servers, click **Add a RADIUS server** and specify the following information:

Host	Enter the IP address of the RADIUS server.
Port	Enter a port for the RADIUS server. The range is

	between **1** and **65535**.
Secret	Enter a shared secret.

10. Select a primary RADIUS server database from the drop-down menu.
11. [**Optional**] Select a secondary RADIUS server database from the drop-down menu.
12. Specify the following information:

3rd party credentials	Check to the box next to Facebook and Google to enable logging in using Facebook and Google account credentials.
Session Timeout	Enter a duration (in minutes) before the connection session automatically times out.
Idle timeout	Enter a duration (in minutes) of allowed inactivity before the captive portal page times out.

13. Click **Save**.
14. Click **Push Configuration**.

8.1.7 Configuring SSID Access Control Settings

8.1.7.1 Configuring SSID MAC Filtering Settings Using MAC ACL

Using MAC Access Control Lists (ACL), users manage access to the network based on the MAC address of the connecting device. Clients with MAC addresses corresponding to MAC addresses in the ACL can be allowed or denied access to the network.

1. Navigate to the **Configure > Access Point > Profiles** page.
2. From the Profile list, click **SSID** under the Actions column of the Profile the SSID you wish to edit.
3. From the SSID list, click the SSID name of the SSID you wish to edit.
4. In the SSID configuration window, click the **Access Control**.
5. In the MAC Filtering section, click **Enable**.
6. Choose a MAC ACL policy:

Allow	Allow devices that correspond with a MAC address in the MAC ACL to connect to the SSID.
Deny	Prevent devices that correspond with a MAC address in the MAC ACL to connect to the SSID.

7. Select a MAC ACL from the drop-down menu.
   Note: To create a MAC ACL, refer to the **MAC ACL section on page 73**.
8. [**Optional**] Click **Add a MAC ACL** to create a new MAC ACL.
9. Click **Save**.
10. Click **Push Configuration**.

8.1.7.2 Configuring SSID MAC Filtering Settings Using RADIUS Authentication

Users can configure an external 802.1x RADIUS server to authenticate users attempting to access the network.

1. Navigate to the **Configure > Access Point > Profiles** page.
2. From the Profile list, click **SSID** under the Actions column of the Profile the SSID you wish to edit.
3. From the SSID list, click the SSID name of the SSID you wish to edit.
4. In the SSID configuration window, click the **Access Control**.
5. In the MAC Filtering section, click **Enable**.
6. Select **RADIUS** as the Filter type
7. [**Optional**] If you have no preconfigured RADIUS servers, click **Add a RADIUS server** and specify the following information:

Host	Enter the IP address of the RADIUS server.
Port	Enter a port for the RADIUS server. The range is between **1** and **65535**.
Secret	Enter a shared secret.

8. Select a primary RADIUS server database from the drop-down menu.
9. [**Optional**] Select a secondary RADIUS server database from the drop-down menu.
10. Click **Save**.
11. Click **Push Configuration**.

8.1.7.3 Configuring SSID IP Filtering

Settings Using IP ACL

Using IP Access Control Lists (ACL), users manage access to the network based on the IP. Clients with IP addresses corresponding to IP addresses in the ACL can be allowed or denied access to the network.

1. Navigate to the **Configure > Access Point > Profiles** page.
2. From the Profile list, click **SSID** under the Actions column of the Profile the SSID you wish to edit.
3. From the SSID list, click the SSID name of the SSID you wish to edit.
4. In the SSID configuration window, click the **Access Control**.
5. In the IP Filtering section, click **Enable**.
6. Choose an IP ACL policy:

Allow	Allow devices that correspond with an IP address in the IP ACL to connect to the SSID.
Deny	Prevent devices that correspond with an IP address in the IP ACL to connect to the SSID.

7. Select an IP ACL from the drop-down menu.
   Note: To create an IP ACL, refer to the **IP ACL section on page 70**.
8. [**Optional**] Click **Add a IP ACL** to create a new IP ACL.
9. Click **Save**.
10. Click **Push Configuration**.

8.1.8 Configuring SSID Schedule Settings

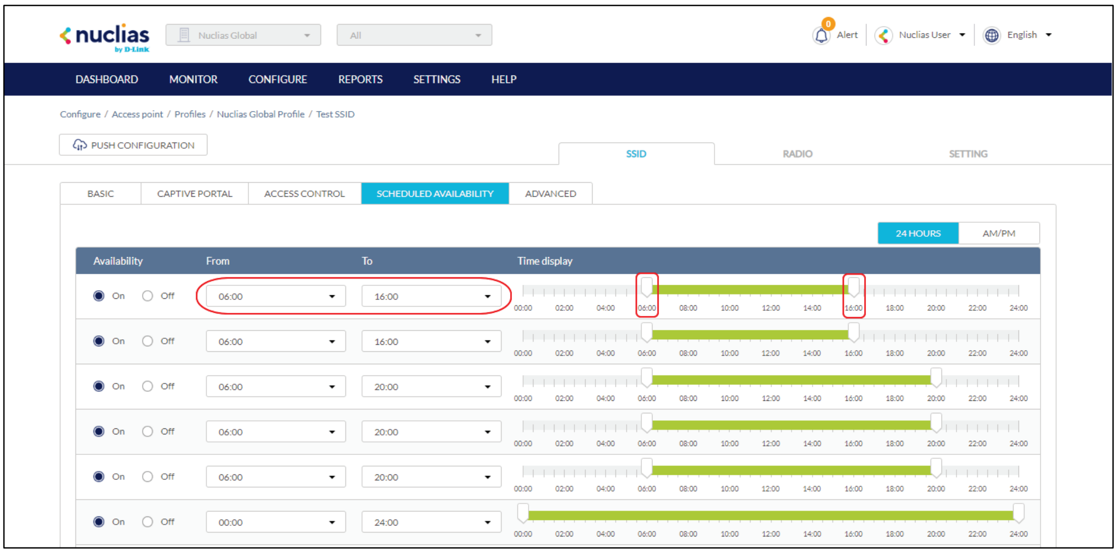
8.1.8.1 Configuring SSID Schedules

1. Navigate to the **Configure > Access Point > Profiles** page.
2. From the Profile list, click **SSID** under the Actions column of the Profile of the SSID you wish to edit.
3. From the SSID list, click the SSID name of the SSID you wish to edit.
4. In the SSID configuration window, click the **Scheduled Availability** tab.
5. [**Optional**] Click the **24 HOURS** or **AM/PM** button in the top-right to change the time display format.

6. In the Availability column, select the schedule behavior for each day of the week:

On	The SSID will be live and broadcasting during the defined time period.
Off	The SSID will be disabled during the defined time period.

7. In the From and To column, select a schedule starting and ending time from the drop-down menu. Alternatively, drag the left and right sliders in the Time display column to define the SSID activity period.



Configure / Access point / Profiles / Nuclias Global Profile / Test SSID

Availability	From	To	Time display
● On ○ Off	06:00	16:00	
● On ○ Off	06:00	16:00	
● On ○ Off	06:00	20:00	
● On ○ Off	06:00	20:00	
● On ○ Off	06:00	20:00	
● On ○ Off	00:00	24:00	

8. Click **Save**.
9. Click **Push Configuration**.

8.1.9 Configuring Advanced SSID Settings

8.1.9.1 Configuring Advanced SSID Settings

1. Navigate to the **Configure > Access Point > Profiles** page.
2. From the Profile list, click **SSID** under the Actions column of the Profile of the SSID you wish to edit.
3. From the SSID list, click the SSID name of the SSID you wish to edit.
4. In the SSID configuration window, click the **Advanced** tab.

5. Specify the following information:

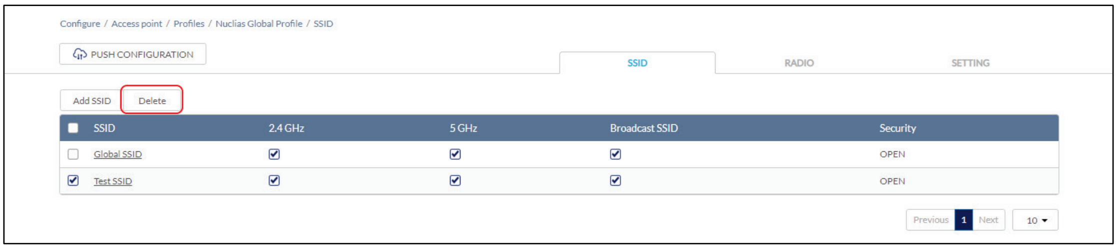
Max Clients	Enter the maximum number of concurrent clients that can connect to the SSID. The maximum is **64**.
Max Allowed Client Retries	Enter the maximum amount of times a client can attempt to reconnect to the SSID once the maximum client limit has been reached. After retrying the set amount times, the client will associate with the AP for a maximum of up to 128 clients. **Note**: If set to 0, no additional clients will be accepted by the AP despite the amount of retries.
Max Upstream	Enter a maximum uploading bandwidth limit (in Kbps) for this SSID.
Max Downstream	Enter a maximum downloading bandwidth limit (in Kbps) for this SSID.
Max Client Upstream	Enter a maximum uploading bandwidth limit (in Kbps) for each client connected to this SSID.
Max Client Downstream	Enter a maximum downloading bandwidth limit (in Kbps) for each client connected to this SSID.
Forward Bonjour Pkts	Enable or disable the forwarding of Apple Bonjour packets from wireless clients to the rest of the network.
IGMP Snooping	Enable or disable IGMP Snooping. This allows the SSID to listen in on IGMP conversations on the network.
Max Mcast Ingress	Enter a maximum multicast ingress bandwidth limit (in Kbps).
RTS Threshold	Enter the packet size threshold to determine when the device will issue a Request To Send (RTS) before sending the packet.
Fragmentation Threshold	Specify the maximum frame size threshold for before a data packet is fragmented. A lower threshold reduces the time to transmit frames and reduces the possibility of data corruption. The range is between **257** and **2346**.
Force Roaming	Enable or disable force roaming. Clients will be forced to roam to another access point once the signal strength falls below the set threshold.
Signal Strength	Enter the signal strength threshold (in dbm) for clients

Threshold	to start roaming.
Enable Weak Signal Exception	Enable or disable weak signal exception. This allows clients with a weak signal to connect to the SSID after a set number of attempts.
Allow weak RSSI Client Associations After	Enter the number of times a client with a weak signal can try to connect, after which the access point will allow the client to connect to it.

6. Click **Save**.
7. Click **Push Configuration**.

8.1.10 Deleting an SSID

1. Navigate to the **Configure > Access Point > Profiles** page.
2. From the Profile list, click **SSID** under the Actions column of the Profile the SSID you wish to delete belongs to.
3. From the SSID list, click the checkbox next to the SSIDs you wish to delete.
4. Click **Delete**.



Configure / Access point / Profiles / Nuclias Global Profile / SSID

☐	SSID	2.4 GHz	5 GHz	Broadcast SSID	Security
☐	Global SSID	☑	☑	☑	OPEN
☑	Test SSID	☑	☑	☑	OPEN

5. When prompted to confirm, click **Yes**.

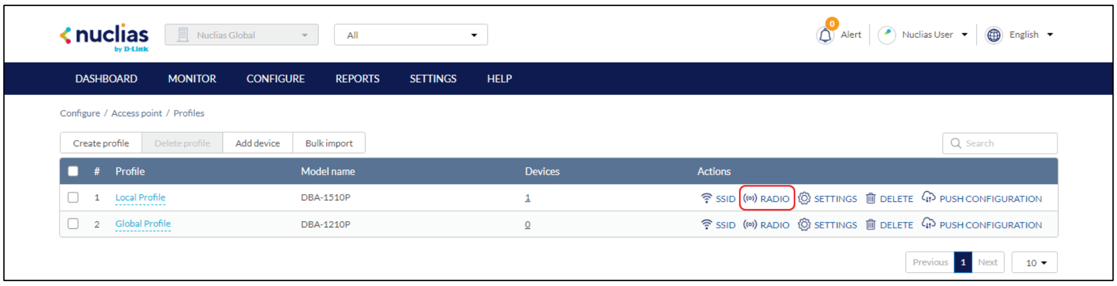
8.1.11 Configuring Profile Radio Settings

From the Radio window, users can configure the 2.4 GHz and 5 GHz wireless bands settings including basic radio functionality, channel selection, and advanced settings and troubleshooting features.

8.1.11.1 Configuring Basic Profile Radio Settings

1. Navigate to the **Configure > Access Point > Profiles** page.

2. From the Profile list, click **RADIO** under the Actions column of the Profile you wish to edit radio settings for.



□	#	Profile	Model name	Devices	Actions
□	1	Local Profile	DBA-1510P	1	SSID RADIO SETTINGS DELETE PUSH CONFIGURATION
□	2	Global Profile	DBA-1210P	0	SSID RADIO SETTINGS DELETE PUSH CONFIGURATION

3. Click the **Basic** tab.
4. Specify the following information:

   Note: The settings below apply to both the 2.4 GHz and 5 GHz bands.

Enabled radio	Choose to enable or disable the 2.4 GHz and 5 GHz wireless band.
Radio Mode	Select a radio mode from the drop-down menu. Only devices that support the selected wireless standards will be able to connect to this wireless band.
Channel Bandwidth	Select the channel transmission bandwidth for the 2.4 and 5 GHz wireless frequencies from the drop-down menu.
Tx power	Enter the maximum transmission power (in %) for the 2.4 GHz and 5 GHz wireless bands.
SSID Isolation	Choose to enable or disable station isolation. Enabling this option prevents clients connected to different SSIDs to see each other.

5. Click **Save**.
6. Click **Push Configuration**.

8.1.11.2 Configuring Profile Radio Channel Settings

1. Navigate to the **Configure > Access Point > Profiles** page.
2. From the Profile list, click **RADIO** under the Actions column of the Profile you wish to edit radio settings for.
3. Click the **Channel** tab.
4. Specify the following information:

Note: The settings below apply to both the 2.4 GHz and 5 GHz bands.

Auto channel	Choose to enable or disable to automatically scan the local area and assign devices to the optimal wireless channel.
Channel	If Auto channel is disabled, select a wireless channel from the drop-down menu.
Eligible channels	Click on a channel number to enable (dark blue) or disable (white) the channel. The SSID will only broadcast on the enabled channels. **Note**: The available channels may vary based on the country of operation.
Force auto channel scan	Choose to enable or disable the auto channel scan to be forced. Forcing the scan is more accurate, but wireless clients may be disconnected during the scan.
Auto channel interval	Specify the interval (in hours) at which the auto-channel scan is performed.

5. [**Optional**] Click **Run Auto Channel now** to manually perform an auto-channel scan.
6. Click **Save**.
7. Click **Push Configuration**.

8.1.11.3 Configuring Advanced Profile Radio Settings

1. Navigate to the **Configure > Access Point > Profiles** page.
2. From the Profile list, click **RADIO** under the Actions column of the Profile you wish to edit radio settings for.
3. Click the **Advanced** tab.
4. Specify the following information:

   Note: The settings below apply to both the 2.4 GHz and 5 GHz bands.

Multi-cast rate	Select the multi-cast rate for the 2.4 GHz and 5 GHz wireless bands from the drop-down menu. This value determines the minimal signal quality for connection. A lower rate allows longer, weaker signals to connect. A higher rate only allows shorter, stronger signals to

	connect.
Beacon interval	Enter a beacon interval value (in ms) between **40** and **3500**. This determines the delay in ms between each information beacon broadcasted by the AP.
DTIM interval	Enter a DTIM interval value between **1** and **255**. This determines the delay between each Delivery Traffic Indication Map (DTIM). The value represents the number of beacons sent before a DTIM is sent.
Preamble mode	Choose a preamble mode. This determines the data string length for error checking purposes. **Long**: Slower, but more accurate. **Short**: Faster, but less accurate.
Protection Mode	Select a protection mode from the drop-down menu. **None**: No protection applied. **CTS-to-Self Protection**: mode for mixed-mode environments with 802.11b devices.
UAPSD	Choose to enable or disable Unscheduled Automatic Power Save Delivery (UAPSD). This feature allows connected clients to save power.
Short guard interval	Choose to enable or disable Short Guard Interval. This reduces signal loss from the multipath effect where multiple signals reach the receiving antenna at different times.

5. Click **Save**.
6. Click **Push Configuration**.

8.1.12 Configuring General Profile Settings

From the General Profile settings, users can configure a proxy server to route traffic and enable IPv6 support.

1. Navigate to the **Configure > Access Point > Profiles** page.
2. From the Profile list, click **Settings** under the Actions column of the Profile you wish to edit general settings for.

3. Specify the following information:

Proxy	Choose to enable or disable proxy server functionality. Using a proxy server causes traffic to route through a remote server for additional security and privacy.
Proxy Host	If proxy server is enabled, enter the proxy server host address.
Proxy Port	If proxy server is enabled, enter the proxy server port. The range is between **1** and **65535**.
IPv6	Choose to enable or disable IPv6 support. This allows the Profile to work in an IPv6 network environment.

4. Click **Save**.
5. Click **Push Configuration**.

8.1.13 Pushing Configuration Changes

The Push Configuration function allows users to quickly apply Profile configuration changes to all devices using this Profile.

Note: Any time a change is made to the Profile or SSID settings, the changes need to be pushed to all associated devices in order to apply these changes.

1. Navigate to the **Configure > Access Point > Profiles** page.
2. From the Profile list, click **Push Configuration** under the Actions column of the Profile you wish to update the configuration settings of.
   Note: A result window will appear providing a summary of the update status.
3. In the Push Configuration Result window, click the **X** icon in the top-right to close the window.

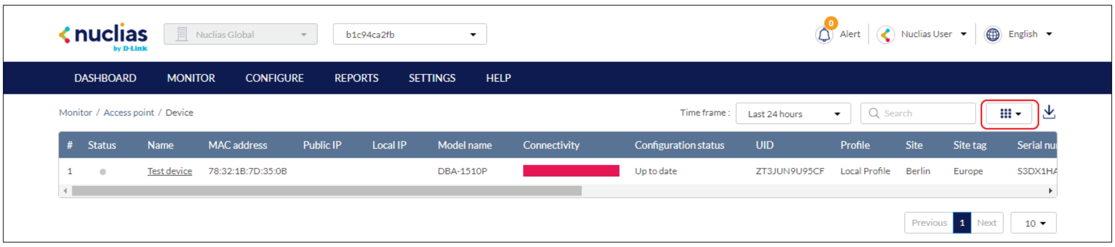
8.2 Devices

From the Devices page, users can add a single device, or bulk import a group of devices, and configure individual devices. This page also provides a detailed overview of all currently registered devices with additional information including status, clients, and general settings.

8.2.1 Filtering Device Information

1. Navigate to the **Monitor > Access Point > Devices** page.
2. Select a time frame from the drop-down menu.

3. Click the filter selection in the top-right.

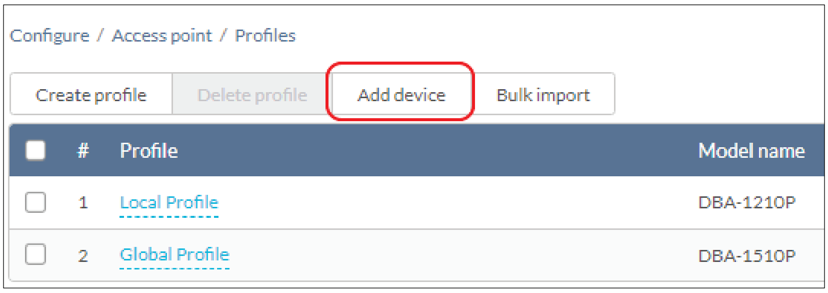


#	Status	Name	MAC address	Public IP	Local IP	Model name	Connectivity	Configuration status	UID	Profile	Site	Site tag	Serial nu
1	●	Test device	78:32:1B:7D:35:0B			DBA-1510P	🟥	Up to date	ZT3JUN9U95CF	Local Profile	Berlin	Europe	S3DX1HA

4. Check the information parameters to display the corresponding device information in the overview window. Check **All** to show all device information parameters.

8.2.2 Adding a Single Device

1. Navigate to the **Configure > Access Point > Devices** page.
2. Click **Add device**.



□	#	Profile	Model name
□	1	Local Profile	DBA-1210P
□	2	Global Profile	DBA-1510P

3. Fill out the required information.

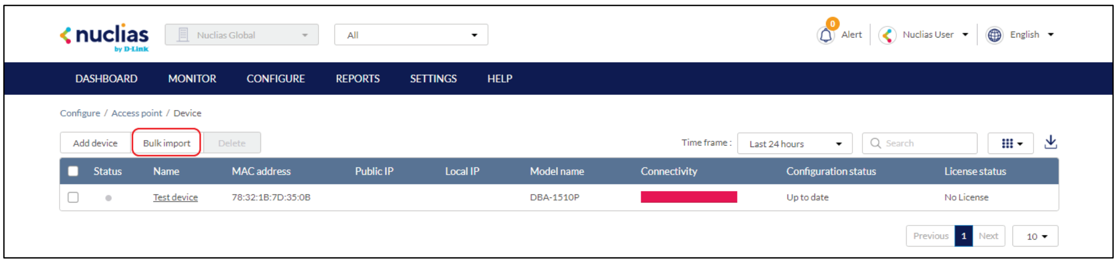
Device UID	Enter the device’s Unique Identifier (UID) found on the label printed on the device. The UID may be listed in the format **XXXX-XXXX-XXXX** or **XXXXXXXXXXXX**. When entering the UID, do not include dashes.
Device name	Enter a name for the device.
Site	Select a Site to link this device to.
Profile	Select a Profile for this device. The device will use the settings configured in that profile.
License Key	[**Optional**] Enter the device license key. **Note**: Every new device will be issued a one year free license key. Once expired, an additional license must be purchased to continue using the device.

4. Click **Save.**

8.2.3 Bulk Adding Multiple Devices to the Inventory

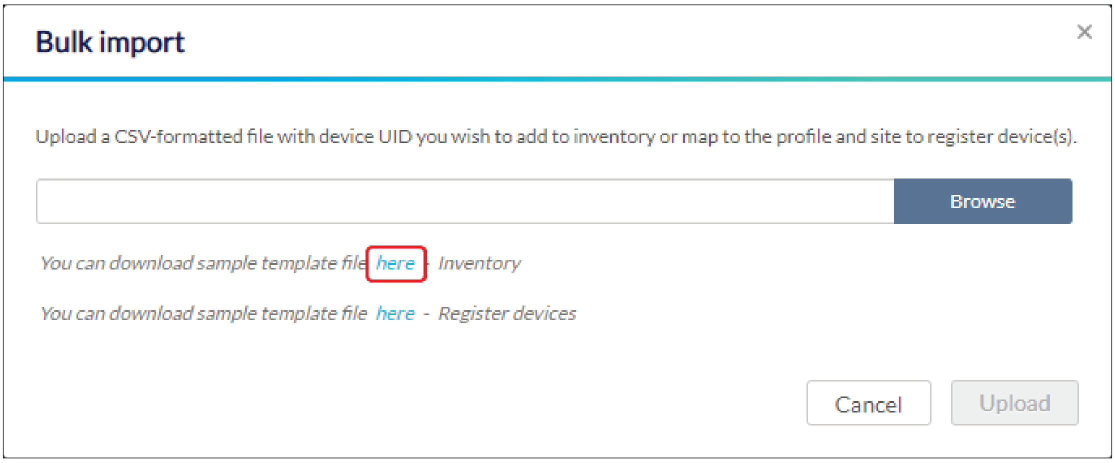
Bulk adding new devices to the Inventory stores the devices in a warehouse where they are kept inactive until they are manually assigned to a Site and Profile by the user at a later point.

1. Navigate to the **Configure > Access Point > Devices** page.
2. Click **Bulk import**.



□	Status	Name	MAC address	Public IP	Local IP	Model name	Connectivity	Configuration status	License status
□	●	Test device	78:32:1B:7D:35:0B			DBA-1510P	🟥	Up to date	No License

3. [**Optional**] Download the reference sample template.


Bulk import

Upload a CSV-formatted file with device UID you wish to add to inventory or map to the profile and site to register device(s).

You can download sample template file here - Inventory

You can download sample template file here - Register devices

4. Click **Browse**.
5. Locate the CSV-formatted file containing the UIDs of the devices.

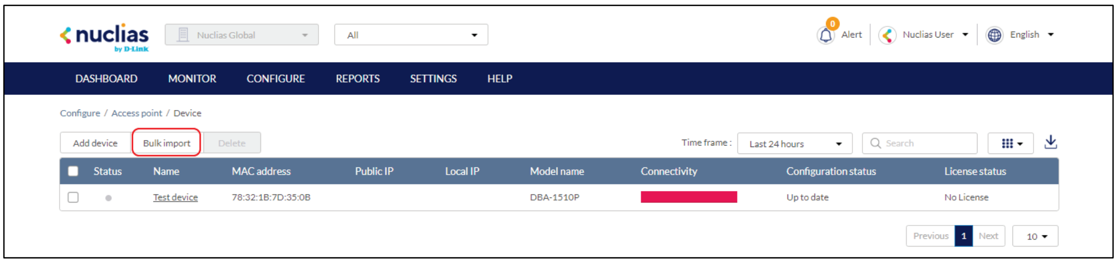
   Note: To add devices to the inventory, use the following format:

   [UID]
6. Click **Upload**.

8.2.4 Bulk Adding and Registering Multiple Devices to a Site

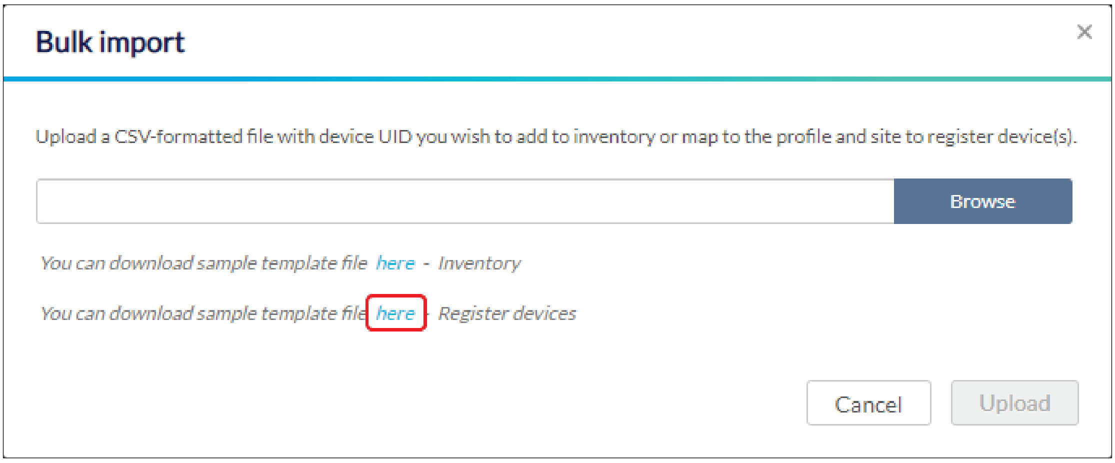
When bulk adding a new device, assigning a Site and Profile to the devices during the device registration process allows them to be used immediately.

1. Navigate to the **Configure > Access Point > Devices** page.
2. Click **Bulk import**.



☐	Status	Name	MAC address	Public IP	Local IP	Model name	Connectivity	Configuration status	License status
☐	●	Test device	78:32:1B:7D:35:0B			DBA-1510P	🟥	Up to date	No License

3. [**Optional**] Download the reference sample template.


Bulk import

Upload a CSV-formatted file with device UID you wish to add to inventory or map to the profile and site to register device(s).

You can download sample template file here - Inventory

You can download sample template file here - Register devices

4. Click **Browse**.
5. Locate the CSV-formatted file containing the UIDs of the devices.

   Note: To directly register devices to a Site, use the following format:

   [UID][Device Name][Profile Name][Site][License Key]
6. Click **Upload**.

8.2.5 Editing a Device

8.2.5.1 Editing the Device Name

1. Navigate to the **Configure > Access Point > Device** page.
2. From the device list, click the device name.
3. Click the device name in the Name field.
4. Enter a new name and press Enter or click outside of the field.
5. Click **Apply**.

8.2.5.2 Changing the Device Site and Profile

1. Navigate to the **Configure > Access Point > Devices** page.
2. From the device list, click the device name.
3. In the Site and Profile section, select a Site from the drop-down menu.
4. In the Site and Profile section, select a Profile from the drop-down menu.
5. Click **Apply**.

8.2.5.3 Changing the Device Connection Type to DHCP

Depending on configuration of the network, the device may require DHCP configuration in order to connect to the Nuclias Cloud.

Note: By default, the connection type is set to **Local Setting**, which refers to the local connection type configured on the physical device. All unmodified devices are configured to use DHCP.

1. Navigate to the **Configure > Access Point > Devices** page.
2. From the device list, click the device name.
3. In the IP Connection section, select **DHCP** as the Type.
   Note: Changing the connection type may disrupt the connection to the Nuclias Cloud.
4. When prompted to confirm, click **Yes**.
5. Specify the following information:

VLAN	[**Optional**] Check to enable VLAN functionality. This segments traffic on the SSID.
VLAN mode	Select the VLAN type. **Tagged**: Adds an 802.1Q header to traffic. **Untagged**: Does not add a tag to traffic.
VLAN tag	If the VLAN mode is set to **Tagged**, specify a VLAN tag. This will segment traffic with the respective VLAN tag.

6. Click **Apply**.

8.2.5.4 Changing the Device Connection to Static IP

Depending on configuration of the network, the device may require a static IP configuration in order to connect to the Nuclias Cloud.

Note: By default, the connection type is set to **Local Setting**, which refers to the local connection type configured on the physical device. All unmodified devices are configured to use DHCP.

1. Navigate to the **Configure > Access Point > Devices** page.
2. From the device list, click the device name.
3. In the IP Connection section, select **Static IP** as the Type.
   Note: Changing the connection type may disrupt the connection to the Nuclias Cloud.
4. When prompted to confirm, click **Yes**.
5. Specify the following information:

Local IP	Enter a valid IP address.
Subnet Mask	Enter a subnet mask.
VLAN	[**Optional**] Check to enable VLAN functionality. This segments traffic on the SSID.
VLAN mode	Select the VLAN type. **Tagged**: Adds an 802.1Q header to traffic. **Untagged**: Does not add a tag to traffic.
VLAN tag	If the VLAN mode is set to **Tagged**, specify a VLAN tag. This will segment traffic with the respective VLAN tag.
Gateway	Enter a default gateway address.
DNS	Enter a Domain Name System (DNS) server address.

6. Click **Apply**.

8.2.5.5 Configuring the Local Device SSID Settings

Under normal circumstances, devices will use the SSID configuration settings of the Profile it is assigned to. If necessary, users can configure individual devices using local settings which override the Profile settings. This may be useful in instances where a device requires customized settings to accommodate a specific use.

1. Navigate to the **Configure > Access Point > Devices** page.
2. From the device list, click the device name.
3. Click the **SSID** tab in the top-right of the screen.

4. In the Use profile configuration field, select **disable**.

   Note: Local settings are configured identically to Profile settings. Refer to the **Profiles section on page** 39 for more information on how to configure each section.

8.2.5.6 Configuring the Local Device Radio Settings

Under normal circumstances, devices will use the radio configuration settings of the Profile it is assigned to. If necessary, users can configure individual devices using local settings which override the Profile settings. This may be useful in instances where a device requires customized settings to accommodate a specific use.

1. Navigate to the **Configure > Access Point > Devices** page.
2. From the device list, click the device name.
3. Click the **Radio** tab in the top-right of the screen.
4. In the Use profile configuration field, select **disable**.

   Note: Local settings are configured identically to Profile settings. Refer to the **Profiles section on page** 39 for more information on how to configure each section.

8.2.5.7 Performing a Device Ping Test

A ping test is used to test the connection of the device to a target IP address.

1. Navigate to the **Configure > Access Point > Devices** page.
2. From the device list, click the device name.
3. Click the **Tools** tab in the top-right of the screen.
4. In the IP address/FQDA field in the **Ping** section, enter a valid IP address or FQDA.
5. Click **Ping**.

8.2.5.8 Performing a Device Traceroute Test

A traceroute test can be used to analyze the amount of hops a data packet requires to reach its destination. This may be useful to diagnose slow data transmissions.

1. Navigate to the **Configure > Access Point > Devices** page.

2. From the device list, click the device name.
3. Click the **Tools** tab in the top-right of the screen.
4. In the IP address/FQDA field in the **Traceroute** section, enter a valid IP address or FQDA.
5. Click **Traceroute**.

8.2.5.9 Performing a Blink LED Test

A blink LED diagnostics test is used to verify the indicator LEDs on the tested device are working correctly.

1. Navigate to the **Configure > Access Point > Devices** page.
2. From the device list, click the device name.
3. Click the **Tools** tab in the top-right of the screen.
4. In the **Others** section, click **Start** to start the test.
   Note: The **Start** button will change to **Stop** once the test begins.
5. Click **Stop** to stop the test.

8.2.5.10 Manually Rebooting a Device

1. Navigate to the **Configure > Access Point > Devices** page.
2. From the device list, click the device name.
3. Click the **Tools** tab in the top-right of the screen.
4. In the **Others** section, click **Reboot**.

8.2.5.11 Adding a License Key to a Device

1. Navigate to the **Configure > Access Point > Devices** page.
2. From the device list, click the device name.
3. Click the **License** tab in the top-right of the screen.
4. In the License Table section, click **Add License**.
5. Enter a valid license key.
6. Click **Save**.

8.2.5.12 Deleting a License Key From a Device

1. Navigate to the **Configure > Access Point > Devices** page.

2. From the device list, click the device name.
3. Click the **License** tab in the top-right of the screen.
4. In the License Table section, from the license key list, click **Delete** under the Actions column of the license key you wish to delete.
5. When prompted to confirm, click **Yes**.

   Note: Deleting a license key from a device will move it back to the license management inventory until it is reassigned to another device.

8.2.6 Deleting a Device

Assigned devices can be unassigned and sent back to the device inventory so they can be reassigned at a later point.

1. Navigate to the **Configure > Access Point > Devices** page.
2. From the device list, click the checkbox next to the device you wish to delete.
3. Click **Delete**.
4. When prompted to confirm, click **Yes**.

   Note: Deleted devices are automatically moved to the inventory until they are reassigned by the user.

8.2.7 Deleting Multiple Devices

Assigned devices can be unassigned and sent back to the device inventory so they can be reassigned at a later point.

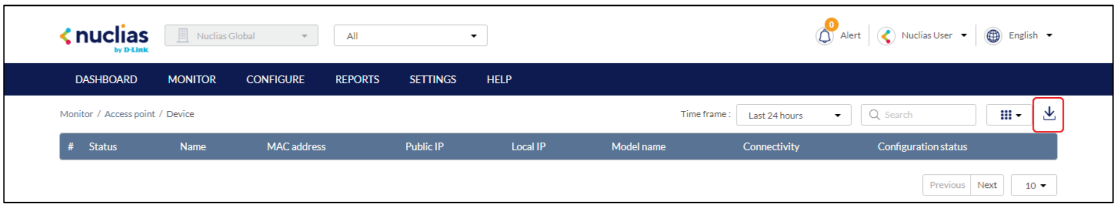
1. Navigate to the **Configure > Access Point > Devices** page.
2. From the device list, click the checkbox next to the devices you wish to delete.
3. Click **Delete**.
4. When prompted to confirm, click **Yes**.

   Note: Deleted devices are automatically moved to the inventory until they are reassigned by the user.

8.2.8 Download the Device List

The device list can be exported in a CSV-formatted file and download to the local device.

1. Navigate to the **Configure > Access Point > Device** page.
2. From the device list, click the **Download** icon in the top-right.



8.3 IP ACLs

8.3.1 Creating an IP ACL Using Single Entries

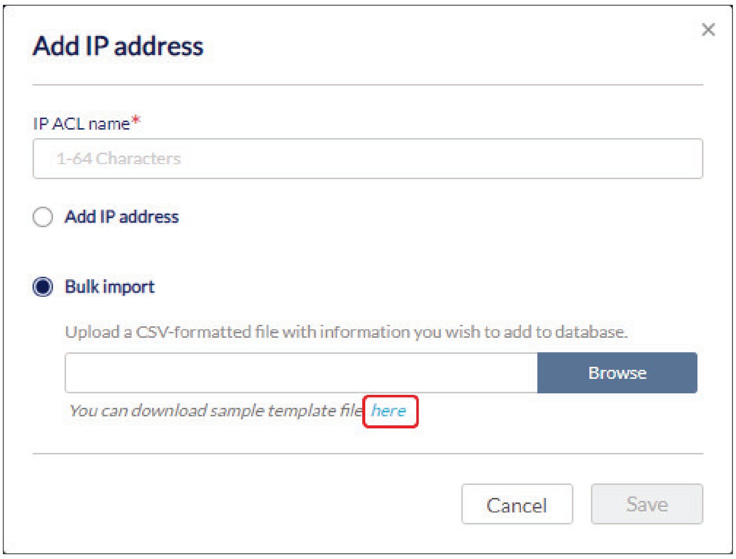
1. Navigate to the **Configure > Access Point > IP ACLs** page.
2. Click **Add IP ACL**.
3. In the Add IP address window, enter a name for the IP ACL.
4. Select **Add IP address**.
5. Specify the following information:

IP address [#]	Enter a valid IP address.
Subnet mask [#]	Enter a valid subnet mask.

6. **[Optional]** Click **Add** to add additional IP entries. Repeat step **4** to **5** for each new entry.
7. Click **Save**.

8.3.2 Creating an IP ACL Using Bulk Import

1. Navigate to the **Configure > Access Point > IP ACLs** page.
2. Click **Add IP ACL**.
3. In the Add IP address window, enter a name for the IP ACL.
4. Select **Bulk import**.
5. [**Optional**] Download the reference sample template.



Add IP address

IP ACL name*

1-64 Characters

○ Add IP address

● Bulk import

Upload a CSV-formatted file with information you wish to add to database.

You can download sample template file here

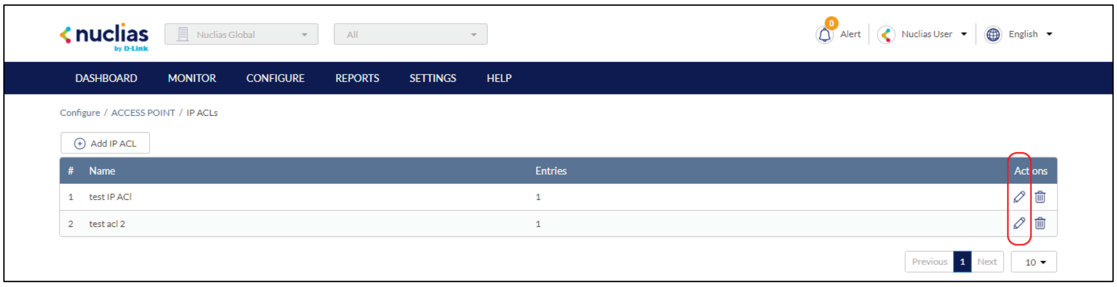
6. Click **Browse**.
7. Locate the CSV-formatted file containing the IP addresses and subnet masks using the following format:

   [IP address][subnet mask]
8. Click **Save**.

8.3.3 Editing Existing IP ACLs

8.3.3.1 Adding IP Addresses to an Existing IP ACL

1. Navigate to the **Configure > Access Point > IP ACLs** page.
2. From the IP ACL list, click the pencil icon under the Actions column of the IP ACL you wish to edit.



Configure / ACCESS POINT / IP ACLs

#	Name	Entries	Actions
1	test IP ACl	1	✎ 🗑
2	test acl 2	1	✎ 🗑

3. In the Update IP ACL window, click **Add IP address**.
4. Specify the following information:

IP Address [#]	Enter a valid IP address.
Subnet mask [#]	Enter a valid subnet mask.

5. **[Optional]** Click **Add** to add additional IP entries. Repeat step **4** for each new entry.
6. Click **Save**.

8.3.3.2 Editing an IP Address in an IP ACL

1. Navigate to the **Configure > Access Point > IP ACLs** page.
2. From the IP ACL list, click the pencil icon under the Actions column of the IP ACL you wish to edit.
3. In the Update IP ACL window, click the pencil icon under the Actions column of the IP entry you wish to edit.
4. In the Edit IP address window, edit the following information:

IP Address [#]	Enter a valid IP address.
Subnet mask [#]	Enter a valid subnet mask.

5. Click **Save**.

8.3.3.3 Deleting an IP Address From an Existing IP ACL

1. Navigate to the **Configure > Access Point > IP ACLs** page.
2. From the IP ACL list, click the pencil icon under the Actions column of the IP ACL you wish to edit.
3. In the Update IP ACL window, click the trash can icon under the Actions column of the IP entry you wish to delete.
4. Click **Save**.
5. When prompted to confirm, click **Yes**.

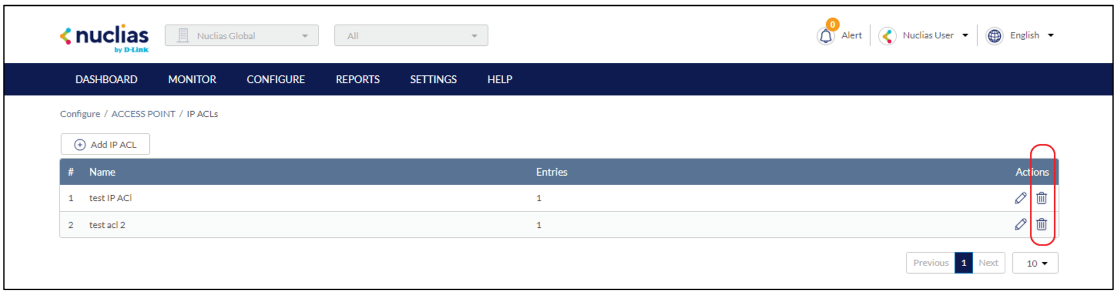
8.3.4 Exporting an IP ACL

IP access control lists can be exported in a CSV-formatted file and download to the local device.

1. Navigate to the **Configure > Access Point > IP ACLs** page.
2. From the IP ACL list, click the pencil icon under the Actions column of the IP ACL you wish to edit.
3. In the Update IP ACL window, click **Export to CSV**.

8.3.5 Deleting an IP ACL

1. Navigate to the **Configure > Access Point > IP ACLs** page.
2. From the IP ACL list, click the trash can icon under the Actions column of the IP ACL you wish to delete.



Configure / ACCESS POINT / IP ACLs

#	Name	Entries	Actions
1	test IP ACl	1	✎ 🗑
2	test acl 2	1	✎ 🗑

3. When prompted to confirm, click **Yes**.

8.4 MAC ACLs

8.4.1 Creating a MAC ACL Using Single Entries

1. Navigate to the **Configure > Access Point > MAC ACLs** page.
2. Click **Add MAC ACL**.
3. In the Add MAC ACL window, enter a name for the MAC ACL.
4. Select **Add MAC address**.
5. Specify the following information:

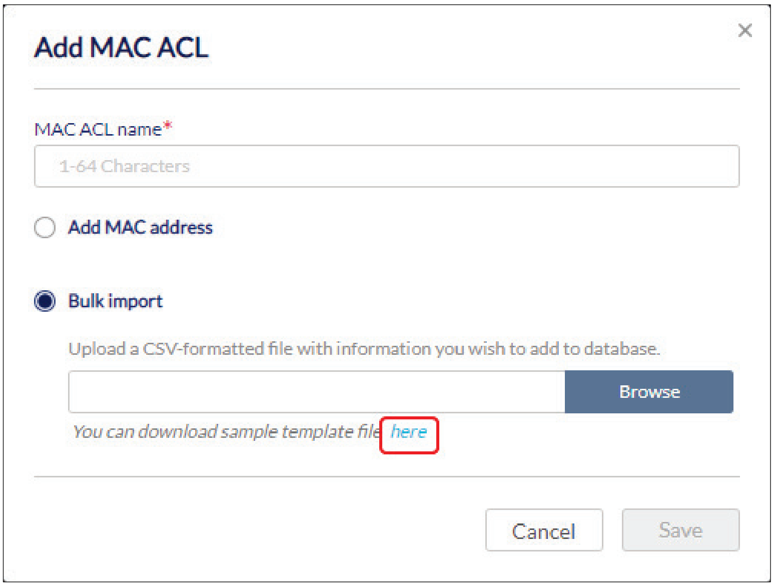
MAC Address [#]	Enter a valid MAC address.

6. **[Optional]** Click **Add** to add additional MAC entries. Repeat step **4** to **5** for each new entry.
7. Click **Save**.

8.4.2 Creating a MAC ACL Using Bulk Import

1. Navigate to the **Configure > Access Point > MAC ACLs** page.

2. Click **Add MAC ACL**.
3. In the Add MAC ACL window, enter a name for the MAC ACL.
4. Select **Bulk import**.
5. [**Optional**] Download the reference sample template.



Add MAC ACL ×

MAC ACL name*

1-64 Characters

○ Add MAC address

● Bulk import

Upload a CSV-formatted file with information you wish to add to database.

Browse

You can download sample template file here

Cancel Save

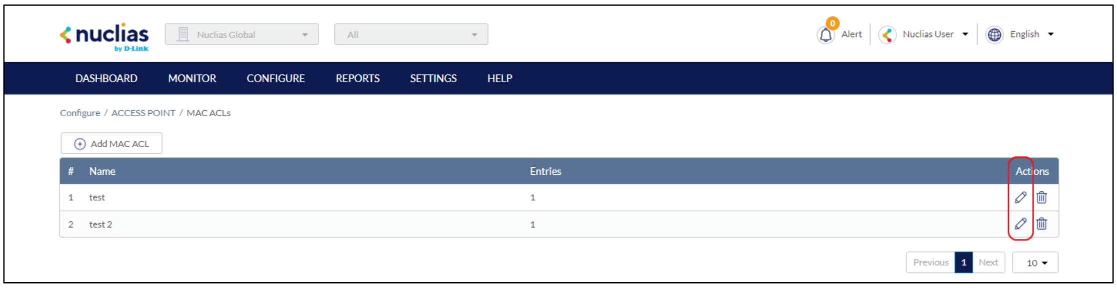
6. Click **Browse**.
7. Locate the CSV-formatted file containing the MAC addresses of the devices using the following format:

   [MAC address]
8. Click **Save**.

8.4.3 Editing Existing MAC ACLs

8.4.3.1 Adding MAC Addresses to an Existing MAC ACL

1. Navigate to the **Configure > Access Point > MAC ACLs** page.
2. From the MAC ACL list, click the pencil icon under the Actions column of the MAC ACL you wish to edit.



Configure / ACCESS POINT / MAC ACLs

⊕ Add MAC ACL

#	Name	Entries	Actions
1	test	1	
2	test 2	1	

Previous 1 Next 10

3. In the Update MAC ACL window, click **Add MAC address**.

4. Specify the following information:

MAC Address [#]	Enter a valid MAC address.

5. **[Optional]** Click **Add** to add additional MAC entries.
6. Click **Save**.

8.4.3.2 Editing a MAC Address in an Existing MAC ACL

1. Navigate to the **Configure > Access Point > MAC ACLs** page.
2. From the MAC ACL list, click the pencil icon under the Actions column of the MAC ACL you wish to edit.
3. In the Update MAC ACL window, click the pencil icon under the Actions column of the MAC entry you wish to edit.
4. In the Edit MAC address window, edit the following information:

MAC Address [#]	Enter a valid MAC address.

5. Click **Save**.

8.4.3.3 Deleting a MAC Address From an Existing MAC ACL

1. Navigate to the **Configure > Access Point > MAC ACLs** page.
2. From the MAC ACL list, click the pencil icon under the Actions column of the MAC ACL you wish to edit.
3. In the Update MAC ACL window, click the trash can icon under the Actions column of the IP entry you wish to delete.
4. Click **Save**.
5. When prompted to confirm, click **Yes**.

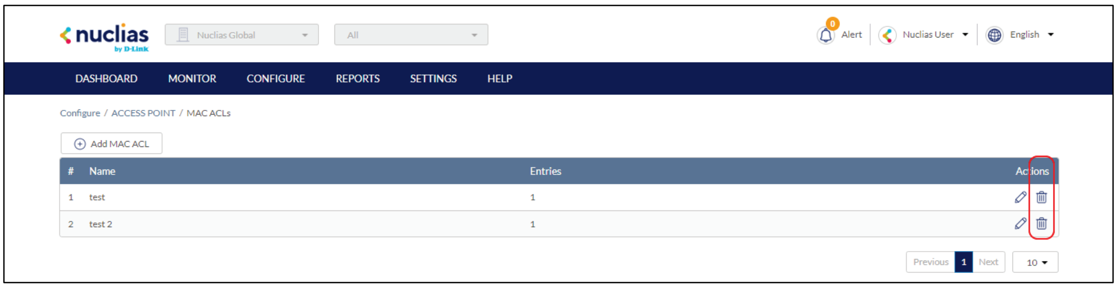
8.4.4 Exporting a MAC ACL

MAC access control lists can be exported in a CSV-formatted file and download to the local device.

1. Navigate to the **Configure > Access Point > MAC ACLs** page.
2. From the MAC ACL list, click the pencil icon under the Actions column of the MAC ACL you wish to edit.
3. In the Update MAC ACL window, click **Export to CSV**.

8.4.5 Deleting a MAC ACL

1. Navigate to the **Configure > Access Point > MAC ACLs** page.
2. From the MAC ACL list, click the trash can icon under the Actions column of the MAC ACL you wish to delete.



#	Name	Entries	Actions
1	test	1	
2	test 2	1	

3. When prompted to confirm, click **Yes**.

8.5 Local Authentication

8.5.1 Creating a Local Authentication Database Using Single Entries

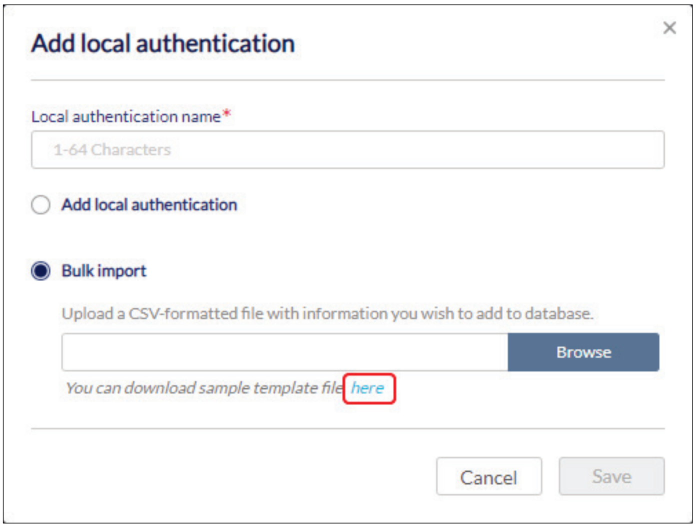
1. Navigate to the **Configure > Access Point > Local authentication list** page.
2. Click **Add local authentication**.
3. In the Add local authentication window, enter a name for the local authentication list.
4. Select **Add local authentication**.
5. Specify the following information:

User name	Enter a local user name.
Password	Enter a password.

6. **[Optional]** Click **Add** to add additional local user accounts. Repeat step **4** to **5** for each new entry.
7. Click **Save**.

8.5.2 Creating a Local Authentication Database Using Bulk Import

1. Navigate to the **Configure > Access Point > Local authentication list** page.
2. Click **Add MAC ACL**.
3. In the Add local authentication window, enter a name for the local authentication list.
4. Select **Bulk import**.
5. [**Optional**] Download the reference sample template.



Add local authentication

Local authentication name*

1-64 Characters

○ Add local authentication

● Bulk import

Upload a CSV-formatted file with information you wish to add to database.

You can download sample template file here

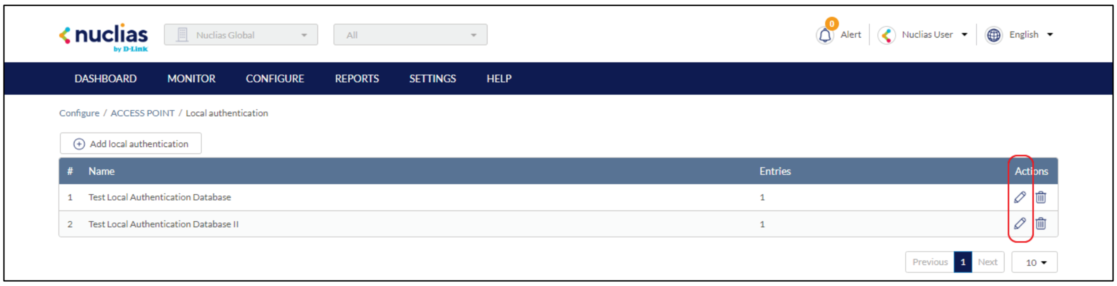
6. Click **Browse**.
7. Locate the CSV-formatted file containing the local user names and passwords using the following format:

   [User name][Password]
8. Click **Save**.

8.5.3 Editing Existing Local Authentication Databases

8.5.3.1 Adding a New Local User to an Existing Local Authentication Database

1. Navigate to the **Configure > Access Point > Local authentication list** page.
2. From the local authentication database list, click the pencil icon under the Actions column of the database you wish to edit.



#	Name	Entries	Actions
1	Test Local Authentication Database	1	
2	Test Local Authentication Database II	1	

3. In the Update local authentication window, click **Add local authentication**.
4. Specify the following information:

User name	Enter a local user name.
Password	Enter a password.

5. **[Optional]** Click **Add** to add additional local user accounts.
6. Click **Save**.

8.5.3.2 Editing an Existing Local User in an Existing Local Authentication Database

1. Navigate to the **Configure > Access Point > Local authentication list** page.
2. From the local authentication database, click the pencil icon under the Actions column of the database you wish to edit.
3. In the Update local authentication window, click the pencil icon under the Actions column of the local user you wish to edit.
4. In the Edit local authentication window, edit the following information:

User name	Enter a local user name.
Password	Enter a password.

5. Click **Save**.

8.5.3.3 Deleting an Existing Local User From an Existing Local Authentication Database

1. Navigate to the **Configure > Access Point > Local authentication list** page.

2. From the local authentication database, click the pencil icon under the Actions column of the database you wish to edit.
3. In the Update local authentication window, click the trash can icon under the Actions column of the local user you wish to delete.
4. Click **Save**.
5. When prompted to confirm, click **Yes**.

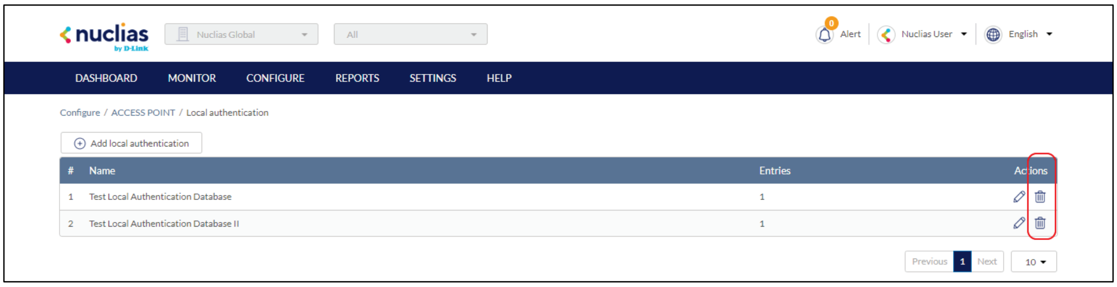
8.5.4 Exporting a Local Authentication Database

Local authentication databases can be exported in a CSV-formatted file and download to the local device.

1. Navigate to the **Configure > Access Point > Local authentication list** page.
2. From the local authentication database list, click the pencil icon under the Actions column of the database you wish to edit.
3. In the Update local authentication window, click **Export to CSV**.

8.5.5 Deleting a Local Authentication Database

1. Navigate to the **Configure > Access Point > Local authentication list** page.
2. From the local authentication database list, click the trash can icon under the Actions column of the database you wish to delete.



Configure / ACCESS POINT / Local authentication

#	Name	Entries	Actions
1	Test Local Authentication Database	1	✎ 🗑
2	Test Local Authentication Database II	1	✎ 🗑

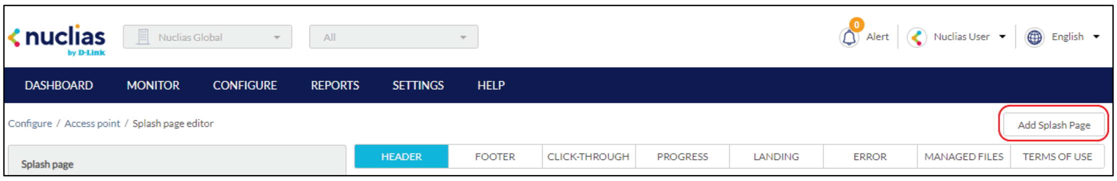
3. When prompted to confirm, click **Yes**.

8.6 Splash Page Editor

From the Splash Page Editor window, users can configure and customize splash pages to use with the SSID. This can be configured to have users click through or enter credentials to access the network. Users can either customize any of the default splash pages or create their own unique splash pages.

8.6.1 Creating a Custom Splash Page

1. Navigate to the **Configure > Access Point > Splash Page Editor** page.
2. In the top-right, click **Add Splash Page**.



3. In the Add Splash Page window, enter the required information:

Name	Enter a name for the splash page.
Type	Select the type of splash page. The following types of splash pages are available: **Click-through:** Only requires users to click through the splash page without entering credentials. **Sign-on with basic login page:** Requires users to log in using local user account credentials. **Sign-on with third party credentials:** Requires users to log in using third party account credentials. **Sign-on with basic login and third party credentials:** Requires users to log in using both local user account and third party account credentials.
Background	Select a default background image for the splash page. [**Optional**] Click **Add Image** to navigate to and upload a custom background image.

4. Click **Save**.

8.6.2 Editing a Splash Page

1. Navigate to the **Configure > Access Point > Splash Page Editor** page.
2. In the Splash page column, click the splash page you wish to edit.

3. Click the respective splash page section tab and edit the following information:

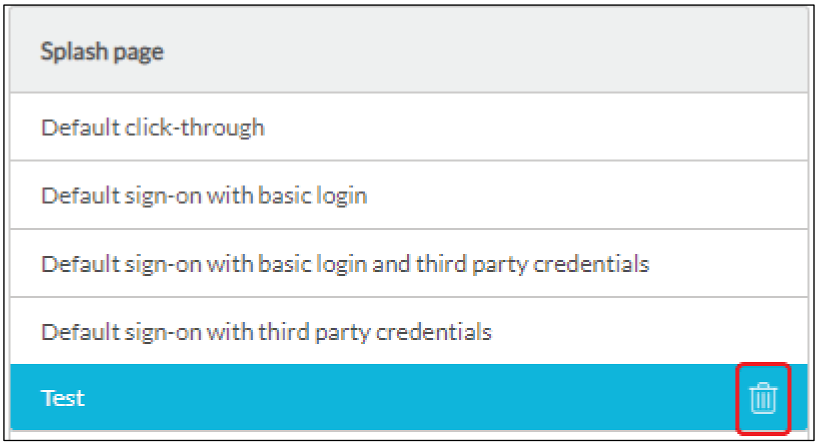
Header	Edit the header section of the splash page.
Footer	Edit the footer section of the splash page.
Click-through [login]	Edit the click-through content. This content will only show if the splash page is using the click-through method.
Progress	Editing the processing page. This content will show while connecting to the SSID.
Landing	Edit the landing page content. This content will show when users have successfully connected to the SSID.
Error	Edit the error page content. This content will show when users have failed to connect to the SSID.
Managed Files	Upload or remove files from the splash page. Example files in include logos, icons, and images.
Terms of Use	Edit the Terms of Use content.

4. Click **Save**.

8.6.3 Deleting a Custom Splash Page

1. Navigate to the **Configure > Access Point > Splash Page Editor** page.
2. In the Splash page column, click the splash page you wish to delete.

   Note: Default splash pages cannot be deleted.
3. Click the trash can icon.



Splash page

Default click-through

Default sign-on with basic login

Default sign-on with basic login and third party credentials

Default sign-on with third party credentials

Test

4. When prompted to confirm, click **Yes**.

9 Reports

From the Reports section, users can view and generate detailed reports for changes on the platform, access point and client activity, network alerts, and license reports.

The following sections provide more detailed information about the different types of reports.

Change Log	From the Change Log section, users can consult a detailed log of changes occurring on the network. Refer to the **Change Log section on page 82** for more information.
Access Point	From the Access Point section, users can view detailed reports about access point activity on the managed network. Refer to the **Access Point section on page 83** for more information.
Alerts	From the Alerts section, users can view a detailed log of all alerts occurring on the network. Refer to the **Alerts section on page 85** for more information.
Licenses	From the Licenses section, users can consult a list of detailed information about licenses assigned to the selected organization. Refer to the **Licenses section on page 87** for more information.

9.1 Change Log

From the Change Log window, users can consult a detailed log of changes to user accounts, profiles, SSIDs, and sites.

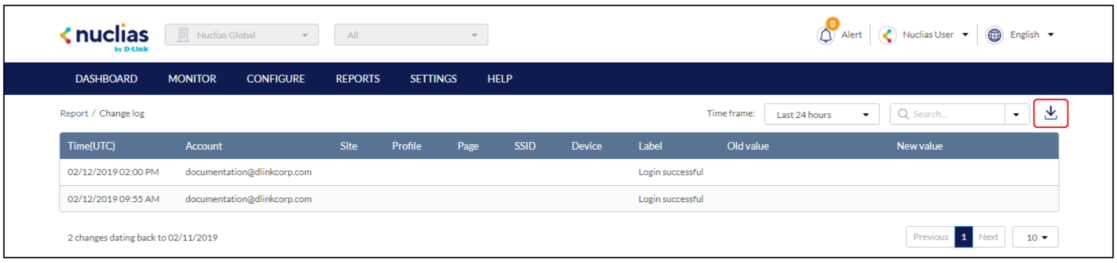
9.1.1 Searching for Change Events

1. Navigate to the **Reports > Change Log** page.
2. [**Optional**] Select a time frame from the drop-down menu.
3. From the change event list, click the **Search** field.
4. Enter the change event name.
   Note: All events matching the value entered in the search field will automatically appear.
5. [**Optional**] Click the filter drop-down menu and enter the following information:
   Note: Multiple filters can be populated to narrow down the search result.

Account	Enter the account name the event is linked to.
Site	Enter the name of the Site the event is linked to.
Profile	Enter the name of the Profile the event is linked to.
SSID	Enter the name of the SSID the event is linked to.
Device	Enter the name of the Device the event is linked to.

9.1.2 Downloading Change Logs

1. Navigate to the **Reports > Change Log** page.
2. From the change log list, click the **Download** icon in the top-right.



Time frame: Last 24 hours

Search...

Time(UTC)	Account	Site	Profile	Page	SSID	Device	Label	Old value	New value
02/12/2019 02:00 PM	documentation@dlinkcorp.com						Login successful		
02/12/2019 09:55 AM	documentation@dlinkcorp.com						Login successful		

2 changes dating back to 02/11/2019

9.2 Access Point

9.2.1 Filtering the Access Point Logs

1. Navigate to the **Reports > Access Point** page.
2. [**Optional**] Select a time frame from the drop-down menu.
3. Check the profiles to filter access point logs for from the Device report drop-down menu.
4. Check the devices to filter access point logs for from the Device drop-down menu.

   Note: Only devices using the profile selected in the previous step will be shown.
5. Check the profiles to filter access point rankings for from the Ranking report drop-down menu.
6. Select the maximum number of entries to display from the Show top results drop-down menu.
7. Check the type of access point logs to show from the Customize report drop-down menu. Select **All** to show all report types.
8. Click **Preview**.

9.2.2 Sending Access Point Logs by

Email

1. Navigate to the **Reports > Access Point** page.
2. [**Optional**] Select a time frame from the drop-down menu.
3. Check the profiles to filter access point logs for from the Device report drop-down menu.
4. Check the devices to filter access point logs for from the Device drop-down menu.
   Note: Only devices using the profile selected in the previous step will be shown.
5. Check the profiles to filter access point rankings for from the Ranking report drop-down menu.
6. Select the maximum number of entries to display from the Show top results drop-down menu.
7. Check the type of access point logs to show from the Customize report drop-down menu. Select **All** to show all report types.
8. [**Optional**] Click Preview to see a preview version of the access point log with the selected parameters.
9. Click **Send email**.

9.2.3 Download Archived Access Point Logs

Monthly access point logs are automatically archived in the system and can be downloaded for reference.

1. Navigate to the **Reports > Access Point** page.
2. From the change log list, click **Archive** in the top-right.
3. Select a time frame from the drop-down menu.
4. Click **Download**.

9.2.4 Download Access Point Logs

1. Navigate to the **Reports > Access Point** page.
2. [**Optional**] Select a time frame from the drop-down menu.
3. Check the profiles to filter access point logs for from the Device report drop-down menu.
4. Check the devices to filter access point logs for from the Device drop-down menu.
   Note: Only devices using the profile selected in the previous step will be shown.
5. Check the profiles to filter access point rankings for from the Ranking report drop-down menu.
6. Select the maximum number of entries to display from the Show top results drop-down menu.

7. Check the type of access point logs to show from the Customize report drop-down menu. Select **All** to show all report types.
8. [**Optional**] Click Preview to see a preview version of the access point log with the selected parameters.
9. Click **Download**.

9.3 Alerts

From the Alerts window, users can view a detailed log of all alerts occurring on the network. Alerts are divided into two types: not processed and processed alerts. Unprocessed alerts are events that have occurred on the network which are pending action by the managing user. Processed alerts are event alerts that have been acknowledged and handled by the managing user.

The type of alerts shown in the alert log can be configured in the Alert Settings. Refer to the **Alert Settings section on page 105** for more information.

9.3.1 Acknowledging Unprocessed Alerts

Unprocessed alerts shown in the alert log can be flagged as acknowledged to keep track of which alerts have been reviewed and handled by the user.

Note: Alerts are managed per user. Multiple users with the required editing rights within the same organizations will see the same alerts. If one user acknowledges or deletes alerts, they will no longer appear for this user, but will still be visible for the other users until they acknowledge or delete these alerts on their respective user accounts.

1. Navigate to the **Reports > Alerts** page.
2. Click the **Not Processed** tab in the top-right of the screen.
3. From the alerts list, click the checkbox next to the alert(s) you wish to acknowledge.
4. Click **Acknowledge**.
   Note: Acknowledged alerts will be automatically moved to the **Processed** tab.

9.3.2 Deleting Unprocessed Alerts

Unprocessed alerts shown in the alert log can be deleted from the log.

Note: Alerts are managed per user. Multiple users with the required editing rights within the same organizations will see the same alerts. If one user acknowledges or deletes alerts, they will no longer appear for this user, but will still be visible for the other users until they acknowledge or delete these alerts on their respective user accounts.

1. Navigate to the **Reports > Alerts** page.
2. Click the **Not Processed** tab in the top-right of the screen.
3. From the alerts list, click the checkbox next to the alert(s) you wish to delete.
4. Click **Delete**.
5. When prompted to confirm, click **Yes**.

   Note: Deleted alerts will be permanently deleted, this action cannot be undone.

9.3.3 Deleting Processed Alerts

Unprocessed alerts shown in the alert log can be deleted from the log.

Note: Alerts are managed per user. Multiple users with the required editing rights within the same organizations will see the same alerts. If one user acknowledges or deletes alerts, they will no longer appear for this user, but will still be visible for the other users until they acknowledge or delete these alerts on their respective user accounts.

1. Navigate to the **Reports > Alerts** page.
2. Click the **Processed** tab in the top-right of the screen.
3. From the alerts list, click the checkbox next to the alert(s) you wish to delete.
4. Click **Delete**.
5. When prompted to confirm, click **Yes**.

   Note: Deleted alerts will be permanently deleted, this action cannot be undone.

9.3.4 Searching for Alerts

1. Navigate to the **Reports > Alerts** page.
2. Click the **Not Processed** or **Processed** tab to the filter the shown alerts.
3. [**Optional**] Select a time frame from the drop-down menu.
4. From the alert list, click the **Search** field.
5. Enter the alert name.

   Note: All alerts matching the value entered in the search field will automatically appear.
6. [**Optional**] Click the filter drop-down menu and enter the following information:

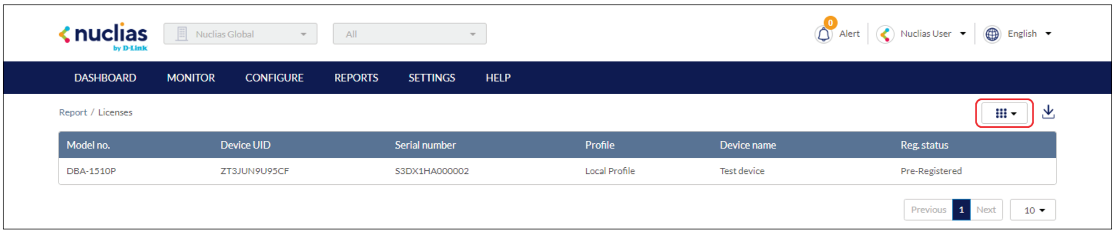
   Note: Multiple filters can be populated to narrow down the search result.

AP	Enter the name of the access point that triggered the alert.
Severity	Select an alert severity level from the drop-down menu.

9.4 Licenses

9.4.1 Filtering the License Logs

1. Navigate to the **Reports > Licenses** page.
2. Click the filter selection in the top-right.

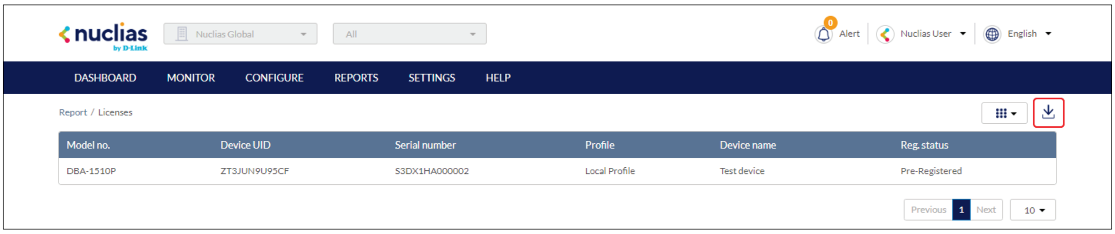


Model no.	Device UID	Serial number	Profile	Device name	Reg. status
DBA-1510P	ZT3JUN9U95CF	S3DX1HA000002	Local Profile	Test device	Pre-Registered

3. Check the information parameters to display the corresponding license information in the overview window. Check **All** to show all license information parameters.

9.4.2 Downloading License Logs

1. Navigate to the **Reports > Licenses** page.
2. From the license log list, click the **Download** icon in the top-right.



Model no.	Device UID	Serial number	Profile	Device name	Reg. status
DBA-1510P	ZT3JUN9U95CF	S3DX1HA000002	Local Profile	Test device	Pre-Registered

10 Settings

Account Management	From the Account Management section, users can consult a full overview and detailed information of all managed user accounts, invite new users, and edit existing users. Refer to the **Account Management section on page 88** for more information.
Organization	From the Organization Management section, users can create

Management	and edit Sites and Site Tags, and invite users to the organization. Refer to the **Organization Management section on page 92** for more information.
License Management	From the License Management section, users can consult more detailed information of all licenses assigned to the organization including status, activation and expiration dates, and how much time is currently left on a license. Refer to the **License Management section on page 94** for more information.
Inventory	From the Inventory section, users can consult comprehensive information about all devices currently assigned to the selected organization, including status, hardware information, and which Site (Tag) it is associated with. New devices can also be added from this window. Refer to the **Inventory section on page 96** for more information.
Firmware	From the Firmware section, users can set device upgrade schedules, or manually upgrade a device's firmware. Refer to the **Firmware section on page 101** for more information.
Alert Settings	From the Alert Settings section, users can choose the type of network events that will trigger alert notifications. Refer to the **Alert Settings section on page 105** for more information.
Add Device	From the Add Device section, users can quickly add a new device to the organization. Refer to the **Add Device section on page 106** for more information.

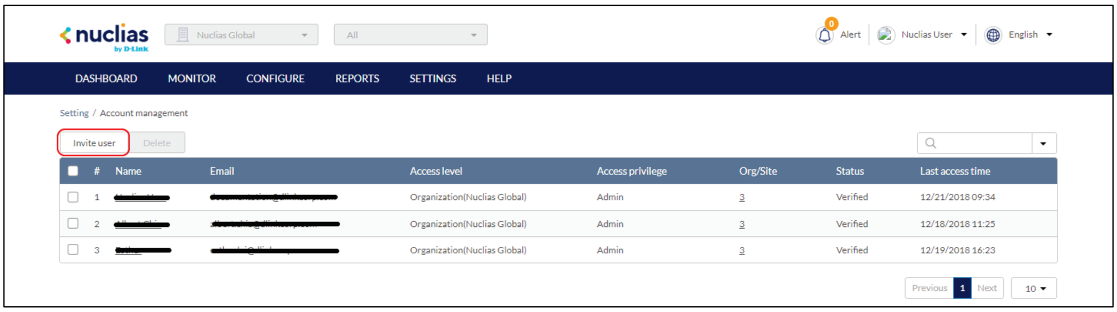
10.1 Account Management

From the Account Management window users can consult an overview of all managed user accounts. It provides additional information about users, including the organization, Site Tag, and Site(s) the user is assigned to, and the user status.

Note: Access to user accounts depends on the account type and privilege level of the managing user.

10.1.1 Inviting a New User

1. Navigate to the **Settings > Account Management** page.
2. Click **Invite User**.



☐	#	Name	Email	Access level	Access privilege	Org/Site	Status	Last access time
☐	1	[redacted]	[redacted]	Organization(Nuclias Global)	Admin	3	Verified	12/21/2018 09:34
☐	2	[redacted]	[redacted]	Organization(Nuclias Global)	Admin	3	Verified	12/18/2018 11:25
☐	3	[redacted]	[redacted]	Organization(Nuclias Global)	Admin	3	Verified	12/19/2018 16:23

3. Specify the following information:

User name	Enter the user’s name.
Access Level	Select the access level of the user. This determines what information the user can view. Based on the selected access level, select the organization from the drop-down menu.
Email address	Enter the user’s email address. This is also the user name to log into the Nuclias Portal interface.
Site Tag	Select a Site tag. This determines which Site tags of the organization can be viewed by the user. Selecting **None** will allow the user to see all Site tags under the selected organization.
Site	Based on the selected Site tag, select a Site. This determines which Sites of the organization can be viewed by the user. Selecting **All** will allow the user to see all Sites under the selected organization.
Role	Select a role for the user. Roles determine the degree of editing and viewing privileges of the user. **Admin**: Full editing and full viewing rights. **Editor**: Partial editing and full viewing rights. **Monitor**: Limited editing and partial viewing rights. **Viewer**: Limited viewing rights.

4. Click **Save change**.

10.1.2 Editing an Existing User

10.1.2.1 Editing a User Name

1. Navigate to the **Settings > Account Management** page.
2. From the user account list, click he user you wish to edit.
3. In the Edit User window, edit the following information:

Name	Enter a user name

4. Click **Save change**.

10.1.2.2 Editing a User’s Access Privilege

1. Navigate to the **Settings > Account Management** page.
2. From the user account list, click he user you wish to edit.
3. In the Edit User window, edit the following information:

Site Tag	Select a Site tag. This determines which Site tags of the organization can be viewed by the user. Selecting **None** will allow the user to see all Site tag under the selected organization.
Site	Based on the selected Site tag, select a Site. This determines which Sites of the organization can be viewed by the user. Selecting **All** will allow the user to see all Sites under the selected organization.
Role	Select a role for the user. Roles determine the degree of editing and viewing privileges of the user. **Admin**: Full editing and full viewing rights. **Editor**: Partial editing and full viewing rights. **Monitor**: Limited editing and partial viewing rights. **Viewer**: Limited viewing rights.

4. Click **Save change**.

10.1.3 Searching for a User

1. Navigate to the **Settings > Account Management**.

2. From the user list, click the **Search** field.
3. Enter the user name.

   Note: All user names matching the value entered in the search field will automatically appear.
4. [**Optional**] Click the filter drop-down menu and enter the following information:

   Note: Multiple filters can be populated to narrow down the search result.

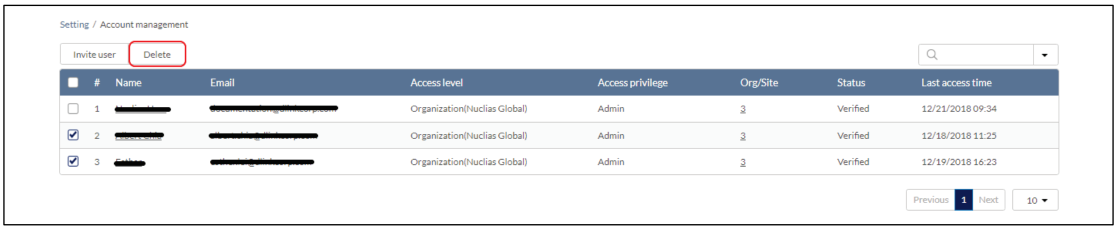
Name	Enter the user name.
Email	Enter the user's email address.
Role	Enter the role assigned to the user.

10.1.4 Deleting a User

Users can be deleted from an organization, permanently removing their ability to view and edit the organization.

Note: The ability to delete a user is dependent on the role and privilege level of the managing user.

1. Navigate to the **Settings > Account Management** page.
2. From the user account list, click the checkbox next to the user account(s) you wish to delete.
3. Click **Delete**.



Setting / Account management

□	#	Name	Email	Access level	Access privilege	Org/Site	Status	Last access time
□	1	[redacted]	[redacted]	Organization(Nuclias Global)	Admin	3	Verified	12/21/2018 09:34
☑	2	[redacted]	[redacted]	Organization(Nuclias Global)	Admin	3	Verified	12/18/2018 11:25
☑	3	[redacted]	[redacted]	Organization(Nuclias Global)	Admin	3	Verified	12/19/2018 16:23

4. When prompted to confirm, enter your user password.

   Note: This is the password of the managing user and not the password of the user to be deleted.
5. click **Yes**.

   Note: The deleted user will receive a notification by email to confirm the account was deleted.

10.2 Organization Management

From the Organization Management window, users can view more information about all organizations linked to the user account including organization type, device status and amount. Users can also create Site and Site Tags, and invite new users.

10.2.1 Creating a New Organization

Organization creation is only available for Managed Services Providers (MSP)-level users. Normal user accounts cannot create additional organizations.

10.2.2 Adding A Site to an Organization

Sites are an easy way for organizations to geographically group devices together. Sites are informational and do not impact the configuration settings of devices that are listed under it. Creating additional Sites allows users to further subdivide and structure the organization and network.

1. Navigate to the **Settings > Organization Management** page.
2. From the organization list, click **Create Site** under the Actions column.
3. Specify the following information:

Site Name	Enter a name for the Site
Site tag	[**Optional**] Select a Site Tag from the drop-down menu. This will place the Site under the selected Site Tag in the organization structure.
Country and local time zone	Select a country and time zone from the respective drop-menu.
Address	Enter a valid address. This is required for the Site to properly show on the Map overview.
NTP server 1	Enter an NTP server address.
NTP server 2	[**Optional**] Enter a secondary NTP server address.
Name	[**Optional**] Enter the name of the Site’s contact person.
Phone	[**Optional**] Enter the contact number of the Site’s contact person.
Email address	[**Optional**] Enter the email address of the Site’s contact person.

4. Click **Save**.

10.2.3 Adding A Site Tag to an Organization

1. Navigate to the **Settings > Organization Management** page.
2. From the organization list, click **Create Site Tag** under the Actions column.
3. Specify the following information:

Site Name	Enter a name for the Site
Parent Tag	Select a Parent Tag from the drop-down menu. This will place this Site Tag under the selected Parent Tag in the organization's structure.

4. Click **Save**.

10.2.4 Invite Users to an Organization

Additional users can be invited to the organization through the organization management window.

Note: The ability to invite users depends on the account role and privilege level of the managing user.

1. Navigate to the **Settings > Organization Management** page.
2. From the organization list, click **Invite User** under the Actions column.
3. Specify the following information:

User name	Enter the user's name.
Access Level	Select the access level of the user. This determines what information the user can view. Based on the selected access level, select the organization from the drop-down menu.
Email address	Enter the user's email address. This is also the user name to log into the Nuclias Portal interface.
Site Tag	Select a Site tag. This determines which Site tags of the organization can be viewed by the user. Selecting **None** will allow the user to see all Site tags under the selected organization.

Site	Based on the selected Site tag, select a Site. This determines which Sites of the organization can be viewed by the user. Selecting **All** will allow the user to see all Sites under the selected organization.
Role	Select a role for the user. Roles determine the degree of editing and viewing privileges of the user. **Admin**: Full editing and full viewing rights. **Editor**: Partial editing and full viewing rights. **Monitor**: Limited editing and partial viewing rights. **Viewer**: Limited viewing rights.

4. Click **Save change**.

10.2.5 Deleting an Organization

Organization deletion is only available for Managed Services Providers (MSP)-level users. Normal user accounts cannot delete additional organizations.

10.3 License Management

The License Management window provides more detailed information for all licenses assigned to the selected organization including status, activation and expiration dates, and how much time is currently left on a license.

10.3.1 Adding a License Key

A single licenses key can be added to the organization so they can be manually assigned to a device at a later point.

1. Navigate to the **Settings > License Management** page.
2. Click **Add License**.
3. In the License Key window, enter the required information:

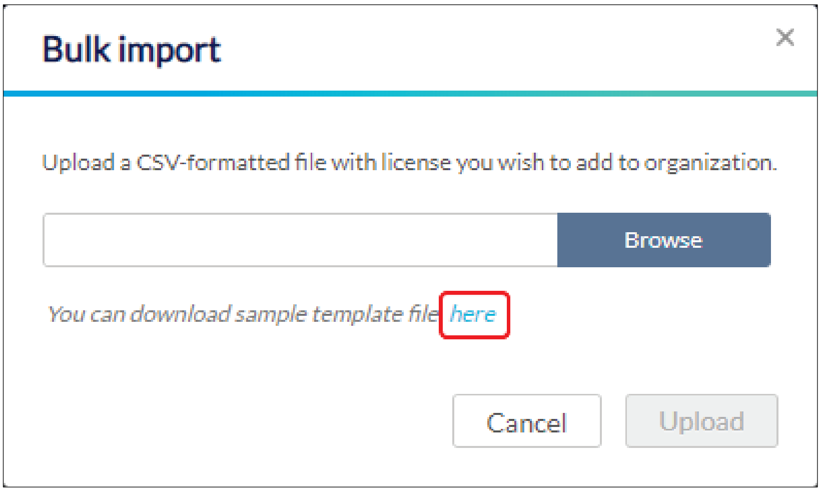
License Key	Enter a valid license key.

4. Click **Save**.

10.3.2 Bulk Adding Multiple Licenses

Multiple licenses keys can be bulk added to the organization so they can be manually assigned to a device at a later point.

1. Navigate to the **Settings > License Management**.
2. Click **Bulk Import**.
3. [**Optional**] Download the reference sample template.



Bulk import

Upload a CSV-formatted file with license you wish to add to organization.

You can download sample template file here

4. Click **Browse**.
5. Locate the CSV-formatted file containing the license keys using the following format:.
   [License key]
6. Click **Upload**.

10.3.3 Searching for a License Key

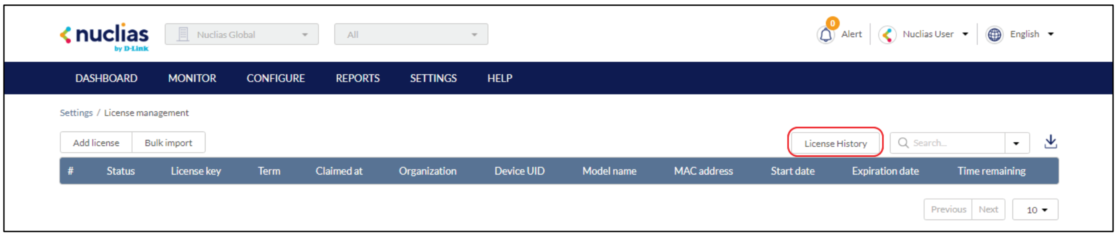
1. Navigate to the **Settings > License Management** page.
2. From the license key list, click the **Search** field.
3. Enter the license key number.
   Note: All license keys matching the value entered in the search field will automatically appear.
4. [**Optional**] Click the filter drop-down menu and enter the following information:
   Note: Multiple filters can be populated to narrow down the search result.

Status	Enter the current status of the license. The available statuses are **Inactive** and **Active**.
License Key	Enter the license key serial number.
Term	Enter the license term. The available terms are **1 Year** and **3 Years**.
Claimed at	Enter the date and time the license was added to the organization in the format **mm/dd/yyyy 00:00 AM/PM**.

Organization	Enter the name of the organization the license key is linked to.
Device UID	Enter the UID of the device the license is linked to.
Model Name	Enter the model name of the device the license is linked to.
MAC Address	Enter the MAC address of the device the license is linked to.
Start Date	Enter the license start date in the format **mm/dd/yyyy.**
Expiration Date	Enter the license expiration date in the format **mm/dd/yyyy**.
Time Remaining	Enter the time remaining on the license in the format **mm/dd/yyyy.**

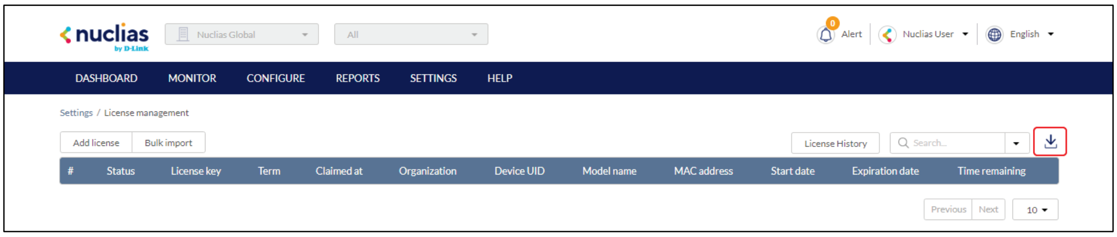
10.3.4 Viewing the License History

1. Navigate to the **Settings > License Management** page.
2. From the license key list, click **License History** in the top-right.



10.3.5 Downloading License Key List

1. Navigate to the **Settings > License Management** page.
2. From the license key list, click the **Download** icon in the top-right.



10.4 Inventory

From the Inventory windows, users can consult comprehensive information about all devices currently assigned to the selected organization, including status, hardware information, and which Site and Profile it is associated with. The inventory is divided into three sections: **Used** (assigned], **Unused** (unassigned devices), and **Both** (all devices).

Note: The displayed devices are based on the selected organization and Site.

10.4.1 Adding and Registering a Single Device to a Site

When adding a new device, assigning a Site and Profile to a device during the device registration process allows it to be used immediately.

1. Navigate to the **Settings > Inventory** page.
2. Click **Add device**.
3. Specify the following information:

Device UID	Enter the device’s Unique Identifier (UID) found on the label printed on the device. The UID may be listed in the format **XXXX-XXXX-XXXX** or **XXXXXXXXXXXX**. When entering the UID, do not include dashes.
Device Name	Enter a name for the device.

4. Under the Register Device option, select **Enable**.
5. Specify the following information:

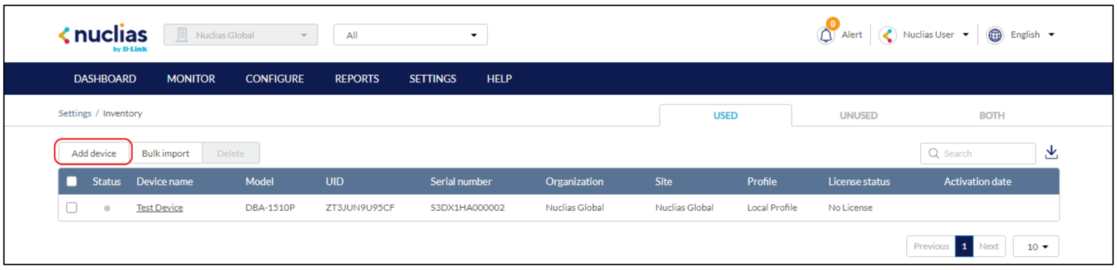
Site	Select a Site to link this device to.
Profile	Select a Profile for this device. The device will use the settings configured in that profile.
License Key	[**Optional**] Enter the device license key. **Note**: Every new device will be issued a one-year free license key. Once expired, an additional license must be purchased to continue using the device.

6. Click **Save**.

10.4.2 Adding a Single Device to the Inventory

Adding a new device to the Inventory stores the device in a warehouse where it is kept inactive until it is manually assigned to a Site and Profile by the user at a later point.

1. Navigate to the **Settings > Inventory** page.
2. Click **Add device**.



☐	Status	Device name	Model	UID	Serial number	Organization	Site	Profile	License status	Activation date
☐	●	Test Device	DBA-1510P	ZT3JUN9U95CF	S3DX1HA000002	Nuclias Global	Nuclias Global	Local Profile	No License	

3. Specify the following information:

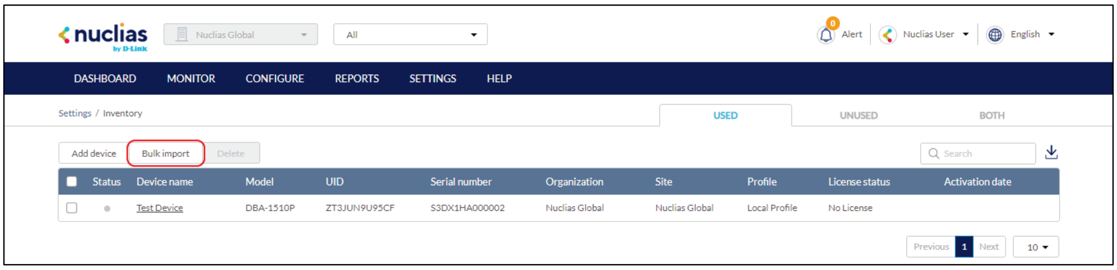
Device UID	Enter the device's Unique Identifier (UID) found on the label printed on the device. The UID may be listed in the format **XXXX-XXXX-XXXX** or **XXXXXXXXXXXX**. When entering the UID, do not include dashes.
Device Name	Enter a name for the device.

4. Under the Register Device option, select **Disable**.
5. Click **Save**.

10.4.3 Bulk Adding Multiple Devices to the Inventory

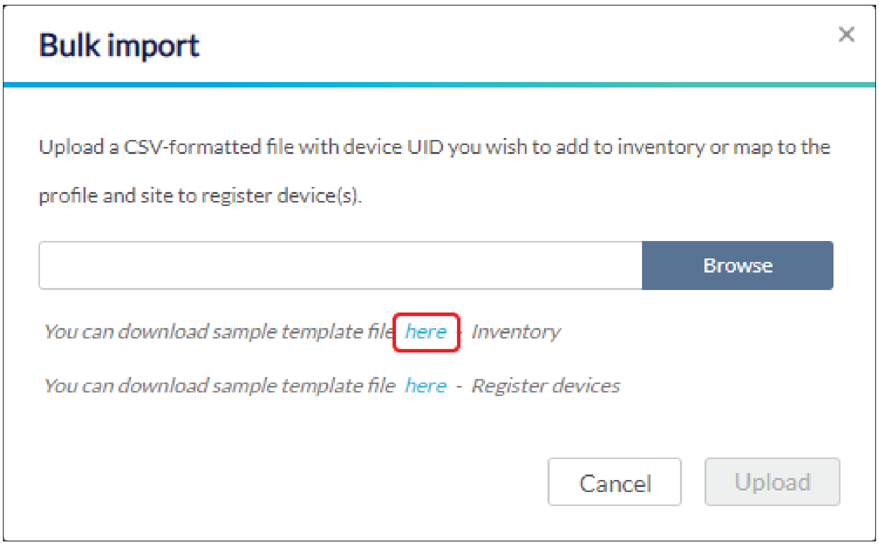
Bulk adding new devices to the Inventory stores the devices in a warehouse where they are kept inactive until they are manually assigned to a Site and Profile by the user at a later point.

1. Navigate to the **Settings > Inventory** page.
2. Click **Bulk import**.



☐	Status	Device name	Model	UID	Serial number	Organization	Site	Profile	License status	Activation date
☐	●	Test Device	DBA-1510P	ZT3JUN9U95CF	S3DX1HA000002	Nuclias Global	Nuclias Global	Local Profile	No License	

3. [**Optional**] Download the reference sample template.



Bulk import

Upload a CSV-formatted file with device UID you wish to add to inventory or map to the profile and site to register device(s).

You can download sample template file here - Inventory

You can download sample template file here - Register devices

4. Click **Browse**.
5. Locate the CSV-formatted file containing the UIDs of the devices.

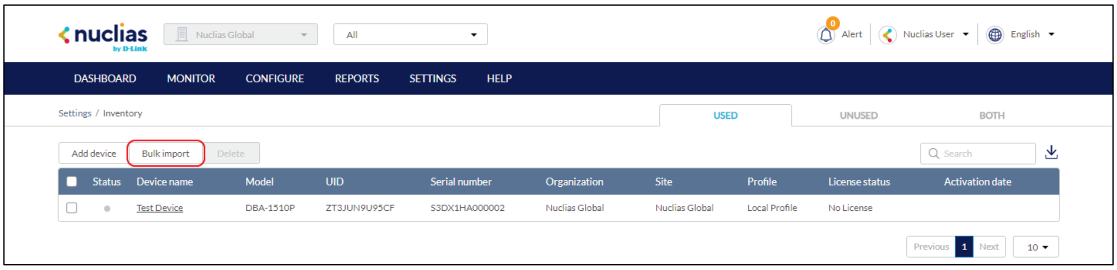
   Note: To add devices to the inventory, use the following format:

   [UID]
6. Click **Upload**.

10.4.4 Bulk Adding and Registering Multiple Devices to a Site

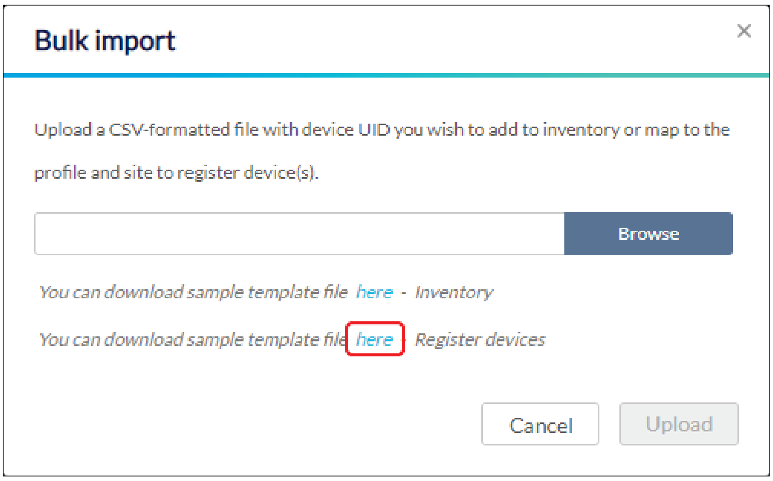
When bulk adding a new device, assigning a Site and Profile to the devices during the device registration process allows them to be used immediately.

1. Navigate to the **Settings > Inventory** page.
2. Click **Bulk import**.



□	Status	Device name	Model	UID	Serial number	Organization	Site	Profile	License status	Activation date
□	●	Test Device	DBA-1510P	ZT3JUN9U95CF	S3DX1HA000002	Nuclias Global	Nuclias Global	Local Profile	No License	

3. [**Optional**] Download the reference sample template.



Bulk import

Upload a CSV-formatted file with device UID you wish to add to inventory or map to the profile and site to register device(s).

You can download sample template file here - Inventory

You can download sample template file here - Register devices

4. Click **Browse**.
5. Locate the CSV-formatted file containing the UIDs of the devices.

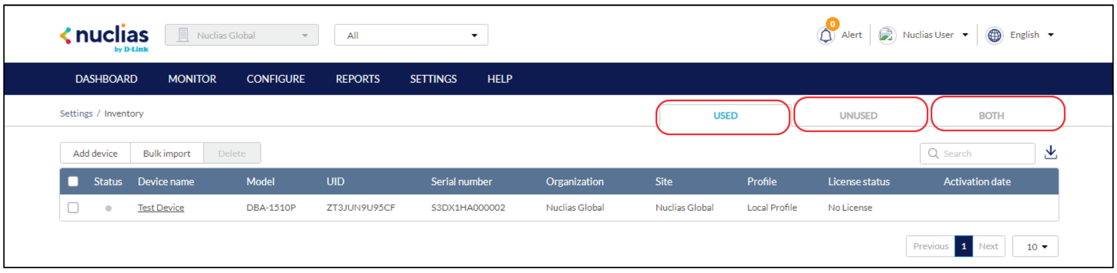
   Note: To directly register devices to a Site, use the following format:

   [UID][Device Name][Profile Name][Site][License Key]
6. Click **Upload**.

10.4.5 Deleting a Device From the Inventory

Deleting a device from the inventory completely removes the device from the organization it was linked to, allowing it to be reassigned to a different organization.

1. Navigate to the **Settings > Inventory** page.
2. Click the tab of the inventory list to filter shown devices.

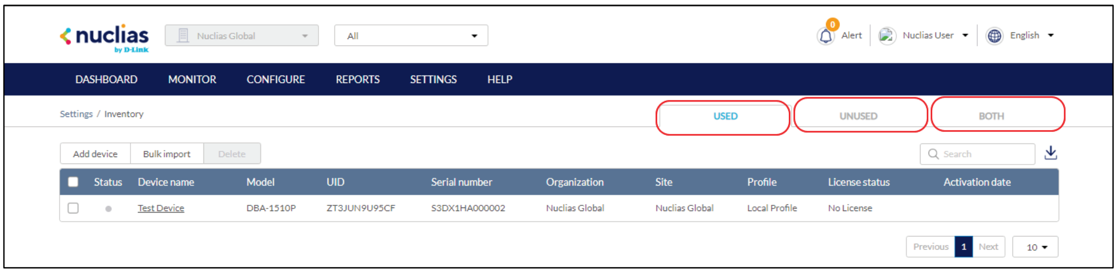


□	Status	Device name	Model	UID	Serial number	Organization	Site	Profile	License status	Activation date
□	●	Test Device	DBA-1510P	ZT3JUN9U95CF	S3DX1HA000002	Nuclias Global	Nuclias Global	Local Profile	No License	

3. From the device list, click the checkbox next to the device(s) you wish to delete.
4. Click **Delete**.
5. When prompted to confirm, click **Yes**.

10.4.6 Searching for a Device

1. Navigate to the **Settings > Inventory** page.
2. Click the tab of the inventory list to filter shown devices.



□	Status	Device name	Model	UID	Serial number	Organization	Site	Profile	License status	Activation date
□	●	Test Device	DBA-1510P	ZT3JUN9U95CF	S3DX1HA000002	Nuclias Global	Nuclias Global	Local Profile	No License	

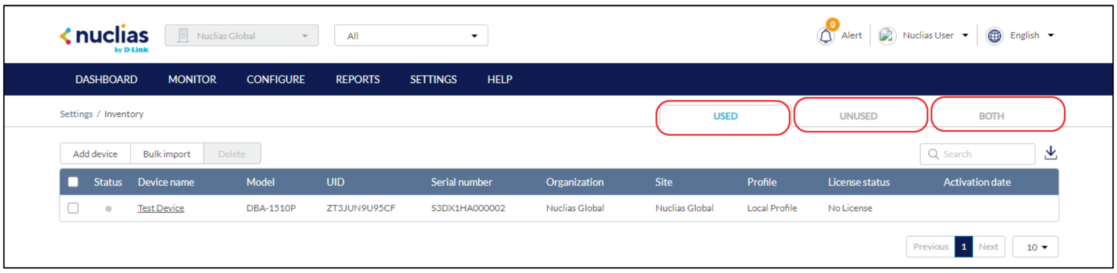
3. From the device list, click the **Search** field.
4. Enter the device name.

   Note: All devices matching the value entered in the search field will automatically appear.

10.4.7 Exporting the Inventory List

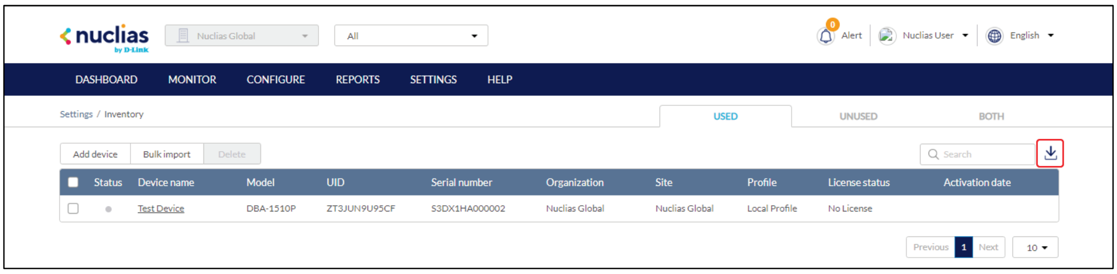
1. Navigate to the **Settings > Inventory** page.
2. Click the tab of the inventory list you wish to export.

   Note: Each tab exports a separate inventory list for the respective tab.



□	Status	Device name	Model	UID	Serial number	Organization	Site	Profile	License status	Activation date
□	●	Test Device	DBA-1510P	ZT3JUN9U95CF	S3DX1HA000002	Nuclias Global	Nuclias Global	Local Profile	No License	

3. From the device list, click the **Download** icon in the top-right.



□	Status	Device name	Model	UID	Serial number	Organization	Site	Profile	License status	Activation date
□	●	Test Device	DBA-1510P	ZT3JUN9U95CF	S3DX1HA000002	Nuclias Global	Nuclias Global	Local Profile	No License	

10.5 Firmware

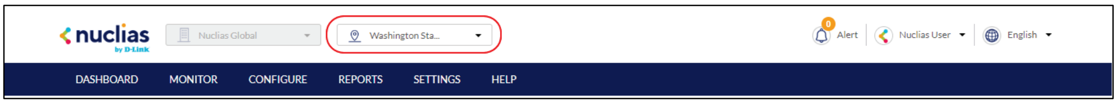
From the Firmware window, users can view basic firmware information, and set up a firmware upgrade schedule. Firmware upgrades are managed at the Site level and configured per device type, which means that all devices of the same type that are linked to that Site will use the same firmware upgrading policy.

10.5.1 Setting an Automatic Upgrade

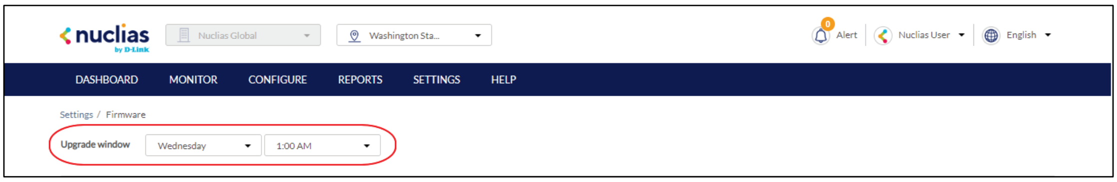
Window

Automatic upgrade windows provide an easy way of regularly maintaining device firmware by setting a fixed weekly time and date to automatically scan for new firmware and upgrade devices if a new firmware version is available.

1. Navigate to the **Settings > Firmware** page.
2. Select a Site from the Site menu in the top of the screen.



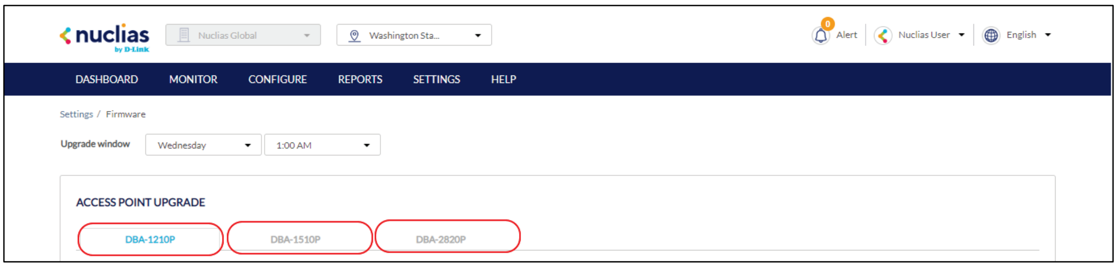
3. Select a day of a week and time of day from the drop-down menu.



Upgrade window: Wednesday, 1:00 AM

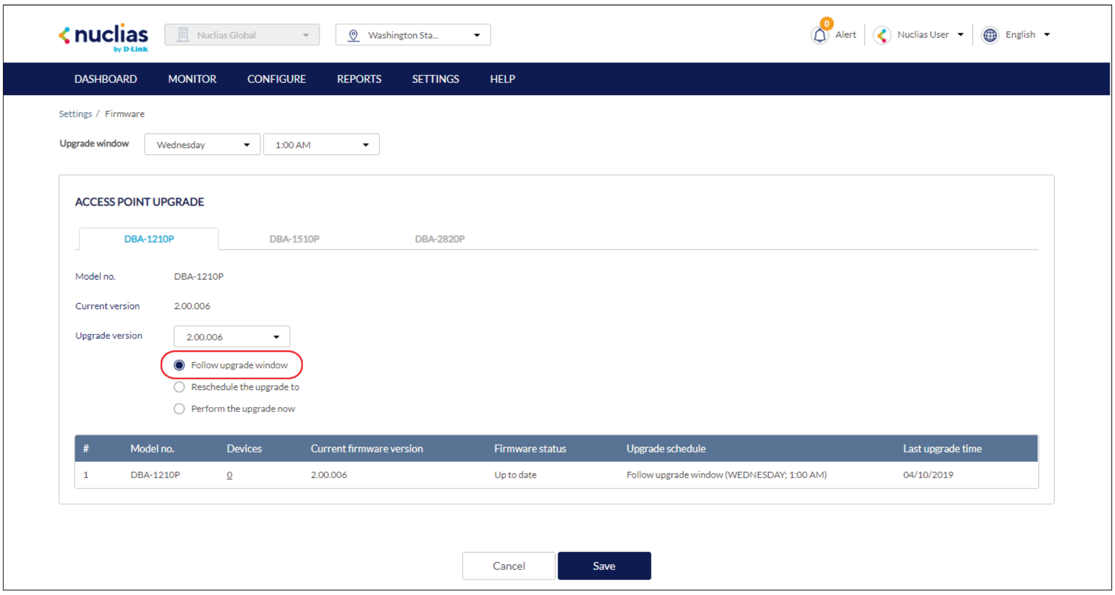
4. Click the tab of the device you wish to configure firmware upgrades for.

   Note: Upgrade windows need to be configured separately for each device type.



Upgrade window: Wednesday, 1:00 AM

5. Select **Follow upgrade window**.



Upgrade window: Wednesday, 1:00 AM

Model no. DBA-1210P

Current version 2.00.006

Upgrade version 2.00.006

● Follow upgrade window

○ Reschedule the upgrade to

○ Perform the upgrade now

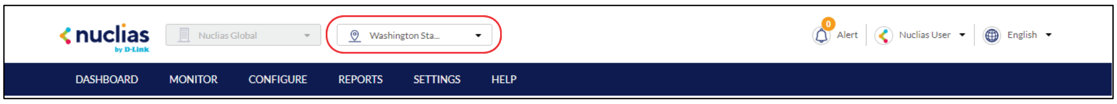
#	Model no.	Devices	Current firmware version	Firmware status	Upgrade schedule	Last upgrade time
1	DBA-1210P	0	2.00.006	Up to date	Follow upgrade window (WEDNESDAY; 1:00 AM)	04/10/2019

6. Click **Save**.

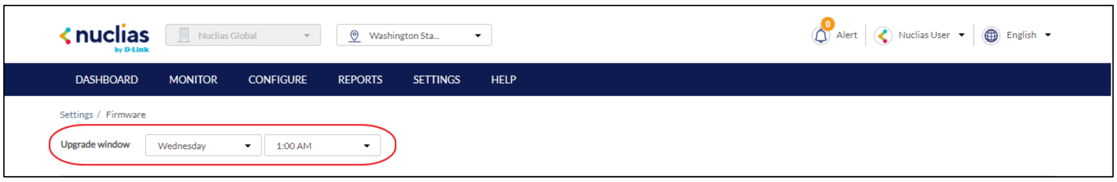
10.5.2 Setting a Custom Device Upgrade Time

Users can define a specific time and date to scan for firmware updates which overrides the automatic upgrade schedule.

1. Navigate to the **Settings > Firmware** page.
2. Select a Site from the Site menu in the top of the screen.



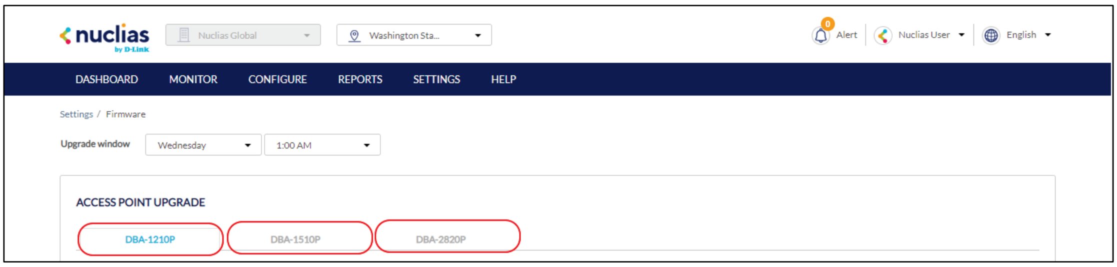
3. Select a day of a week and time of day from the drop-down menu.



Upgrade window: Wednesday, 1:00 AM

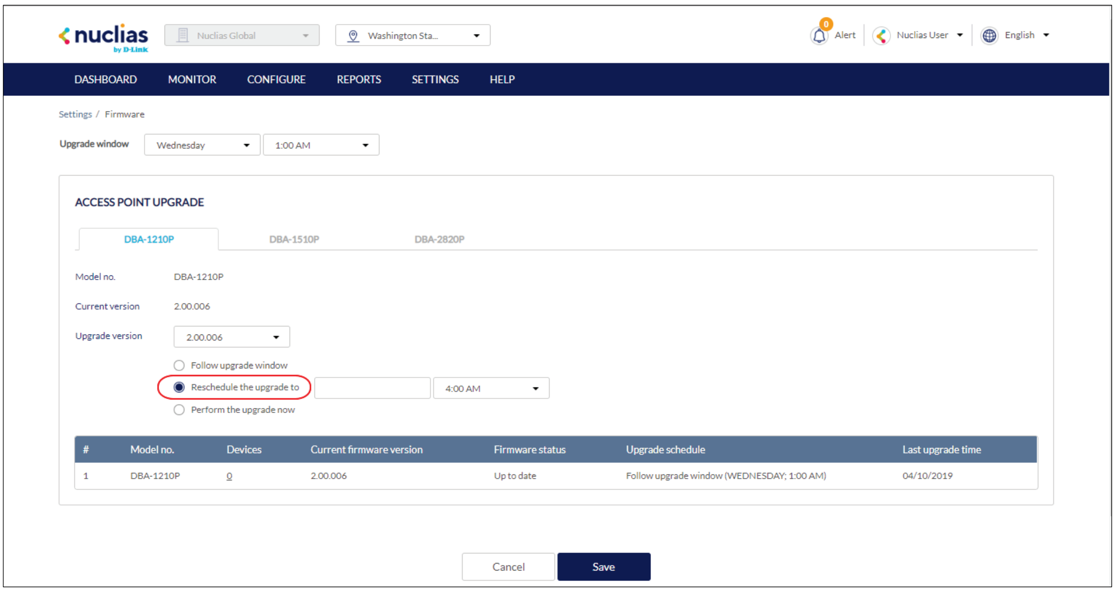
4. Click the tab of the device you wish to configure firmware upgrades for.

   Note: Upgrade windows need to be configured separately for each device type.



Upgrade window: Wednesday, 1:00 AM

5. Select **Reschedule the upgrade to**.



Upgrade window: Wednesday, 1:00 AM

ACCESS POINT UPGRADE

DBA-1210P | DBA-1510P | DBA-2820P

Model no. DBA-1210P

Current version 2.00.006

Upgrade version 2.00.006

○ Follow upgrade window

● Reschedule the upgrade to _____ 4:00 AM

○ Perform the upgrade now

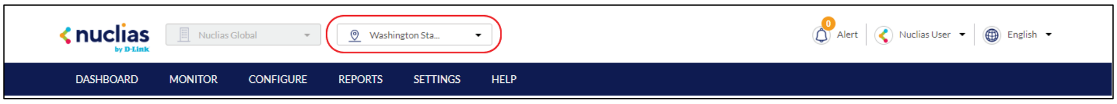
#	Model no.	Devices	Current firmware version	Firmware status	Upgrade schedule	Last upgrade time
1	DBA-1210P	0	2.00.006	Up to date	Follow upgrade window (WEDNESDAY; 1:00 AM)	04/10/2019

6. Click the date field to choose a date and select a time from the drop-down menu.
7. Click **Save**.

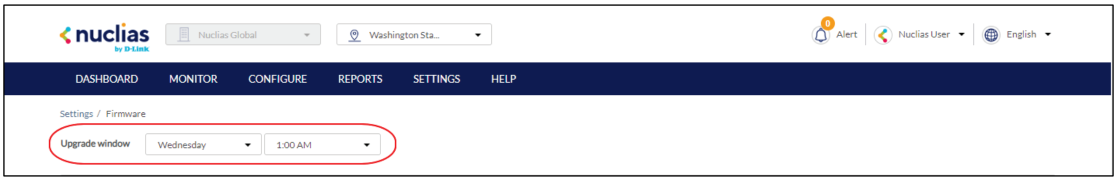
10.5.3 Performing a Manual Firmware Upgrade

Devices can be manually upgraded by performing an on-the-spot firmware upgrade check.

1. Navigate to the **Settings > Firmware** page.
2. Select a Site from the Site menu in the top of the screen.



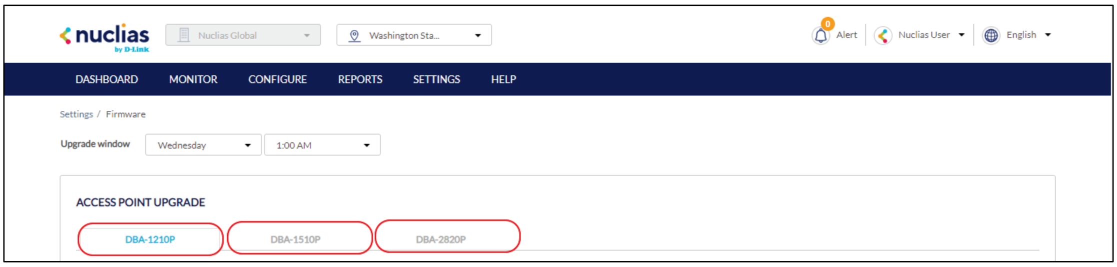
3. Select a day of a week and time of day from the drop-down menu.



Upgrade window: Wednesday, 1:00 AM

4. Click the tab of the device you wish to configure firmware upgrades for.

   Note: Upgrade windows need to be configured separately for each device type.

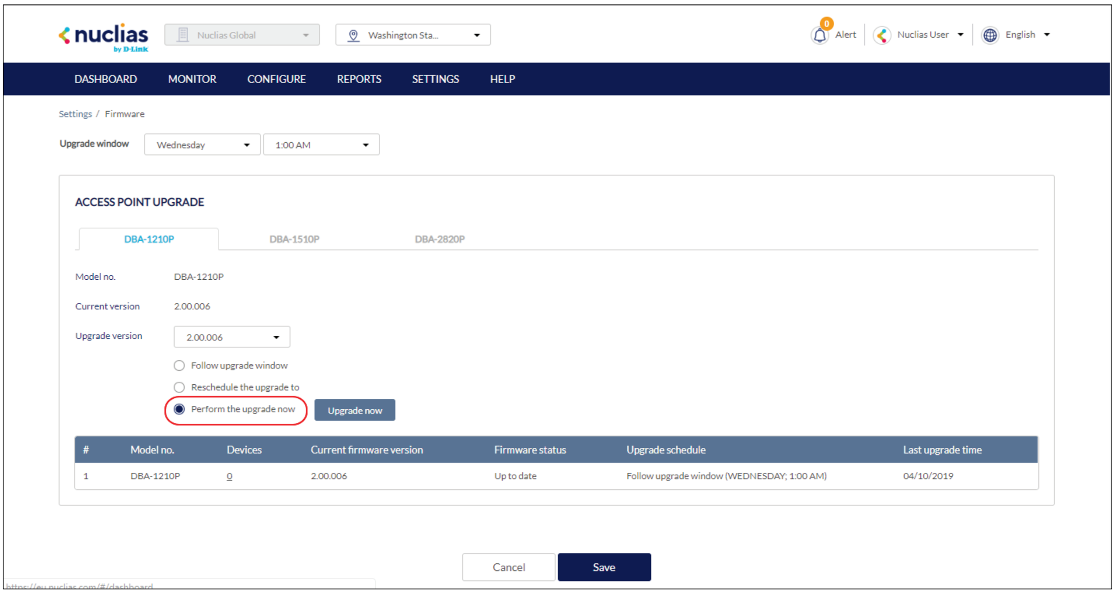


Settings / Firmware

Upgrade window: Wednesday, 1:00 AM

ACCESS POINT UPGRADE

5. Select **Perform the upgrade now**.



Settings / Firmware

Upgrade window: Wednesday, 1:00 AM

ACCESS POINT UPGRADE

Model no. DBA-1210P

Current version 2.00.006

Upgrade version 2.00.006

○ Follow upgrade window
○ Reschedule the upgrade to
● Perform the upgrade now

#	Model no.	Devices	Current firmware version	Firmware status	Upgrade schedule	Last upgrade time
1	DBA-1210P	0	2.00.006	Up to date	Follow upgrade window (WEDNESDAY; 1:00 AM)	04/10/2019

6. Click **Upgrade now**.
7. When prompted to confirm, click **Yes**.

10.6 Alert Settings

10.6.1 Configuring Alert Notifications

Users can customize what type of network events will trigger alert notifications. Events are divided into general and device-specific events.

1. Navigate to the **Settings > Alert Settings** page.
2. In the General section, select the event types to receive alert notifications for:

Firmware upgraded	Sends an alert notification when a device firmware has been successfully upgraded.
Firmware upgrade failed	Sends an alert notification when a device firmware upgrade has failed.
Device added to	Sends an alert notification when a device has been

profile	assigned to a Profile.
Device removed from profile	Sends an alert notification when a device has been unassigned from a Profile.
Device connected to Nuclias	Sends an alert notification when a device has successfully connected to the Nuclias server.
Configuration pushed to devices	Sends an alert notification when a configuration update has been successfully pushed to affected devices.
Configuration failed to push to device	Sends an alert notification when a configuration update failed to be pushed to affected devices.

3. In the Access Point section, check the **Send alert when AP offline** option and select a time (in minutes) from the drop-down menu.
4. Click **Save**.

10.7 Add Device

1. Navigate to the **Settings > Add device** page.
   Note: The add device window will automatically appear.
2. Specify the following information:

Device UID	Enter the device's Unique Identifier (UID) found on the label printed on the device. The UID may be listed in the format **XXXX-XXXX-XXXX** or **XXXXXXXXXXXX**. When entering the UID, do not include dashes.
Device name	Enter a name for the device.
Site	Select a Site to link this device to.
Profile	Select a Profile for this device. The device will use the settings configured in that profile.
License Key	[**Optional**] Enter the device license key. **Note**: Every new device will be issued a one year free license key. Once expired, an additional license must be purchased to continue using the device.

3. Click **Save**.

11 Help

11.1 Contact Us

From the Contact Us window, users can submit a support ticket for various issues with devices or the platform as well as provide feedback so we may continue to improve the quality of our platform.

11.1.1 Contacting Nuclias Support

1. Navigate to the **Help > Contact Us** page.
2. Specify the following information:

Name	Click to enter a sender name. The recipient will see this name. By default, this is the user name.
E-mail	Enter an email address. Responses to submitted tickets will be received on this email address. By default, this is the user account email.
Phone	[**Optional**] Enter a contact number.
Issue category	Select a category type from the drop-down menu.
Problem device	If Installation, Device Problem, or License Issue is selected as the category, enter the UID of the affected device. [**Optional**] Click **Add** to enter additional device UIDs.
Description	Enter a description of the issue or feedback.

3. [**Optional**] Drag and drop an image file of up to 2 mb in size. Alternatively, click **Browse** and navigate to the image file.
4. Click **Submit**.