



Questo manuale d'istruzione è fornito da trovaprezzi.it. Scopri tutte le offerte per [D-Link DBA-3621P](#) o cerca il tuo prodotto tra le [migliori offerte di Altri dispositivi di rete](#)



Questo manuale d'istruzione è fornito da trovaprezzi.it. Scopri tutte le offerte per [D-Link DBA-3621P](#) o cerca il tuo prodotto tra le [migliori offerte di Wireless e Bluetooth](#)

**D-Link**

2020 | Business Class Networking

# NUCLIAS CLOUD DOCUMENTATION

V 1.00



# Table of Contents

Getting Started with Nuclias .....	7
Getting Started .....	7
Creating an Account .....	8
Logging in to Nuclias .....	10
Adding a Device .....	11
Adding a Single Device .....	11
Bulk Adding Devices .....	12
Bulk Assigning Devices .....	13
Adding a Device from QR Code .....	13
Portal .....	14
Portal - Overview .....	14
Introduction .....	15
Audience .....	15
Conventions .....	15
Terms and Concepts .....	15
Interface .....	17
Overview .....	17
Global Toolbar .....	18
Account Menu .....	18
Language Menu .....	20
Management Toolbar .....	22
Dashboard .....	23
Customizing the Overview .....	23
Sending a Dashboard Snapshot by Email .....	24
Monitor .....	27
Overview .....	27
Access Point .....	28
Devices .....	28
Clients .....	28
Event Logs .....	29
Switch .....	31
Customizing the Device Monitor Overview .....	31
Downloading Device Monitoring Logs .....	31
Changing the Device Site and Profile .....	31
Changing the Device Connection Type to DHCP .....	32
Changing the Device Connection to Static IP .....	32
Viewing and Customizing the Switch Performance Summary .....	32
Viewing and Customizing the Switch Port Status Overview .....	33

Viewing and Customizing the Switch Power Consumption Overview .....	34
Performing a Device Ping Test .....	35
Performing a MAC Forwarding Table Test .....	35
Performing a Cable Test .....	35
Performing a Port Cycle Test .....	35
Performing a Blink LED Test .....	35
Manually Rebooting a Device .....	35
Adding a Licence Key to a Device .....	36
Deleting a License Key from a Device .....	36
Clients .....	36
Customizing the Client Monitor Overview .....	36
Downloading Client Monitoring Logs .....	37
Event Logs .....	37
Filtering Event Log Parameters .....	37
Downloading Event Logs .....	37
Map .....	39
Navigating the Map .....	39
Navigating Sites on the Map Using the Site List .....	40
Floor Plans .....	42
Adding a Floor Plan .....	42
Editing a Floor Plan .....	42
Deleting a Floor Plan .....	45
Configure - Access Point .....	46
Overview .....	46
Profiles .....	47
Creating a Profile .....	47
Deleting a Profile .....	47
Configuring SSID Captive Portal Settings .....	54
Configuring SSID Access Control Settings .....	58
Configuring SSID Schedule Settings .....	60
Deleting an SSID .....	62
Configuring Profile Radio Settings .....	62
Configuring General Profile Settings .....	66
Pushing Configuration Changes .....	66
Configuring Advanced SSID Settings .....	60
Devices .....	67
Filtering Device Information .....	67
Adding a Single Device .....	67
Bulk Adding Multiple Devices to the Inventory .....	68

&#39;&#39; &#39;Video Tutorials&#39;	68
Bulk Adding and Registering Multiple Devices to a Site .....	68
Editing a Device .....	69
Deleting a Device .....	73
Deleting Multiple Devices .....	73
Download the Device List .....	73
IP ACLs .....	74
Creating an IP ACL Using Single Entries .....	74
Creating an IP ACL Using Bulk Import .....	74
Editing Existing IP ACLs .....	74
Exporting an IP ACL .....	75
Deleting an IP ACL .....	76
MAC ACLs .....	77
Creating a MAC ACL Using Single Entries .....	77
Creating MAC ACL Using Bulk Import .....	77
Editing Existing MAC ACLs .....	77
Exporting a MAC ACL .....	78
Deleting a MAC ACL .....	78
Local Authentication .....	80
Creating a Local Authentication Database Using Single Entries .....	80
Creating a Local Authentication Database Using Bulk Import .....	80
Editing Existing Local Authentication Databases .....	80
Exporting a Local Authentication Database .....	82
Deleting a Local Authentication Database .....	82
LDAP Servers .....	83
RADIUS Servers .....	85
Splash Page Editor .....	87
Creating a Custom Splash Page .....	87
Editing a Splash Page .....	88
Walled Garden .....	90
Configure - Switch .....	92
Overview .....	92
Profiles .....	93
Creating a Profile .....	93
Deleting a Profile .....	93
Deleting Multiple Profiles .....	93
Configuring Switch Port Settings .....	94
Configuring Switch Port Schedules .....	99
Configuring Basic Switch Profile Settings .....	101
Configuring Quality of Service Settings .....	105
Configuring Access Policies .....	108

Pushing Configuration Changes .....	109
Devices .....	110
Filtering Device Information .....	110
Adding a Single Device .....	110
Bulk Adding Multiple Devices to the Inventory .....	111
Bulk Adding and Registering Multiple Devices to a Site .....	111
Adding a Tag to One or More Devices .....	112
Editing a Device .....	113
Deleting a Device .....	113
Deleting Multiple Devices .....	113
Download the Device List .....	113
Switch Ports .....	115
Customizing the Switch Ports Configuration Overview .....	115
Configuring Local Port Settings for One or More Switch Ports .....	116
Aggregating Switch Ports .....	117
Splitting Aggregated Switch Ports .....	118
Undoing Port Traffic Mirroring .....	119
Adding a Tag to One or More Switch Ports .....	119
Removing a Tag from One or More Switch Ports .....	119
Reports .....	120
Overview .....	120
Change Log .....	121
Searching for Change Events .....	121
Downloading Change Logs .....	121
Access Point .....	122
Filtering the Access Point Logs .....	122
Sending Access Point Logs by Email .....	122
Download Archived Access Point Logs .....	122
Download Access Point Logs .....	122
Switch .....	124
Filtering the Switch Logs .....	124
Sending Switch Logs by Email .....	124
Download Archived Switch Logs .....	124
Download Switch Logs .....	124
Alerts .....	125
Acknowledging Unprocessed Alerts .....	125
Deleting Unprocessed Alerts .....	125
Deleting Processed Alerts .....	125
Searching for Alerts .....	126

Licenses .....	127
Filtering the License Logs .....	127
Downloading License Logs .....	127
Settings .....	128
Overview .....	128
Account Management .....	129
Inviting a New User .....	129
Editing an Existing User .....	129
Searching for a User .....	130
Deleting a User .....	130
Organization Management .....	132
Creating a New Organization .....	132
Adding a Site to an Organization .....	132
Adding a Site Tag to an Organization .....	133
Invite Users to an Organization .....	133
Deleting an Organization .....	134
License Management .....	135
Adding a License Key .....	135
Bulk Adding Multiple Licenses .....	135
Searching for a License Key .....	136
Viewing the License History .....	137
Downloading License Key List .....	137
Inventory .....	138
Adding and Registering a Single Device to a Site .....	138
Adding a Single Device to the Inventory .....	138
Bulk Adding Multiple Devices to the Inventory .....	139
Bulk Adding and Registering Multiple Devices to a Site .....	140
Deleting a Device from the Inventory .....	140
Searching for a Device .....	140
Exporting the Inventory List .....	141
Firmware .....	142
Setting an Automatic Upgrade Window .....	142
Setting a Custom Device Upgrade Time .....	142
Performing a Manual Firmware Upgrade .....	143
Alert Settings .....	144
Configuring Alert Notifications .....	144
Add Device .....	145
Help .....	146
Contact Us .....	146
Nuclias Cloud Mobile App .....	147

Cloud - Supported Devices ..... 148

    Access Points ..... 148

    Switches ..... 152

# Getting Started

---



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 Nuclias, including how to create an account and adding a new device using the provided Default Profile template that sets up a Wi-Fi network with recommended settings.

Below you will find a list of topics to help you get started:

[Creating an Account](#)

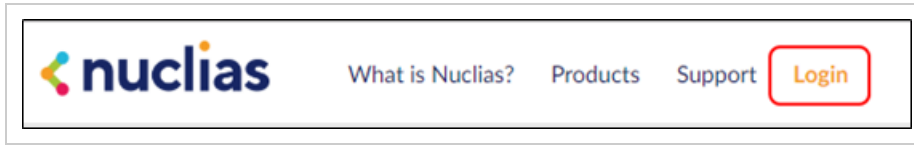
[Logging in to Nuclias Cloud](#)

[Adding a Device](#)

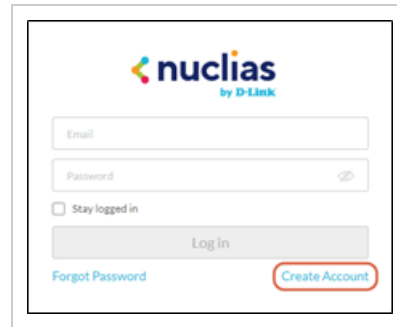
# Creating an Account

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

1. Go to [www.nuclias.com](http://www.nuclias.com) and click **Login**.



2. Click **Create Account**.



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

<b>Server Region</b>	Select which server region to store your data on.
<b>Country</b>	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:

<b>Email</b>	Enter your email address. This is also your username to log into the Nuclias Portal interface.
<b>Full Name</b>	Enter your full name
<b>Password</b>	Enter your account password.
<b>Confirm Password</b>	Confirm your password.
<b>Organization Name</b>	Enter your organization name. This will automatically create an organization with this name.
<b>Region</b>	Select a region. This will automatically create a Site using this region.

<b>Timezone</b>	Select a time zone.
<b>Address</b>	Enter your address.

4. Click **Create Account**.

5. 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.

# Log In and Out of Nuclias Cloud

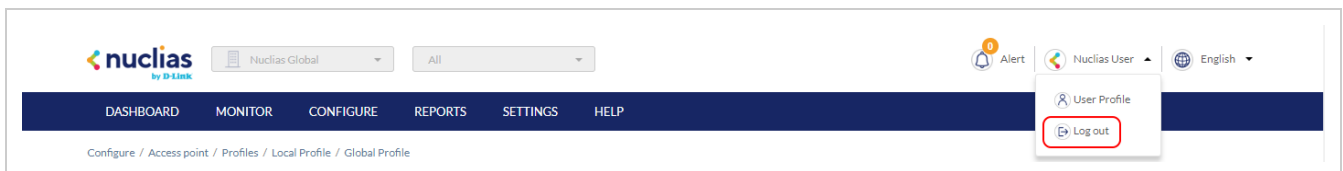
---

## Log In

1. In your web browser, go to [login.nuclias.com](https://login.nuclias.com).
2. Enter your registration email address and password.
3. Click **Log In**.

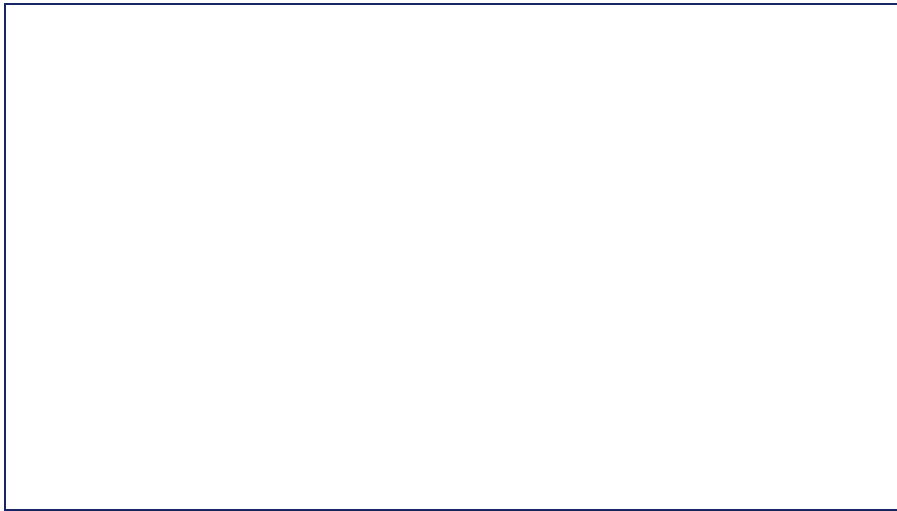
## Log Out

1. In the Nuclias Cloud portal, click the username in the top-right corner.
2. Click **Log out**.



# Adding a Device

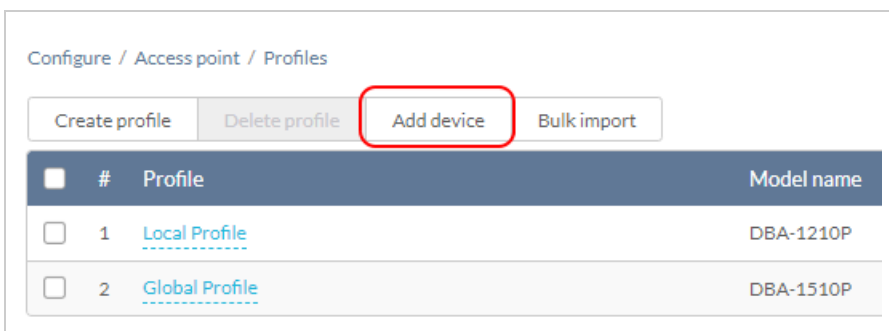
In order to be able to manage the network, devices need be added to the organization and assigned to Sites. There are multiple ways of adding devices to an organization.



## 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 **Configure > Access Point/Switch > Profiles**.
2. Click **Add device**.



Fill out the required information.

<b>Device UID</b>	Enter the device's UID found on the label printed on the device.  The UID may be listed in the format <b>XXXX-XXXX-XXXX</b> or <b>XXXXXXXXXXXX</b> . When entering the UID, do not include dashes.
<b>Device name</b>	Enter a name for the device.

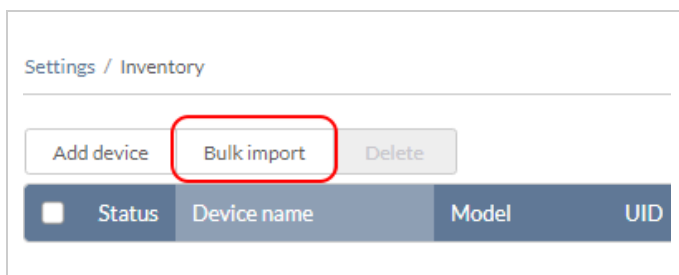
Site	Select a Site to link this device to.
Profile	Select a Profile for this device. The device will use the settings configured in that profile.
License Key	<p>[Optional] Enter the device license key.</p> <p><b>Note:</b> Every new device will be issued a one year free license key. Once expired, an additional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

Click **Save** when you are done.

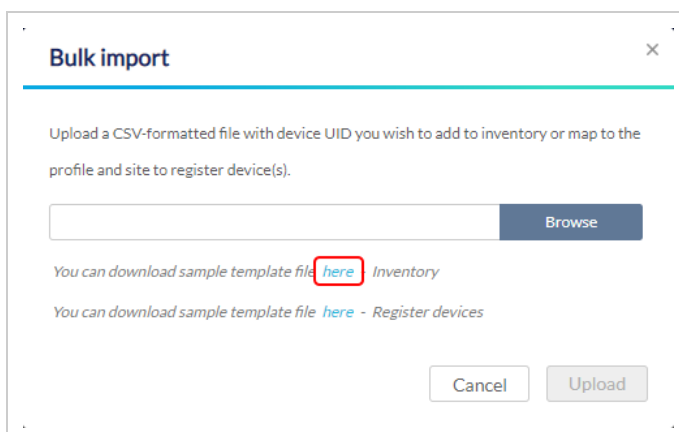
## Bulk Adding Devices to Inventory

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

1. Navigate to **Configure > Access Point/Switch > Profiles**.
2. Click **Bulk import**.



3. [Optional] Download the reference sample template.



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**.

# Bulk Assigning Devices to Sites

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

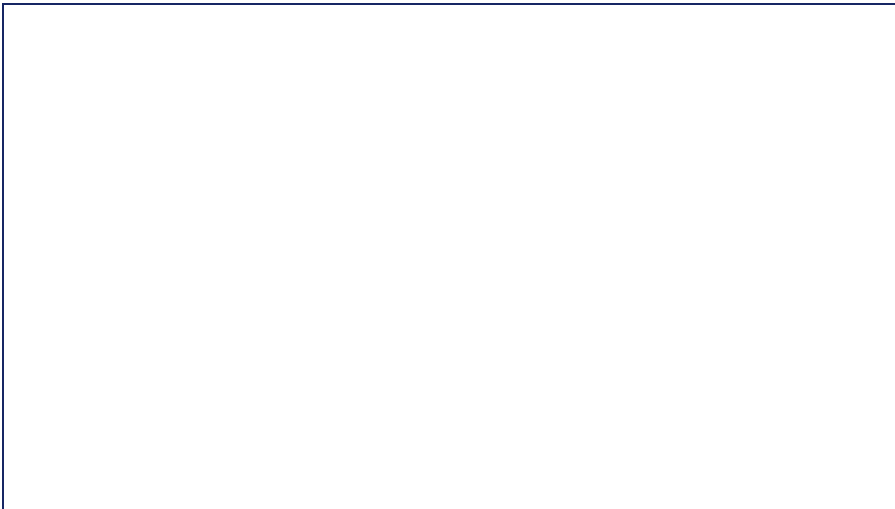
1. Navigate to **Configure > Access Point/Switch > Profiles**.
2. Click **Bulk import**.

# Adding a Device from QR Code

Devices can be imported and immediately registered to a Site by scanning the QR code on the back or bottom of the device.

# Nuclias Cloud

---



Below you will find a list of topics to help you learn how to use and navigate the Nuclias Cloud Online Portal.

[Introduction](#)

[Interface Overview](#)

[Dashboard](#)

[Monitor](#)

[Configure - Access Point](#)

[Configure - Switch](#)

[Reports](#)

[Settings](#)

[Help](#)

# Introduction

---

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

## Audience

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

## Conventions

<b>Boldface Font</b>	Indicates a button, a toolbar icon, menu, or menu item. For example: Open the <b>File</b> menu and choose <b>Cancel</b> . Used for emphasis.  May also indicate system messages or prompts appearing on screen. For example: <b>You have mail</b> .  Bold font is also used to represent file names, program names, and commands. For example: Use the <b>Copy</b> 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. <b>Device &gt; Port &gt; Port Properties</b> means the Port Properties menu option under the Port menu option that is located under Device.

## 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 Cloud 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 Cloud 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.

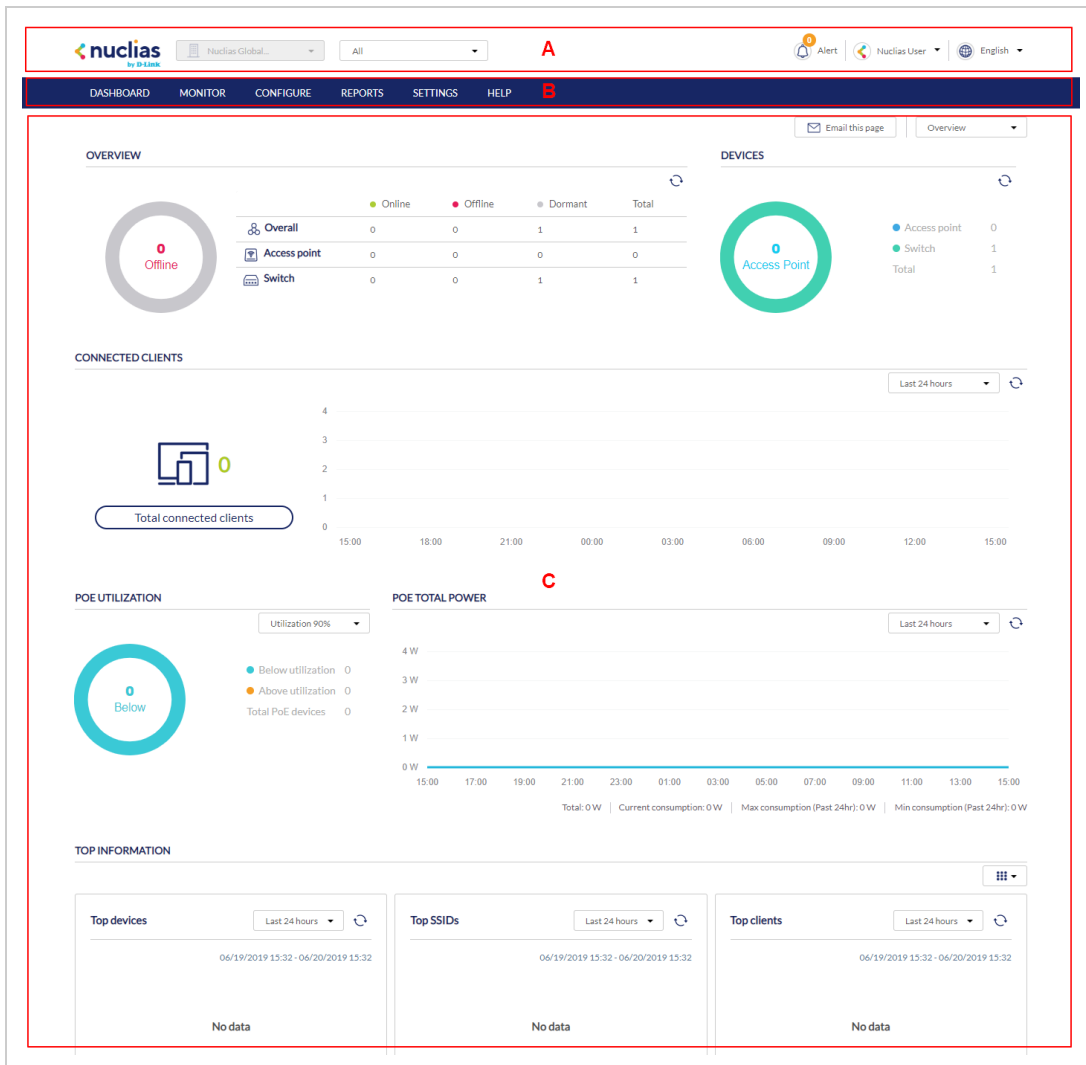
**Site:** A Site is a label representing a physical location. Sites are used to group devices together for easier management. Sites can also be associated with a Site Tag, in which case the Site will branch off from the Site Tag. Examples of Sites include cities, branch offices, and work floors, depending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

<b>Admin</b>	An administrator has full access to all elements of the Portal interface and has full management capabilities.
<b>Editor</b>	An editor shares similar rights as an administrator, but cannot add or delete devices, users, or organizations.
<b>Monitor</b>	A monitor is limited to read-only access to configurations and analysis, and cannot configure or edit devices, users, or organizations.
<b>Viewer</b>	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.

# Interface Overview

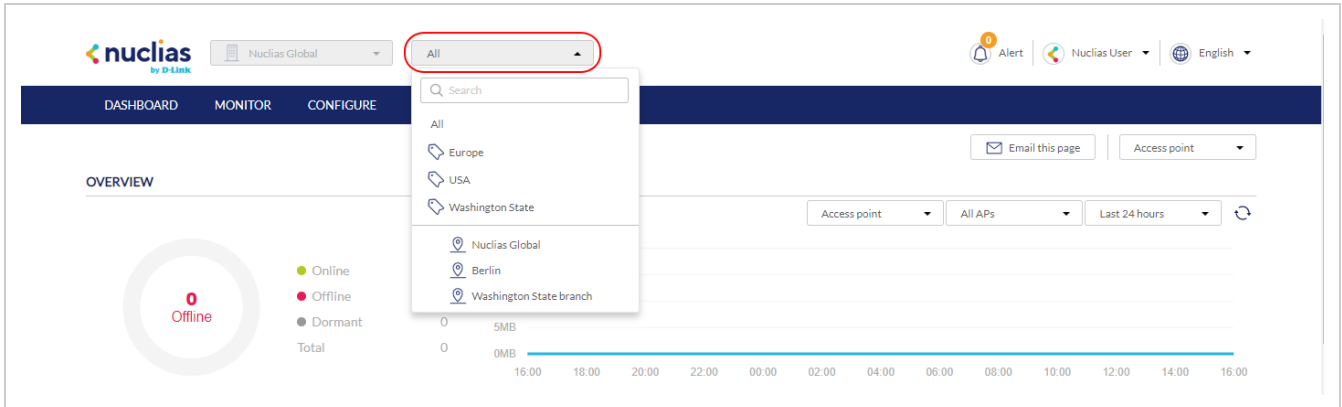


Section	Item	Description
A	<a href="#">Global Toolbar</a>	Provides access to the organization and site selection menu as well as alerts, user account, and language menu.
B	<a href="#">Management Toolbar</a>	Provides access to the various device management, report, and inventory sections.
C	<a href="#">Dashboard</a>	The interactive dashboard to manage and configure through the Nuclias Portal. Information and options displayed in the dashboard depend on the currently active management section.

# Global Toolbar

## 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. For most configuration options, it is necessary to select a Site to manage. Site Tags are marked by a tag icon, while Sites are marked by a single pin icon.



## 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.

## 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.



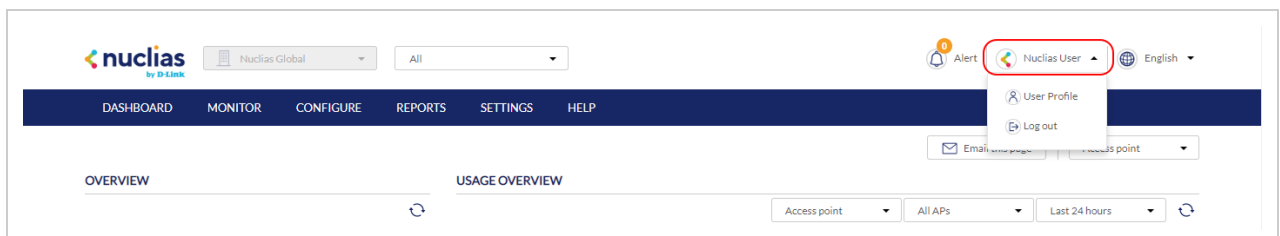
## Editing a User Profile

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.

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**
    1. Click the username in the Name field.
    2. Enter a new name and press **Enter** or click outside of the field.
  - b. **Change password**
    1. Enter your current password in the **Current Password** field.
    2. Enter a new password in the **New Password** field.
    3. Enter the new password again in the **Confirm Password** field.
  - c. **Edit profile image**
    1. Click on the green pencil icon in the bottom-right corner of the profile image.
    2. In the Upload Image window click **Browse** and navigate to the image you want to use.
    3. Click **Save**.
  - d. **Email user information**
    1. Click the **Email this page** button to send your user information to your registered email address.
4. Click **Save**.

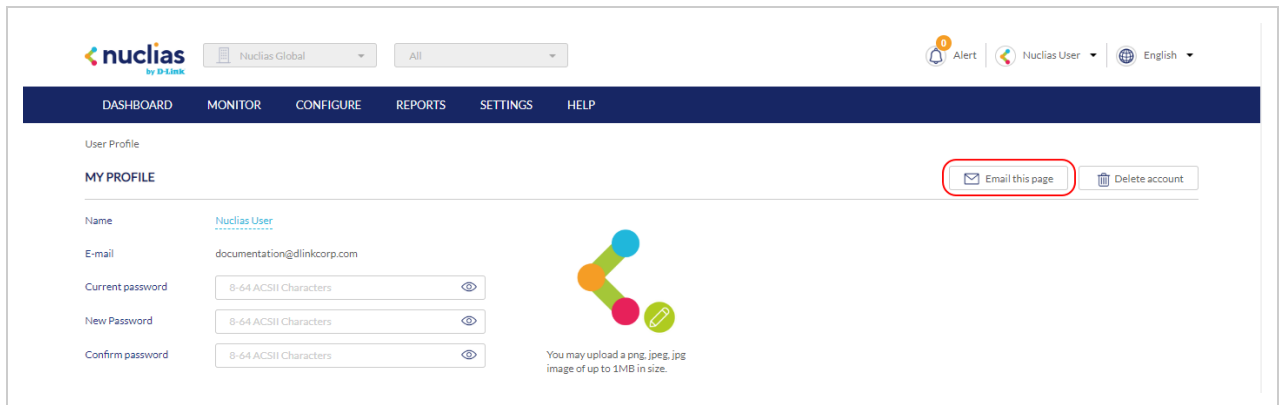
## Sending A User Profile Snapshot by Email

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



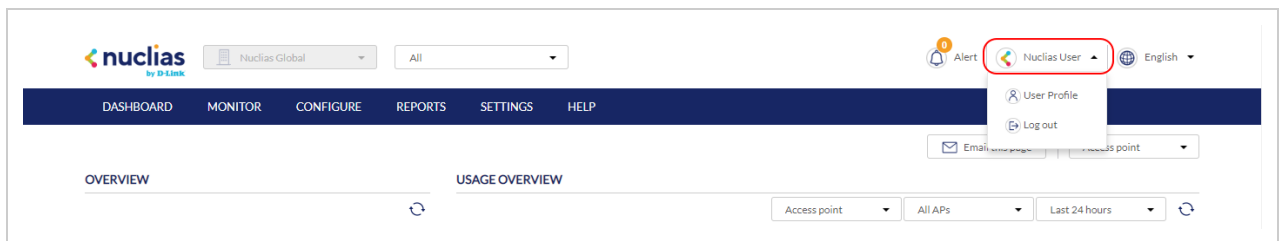
2. Select **User Profile**.
3. Click **Email this page**.

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

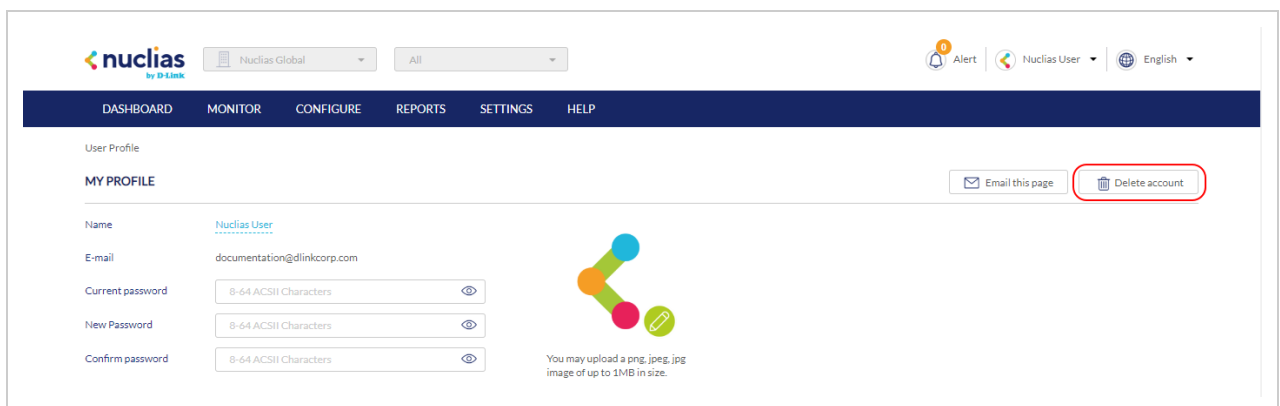


## Deleting a User Account

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



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

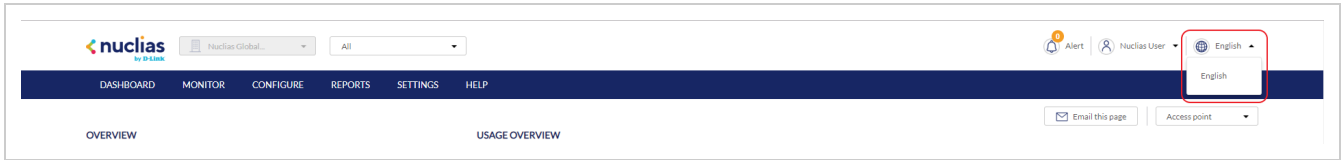


4. Enter your account password and click **Save**.  
 Note: Deleting an account will remove all data associated with this user. This is permanent and cannot be undone.

## Language Menu

### 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.

# 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.

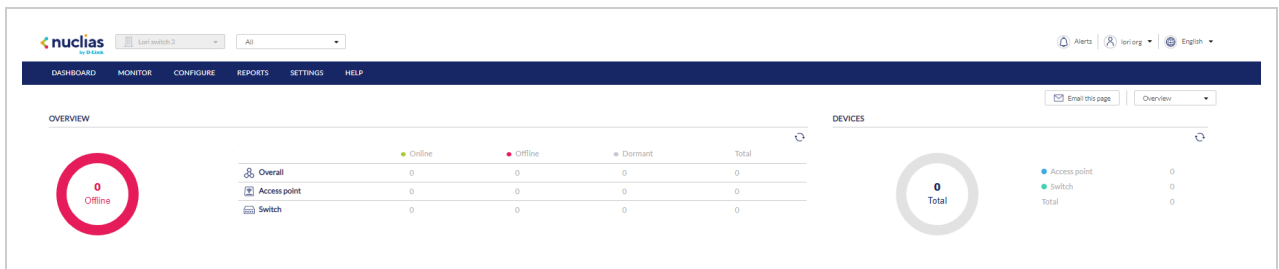
<b>Dashboard</b>	<p>The Dashboard offers users a real time overview of the status of the network including device and user activity and performance.</p> <p>Refer to the <a href="#">Dashboard</a> section for more information.</p>
<b>Monitor</b>	<p>The Monitor section grants access to detailed device, client, and event logs as well as the interactive map and floor plan tools.</p> <p>Refer to the <a href="#">Monitor</a> section for more information.</p>
<b>Configure</b>	<p>The Configure section grants access to the main configuration section including Profiles and individual device settings.</p> <p>Refer to the <a href="#">Configure - Access Point</a> or <a href="#">Configure - Switch</a> sections respectively for more information.</p>
<b>Reports</b>	<p>The Reports section grants access to detailed reports for changes on the platform, device activity,</p> <p>Refer to the <a href="#">Reports</a> section for more information.</p>
<b>Settings</b>	<p>The Settings section grants access to organization and user management, the device and license inventory, and firmware management.</p> <p>Refer to the <a href="#">Settings</a> section for more information.</p>
<b>Help</b>	<p>The Help section offers users a platform to submit support tickets and provide feedback.</p> <p>Refer to the <a href="#">Help</a> section for more information.</p>

# Dashboard

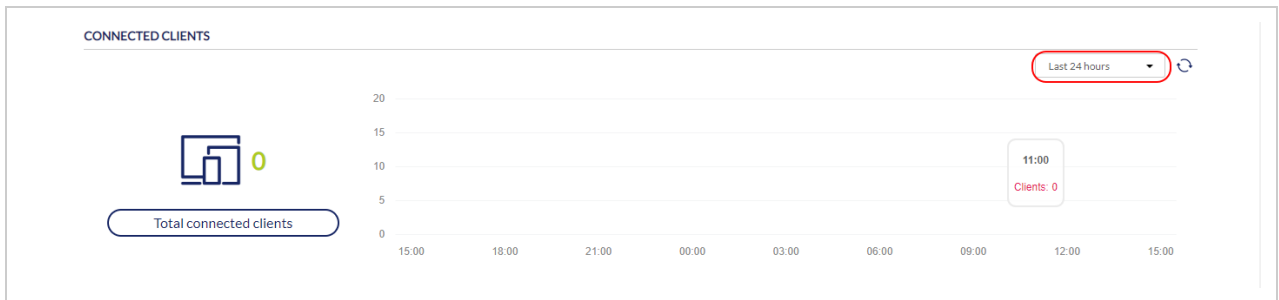
The Dashboard page is the default window that is displayed after logging into the Nuclias Cloud Portal interface. It can also be reached by clicking the Dashboard tab in the tool bar, and. It provides an overview of the devices, connected clients, and device activity for the selected organization. It 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.

## Customizing the Overview

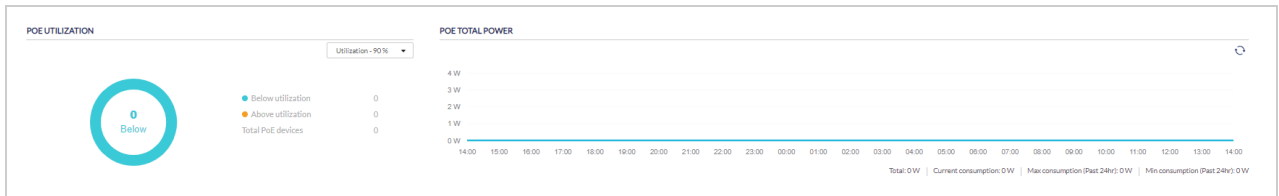
1. Navigate to the Dashboard page
2. Select a Site from the Site menu.  
Note: Selecting a Site will only show network and device information for the selected Site. Select **All** to show network, client, and device information for all Sites.
3. In the Usage Overview section, select device type or SSID, the devices(s) and SSID(s), and the time frame from the drop-down menus.



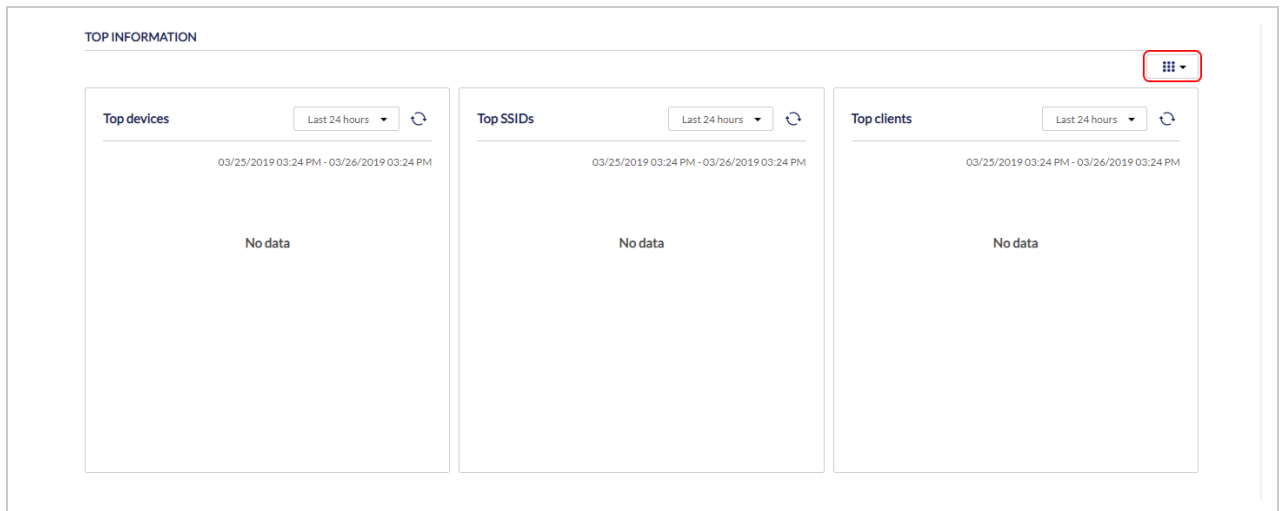
4. In the Connected Clients section, select a time frame from the drop-down menu.



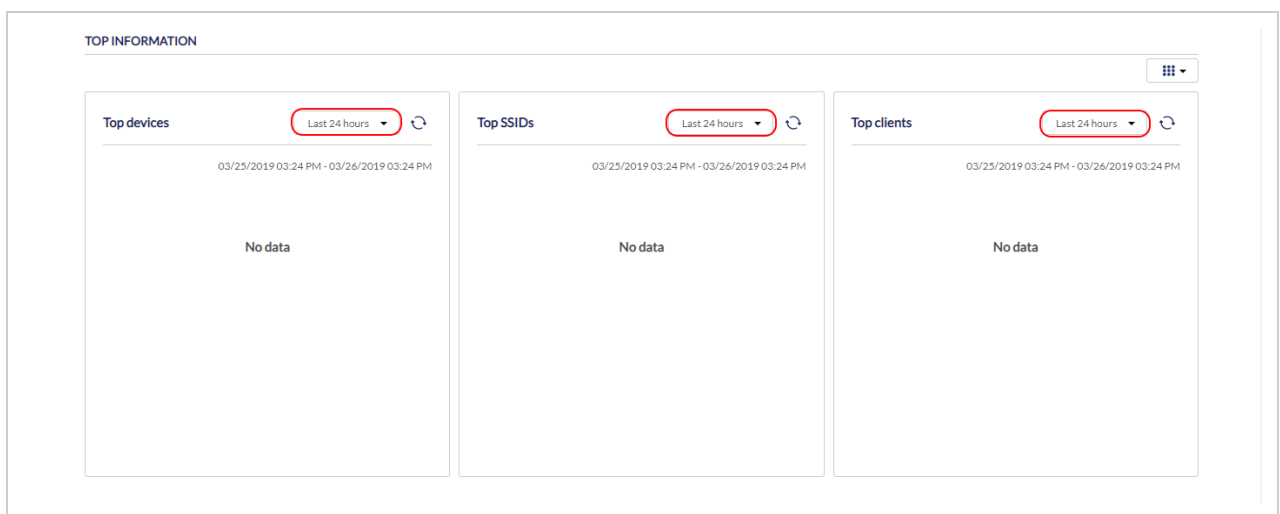
5. The PoE Utilization section helps manage and monitor how much power each switch is using.
6. The PoE Total Power section shows how much power is being used by PoE devices by the hour.



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



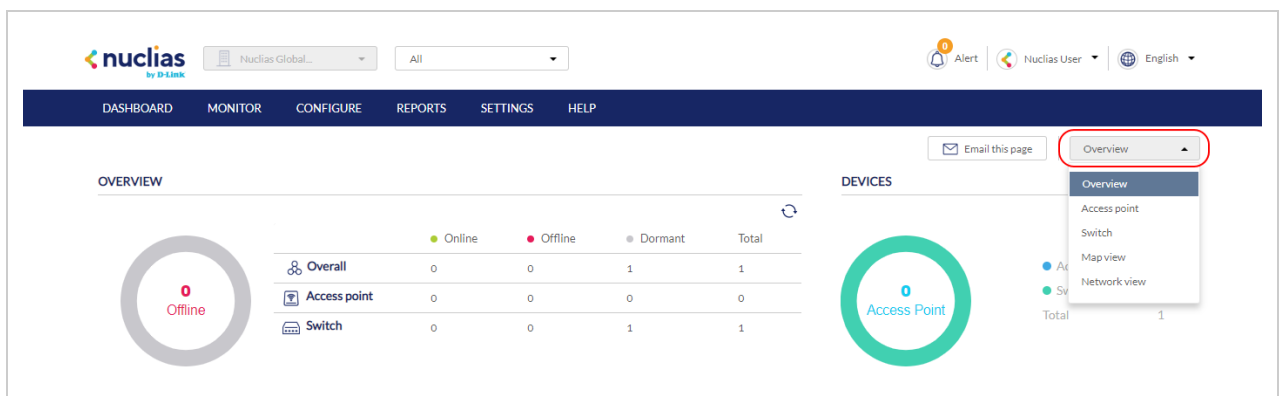
8. Check the information parameters to display the corresponding top information in the overview window.
9. In the Top Information section, select a time frame from the drop-down menu for each enabled section.



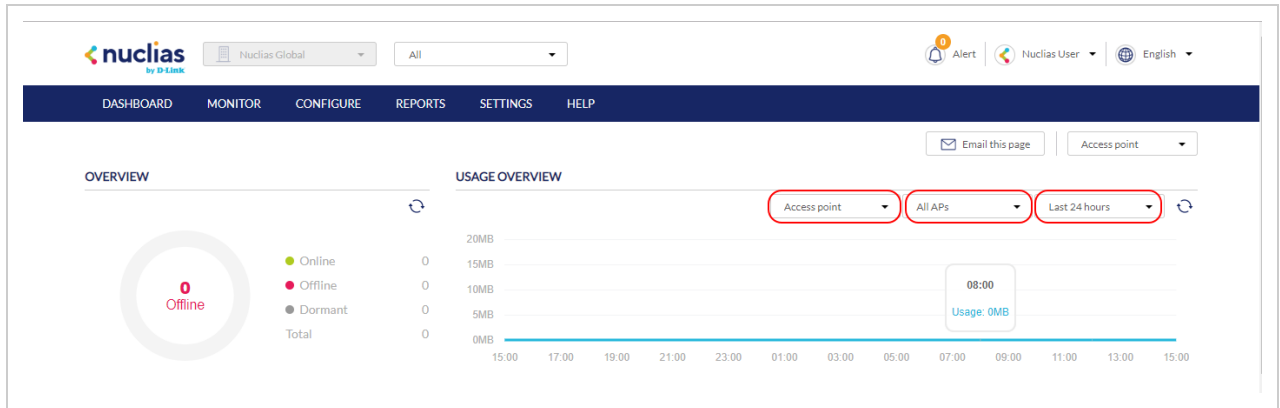
## Sending a Dashboard Snapshot by Email

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

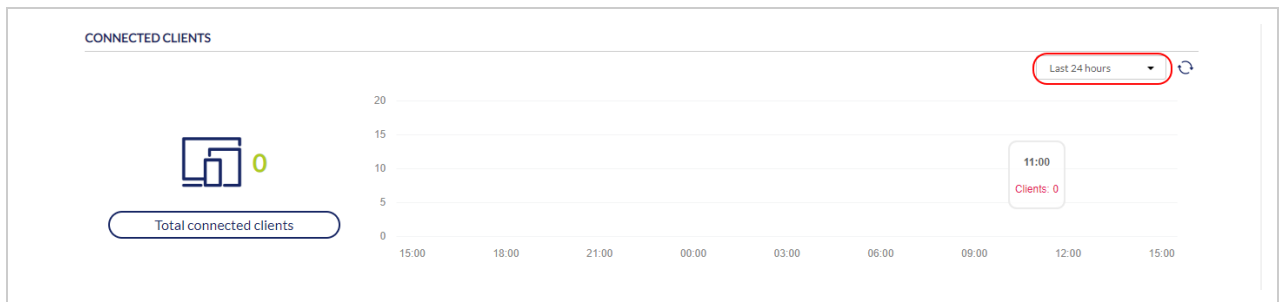
1. Navigate to the Dashboard.
2. Select a dashboard viewing mode from the drop-down menu in the top-right of the screen.  
Note: The information and subsequent sections on the dashboard vary depending on the currently selected viewing mode.



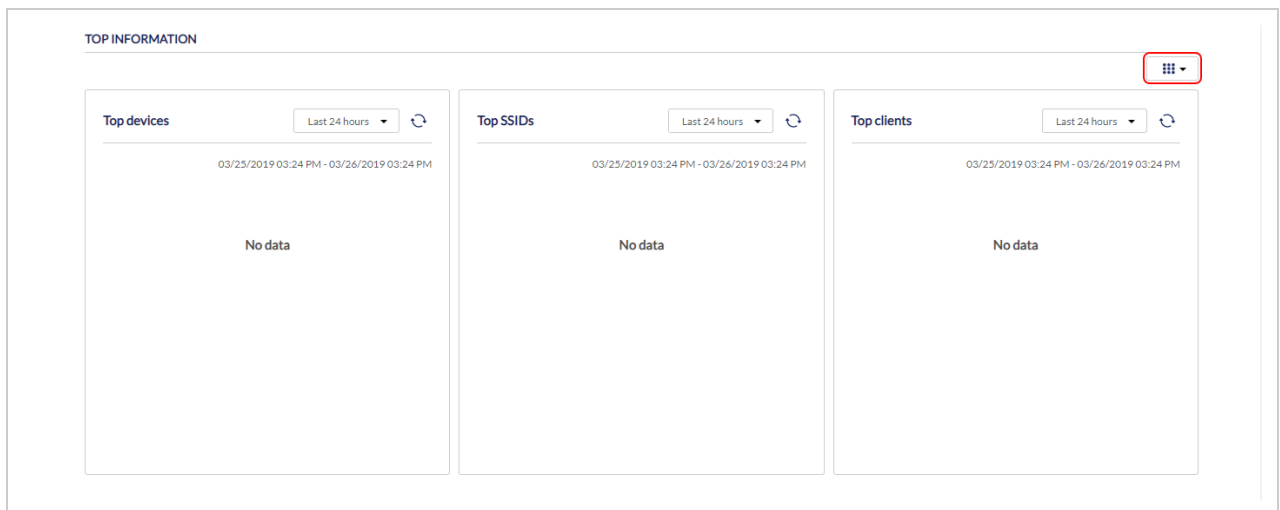
3. In the Usage Overview section, select device type or SSID, the device(s) and SSID(s), and the time frame from the drop-down menus.



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.



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

8. Click **Email this page** in the top-right.
9. In the Email report window, enter the email address of the recipient(s).  
**Note:** Up to 10 recipients can be added, separated by “,”.
10. Click **Send email**.

# Overview

---

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

<a href="#">Switch</a>	<p>The Switch section provides detailed logs for switch devices, connected clients, and events.</p> <p>Refer to the <a href="#">Switch</a> section for more information.</p>
<a href="#">Access Point</a>	<p>The Access Point section provides detailed logs for AP devices, connected clients, and events.</p> <p>Refer to the <a href="#">Access Point</a> section for more information.</p>
<a href="#">Map</a>	<p>The Map section provides users with an interactive map that offers a geographical overview of the organization's Sites.</p> <p>Refer to the <a href="#">Map</a> section for more information.</p>
<a href="#">Floor Plans</a>	<p>The Floor Plans section allows users to create, edit, manage, and delete floor plans.</p> <p>Refer to the <a href="#">Floor Plans</a> section for more information.</p>

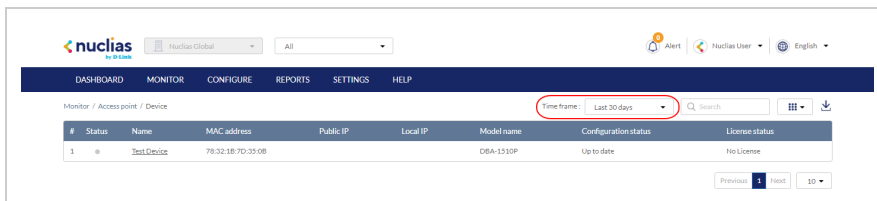
# Monitor-Access Point

## Devices

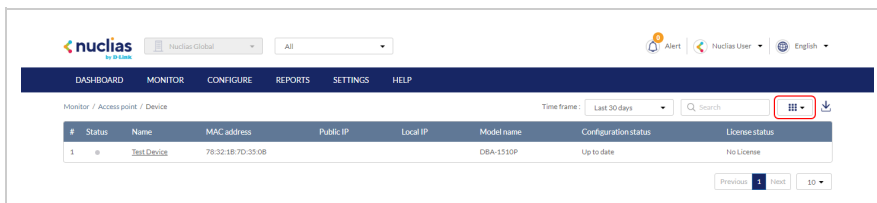
From the Devices window, users can consult a detailed log of events occurring on the network. Users can also filter events using specific event filter parameters, including event type and time period.

## Customizing the Device Monitor Overview

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



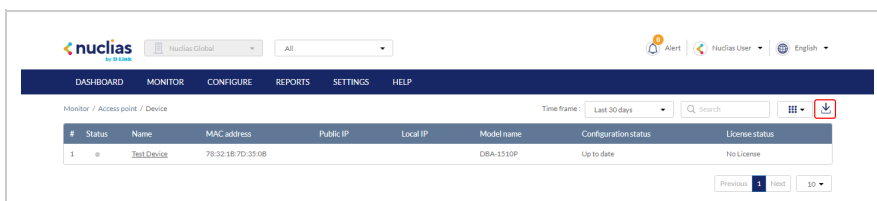
3. Click the filter parameter icon.



4. Click the checkbox next to the parameters to display them in the overview.  
Note: All checked parameters will automatically appear.

## Downloading Device Monitoring Logs

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

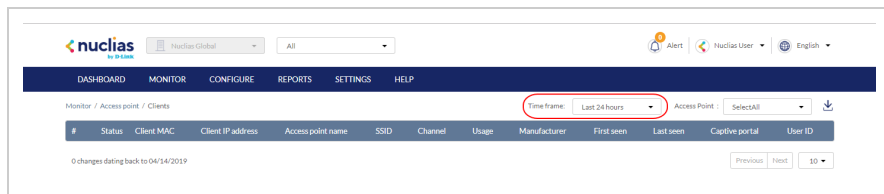


## Clients

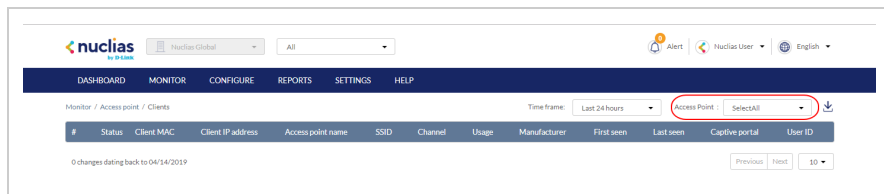
From the Clients window, users can consult a detailed overview of all currently registered devices with additional information including status, clients, and general settings.

## Customizing the Client Monitor Overview

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

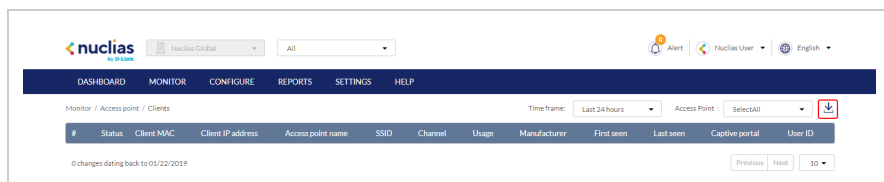


3. Select an access point from the access point drop-down menu.



## Downloading Client Monitoring Logs

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



## 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.

## Filtering Event Log Parameters

1. Navigate to **Monitor > Access Point > Event Logs**.
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.

## Downloading Event Logs

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

Monitor / Access point / Event log

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

Reset filters Filter Download

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

Previous Next 10

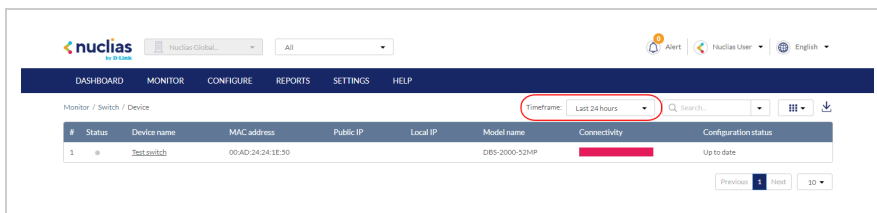
# Monitor- Switch

## Devices

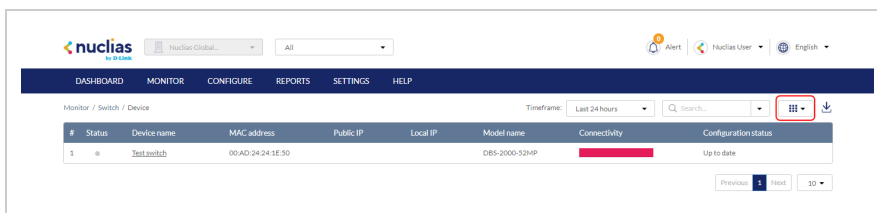
From the Devices window, users can consult a detailed log of events occurring on the network. Users can also filter events using specific event filter parameters, including event type and time period.

### Customizing the Device Monitor Overview

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



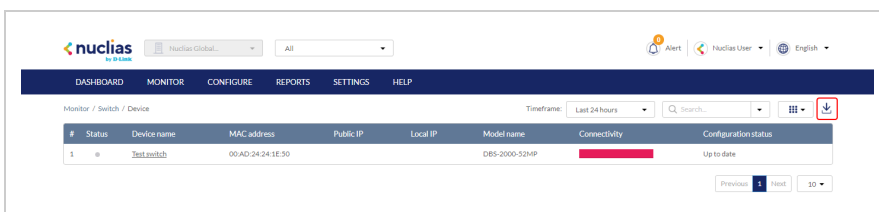
3. Click the filter parameter icon.



4. Click the checkbox next to the parameters to display them in the overview.  
Note: All checked parameters will automatically appear.

### Downloading Device Monitoring Logs

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



### Changing the Device Site and Profile

1. Navigate to **Monitor > Switch > Device** and select a device from the list.
2. Select the **Basic** tab in the top-right of the screen.
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**.

## Changing the Device Connection Type to DHCP

1. Navigate to **Monitor > Switch > Device** and select a device from the list.
2. Select the **Basic** tab in the top-right of the screen.
3. In the IP Connection section, select a 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. Select a VLAN ID from the drop-down menu to assign the switch to a VLAN.  
Note: VLAN and Voice VLAN settings can be configured on the Profile Basic Settings page. Refer to the [Configuring Basic Switch Profile Settings](#) section for more information.
6. Click **Apply**.

## Changing the Device Connection to Static IP

1. Navigate to **Monitor > Switch > Device** and select a device from the list.
2. Select the **Basic** tab in the top-right of the screen.
3. In the IP Connection section, select a 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:

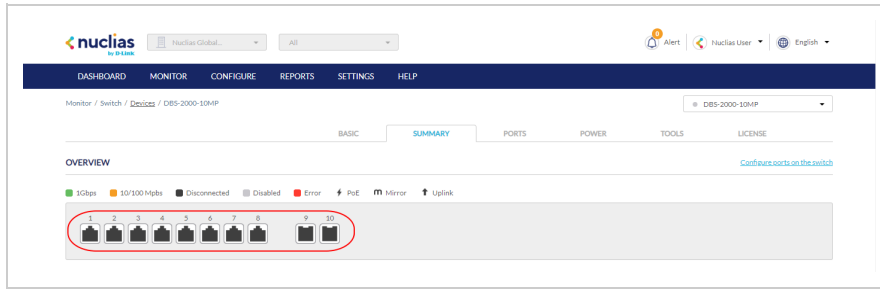
Local IP	Enter a valid IP address.
VLAN	[Optional] Check to enable VLAN functionality. This segments traffic on the SSID.
Subnet Mask	Enter a Subnet Mask.
Gateway	Enter a default gateway address.
DNS #1	Enter a primary DNS address.
DNS #2	[Optional] Enter a secondary DNS address.
DNS #3	[Optional] Enter a tertiary DNS address.

6. Click **Apply**.

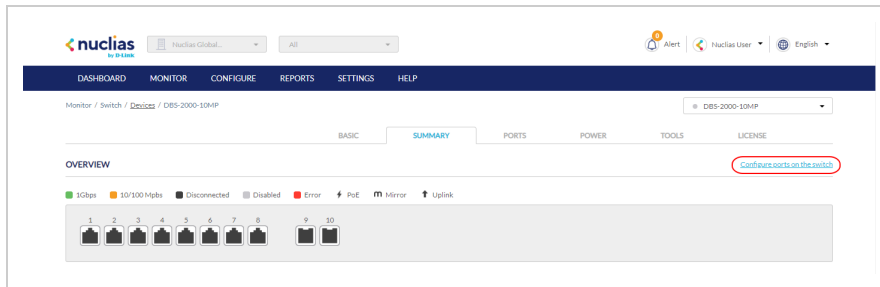
## Viewing and Customizing the Switch Performance Summary

1. Navigate to **Monitor > Switch > Device** and select a device from the list.
2. Select the **Summary** tab in the top-right of the screen.
3. In the Connectivity and CPU Utilization sections, select a time frame from the drop-down menu to show data for the specified time frame. Click the refresh icon to renew the data.

4. [Optional] Click on a port on the interactive switch diagram to view port-specific information.



5. [Optional] Click Configure ports on the switch to go to the switch port configuration window. Refer to the [Switch Ports](#) section for more information.



## Viewing and Customizing the Switch Port Status Overview

1. Navigate to **Monitor > Switch > Device** and select a device from the list.
2. Select the **Ports** tab in the top-right of the screen.
3. Click on a port on the interactive switch diagram to view specific information for that port.
4. Select a time frame from the drop-down menu to show data for the specified time frame. Click the refresh icon to renew the data.
5. In the Current Configuration section, click **Edit** to configure the selected port's settings. Specify the following information:

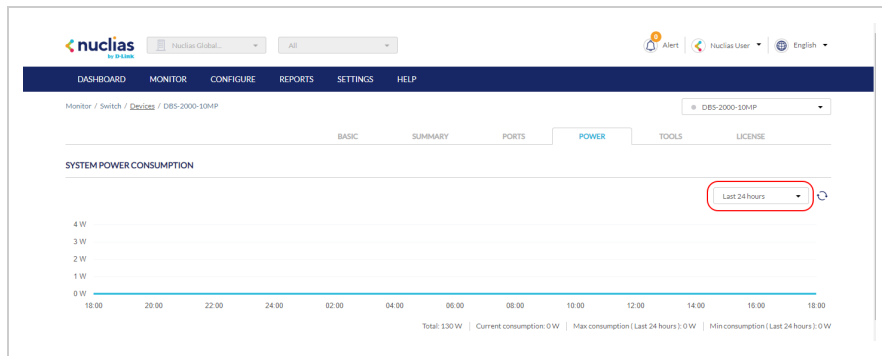
Port name	Enter a name for the port. If multiple ports are selected, this name will be applied to all ports.
Port state	Choose to enable or disable the port.
RSTP	Choose to enable or disable RSTP Note: RSTP cannot be used in conjunction with LBD.
STP guard	If RSTP is enabled, choose the guard type.  Disabled: Do not use root guard enhancement.  Root guard: Root guard enhancement allows administrators to define the position of the root bridge port in the network.

LBD	<p>Choose to enable or disable LBD</p> <p>Note: LBD cannot be used in conjunction with RSTP.</p>
Type	<p>Choose the function type of the port.</p> <p>Trunk: Sends and receives tagged data from different VLANs.</p> <p>Access: Only sends and receives untagged data from the VLAN the port belongs to.</p>
Native VLAN	<p>Enter the ID of the native VLAN the port belongs to.</p>
Allowed VLANs	<p>Enter the IDs of the VLANs that can route traffic through this port. Enter All to allow all traffic from all VLANs to pass through this port.</p>
Tags	<p>Enter a descriptive tag for the port. Multiple tags can be entered. If multiple ports are selected, any tags will be applied to all ports.</p>
Link (RJ45)	<p>Choose the maximum link speed of the port. Select <b>Auto</b> to allow the port to auto-negotiate port speed with the partner port or device.</p>
PoE	<p>Choose to enable or disable PoE functionality on this port.</p> <p>Note: The PoE setting will only apply to ports that support Power over Ethernet.</p>
Port Schedule	<p>Choose a port schedule. Port schedules are configured separately. Refer to the <a href="#">Creating a Switch Port Schedule</a> section.</p>

6. Click **Apply**.
7. In the Cable Test window of the Troubleshooting section, click **Test** to perform a cable test on this port. This will scan the physical connection to the port for any problems.
8. In the Cycle Port window of the Troubleshooting section, click **Test** to perform a port cycle test on this port. This will disable and re-enable the port.
9. In the Overview Packets section, select a time frame from the drop-down menu to display data for the selected time period.

## Viewing and Customizing The Switch Power Consumption Overview

1. Navigate to **Monitor > Switch > Device** and select a device from the list.
2. Select the **Power** tab in the top-right of the screen.
3. Select a time frame from the drop-down menu to show data for the specified time frame. Click the refresh icon to renew the data.



## Performing a Device Ping Test

1. Navigate to **Monitor > Switch > Device** and select a device from the list.
2. Select the **Tools** tab in the top-right of the screen.
3. In the IP address/FQDA field in the Ping section, enter a valid IP address or FQDA.
4. Click **Ping**.

## Performing a MAC Forwarding Table Test

1. Navigate to **Monitor > Switch > Device** and select a device from the list.
2. Select the **Tools** tab in the top-right of the screen.
3. In the MAC Forwarding Table section, click **Run**.

## Performing a Cable Test

1. Navigate to **Monitor > Switch > Device** and select a device from the list.
2. Select the **Tools** tab in the top-right of the screen.
3. In the Cable Test section, enter the port numbers to run the cable test on.  
Note: The scan will only be performed on ports with a physical connection.
4. Click **Test**.

## Performing a Port Cycle Test

1. Navigate to **Monitor > Switch > Device** and select a device from the list.
2. Select the **Tools** tab in the top-right of the screen.
3. In the Cycle Port section, enter the port numbers to run the cable test on.
4. Click **Test**.

## Performing a Blink LED Test

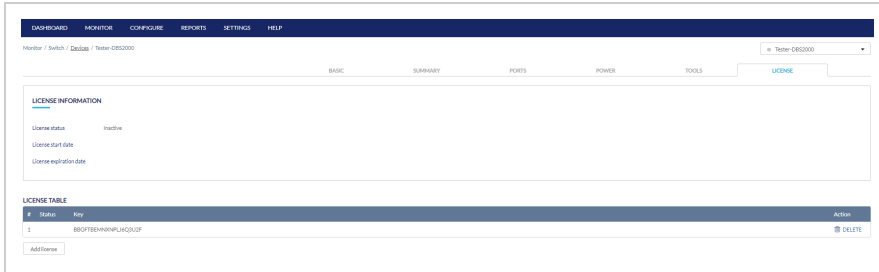
1. Navigate to **Monitor > Switch > Device** and select a device from the list.
2. Select the **Tools** tab in the top-right of the screen.
3. In the Others section, click **Start**.  
Note: The Start button will change to Stop once the test begins.
4. Click **Stop** to end the test.

## Manually Rebooting a Device

1. Navigate to **Monitor > Switch > Device** and select a device from the list.
2. Select the **Tools** tab in the top-right of the screen.
3. In the Others section, click **Reboot**.

## Adding a License Key to a Device

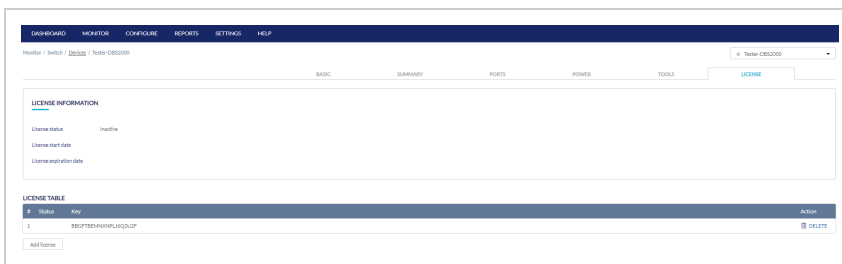
1. Navigate to **Monitor > Switch > Device** and select a device from the list.
2. Select the **License** tab in the top-right of the screen.
3. In the License Table section, click **Add License**.
4. Enter a valid license key.
5. Click **Save**.



## Deleting a License Key From a Device

1. Navigate to **Monitor > Switch > Device** and select a device from the list.
2. Select the **License** tab in the top-right of the screen.
3. In the License Table section, from the license key list, click **Delete** under the Actions column of the license key you wish to delete.
4. 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.

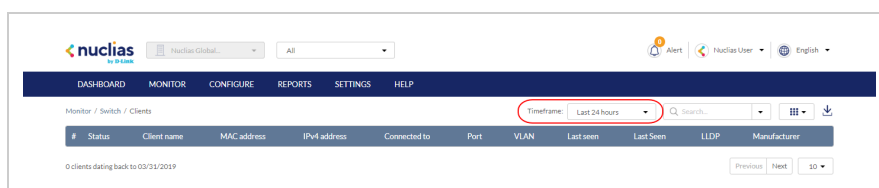


## Clients

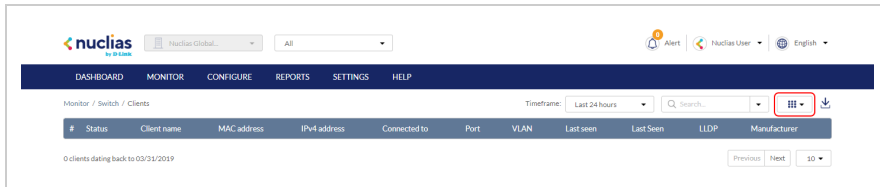
From the Clients window, users can consult a detailed overview of all currently registered devices with additional information including status, clients, and general settings.

## Customizing the Client Monitor Overview

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



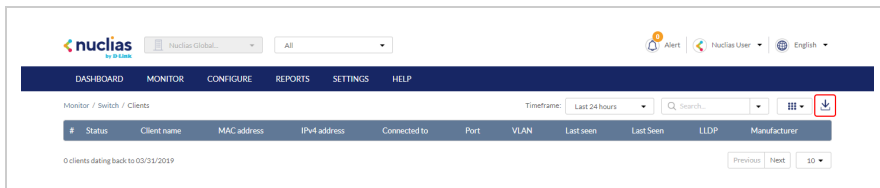
3. Click the parameter filter icon.



4. Click the checkbox next to the parameters to display them in the overview.  
Note: All checked parameters will automatically appear.

## Downloading Client Monitoring Logs

1. Navigate to **Monitor > Switch > Clients**.
2. From the device list, click the download icon in the top-right.



## Event Logs

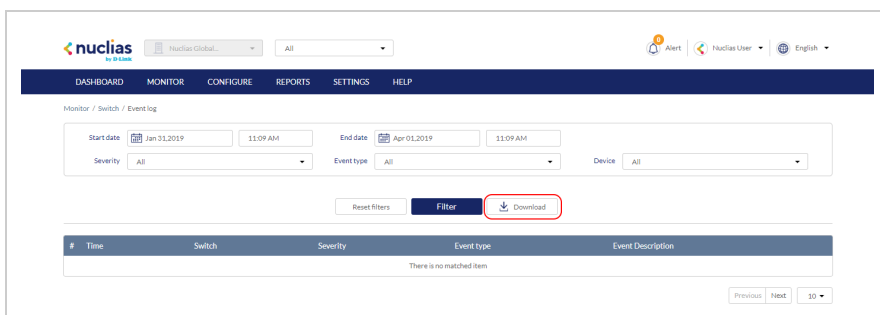
From the Events Logs window, users can consult a detailed log of events occurring on the network. Users can define event filter parameters, including event type and time period.

### Filtering Event Log Parameters

1. Navigate to **Monitor > Switch > Event Logs**.
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 the Device drop-down menu and select a device who's events logs you wish to filter.  
Note: Select All to show event logs for all devices.
7. Click **Filter** to display all events matching the defined parameters.
8. [Optional] Click **Reset filters** to reset all currently set parameters.

### Downloading Event Logs

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





# Map

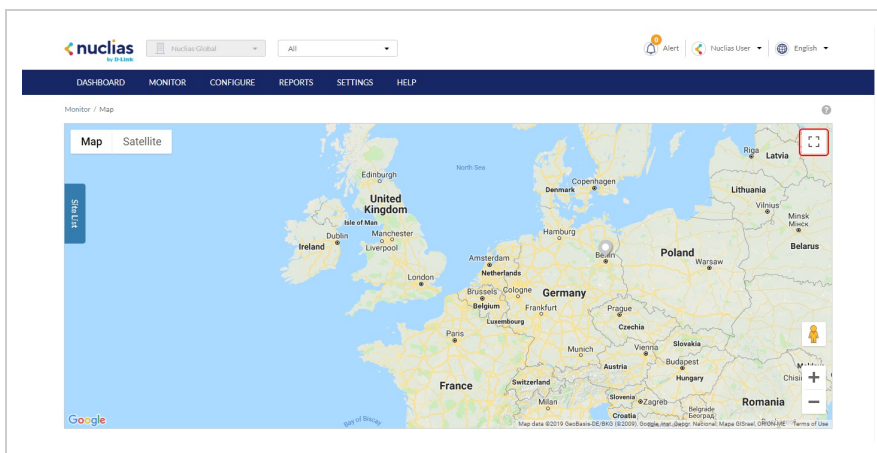
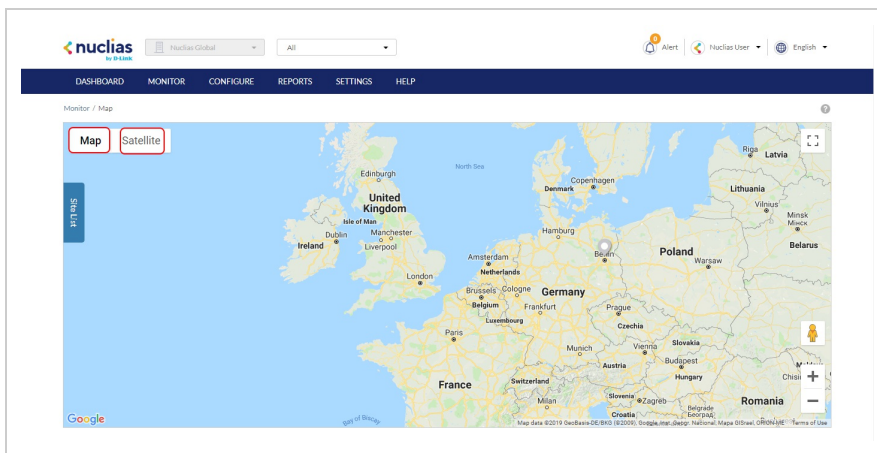
From the Map window, users can consult a geographical overview of the organization's Sites in the form of an interactive world map.

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

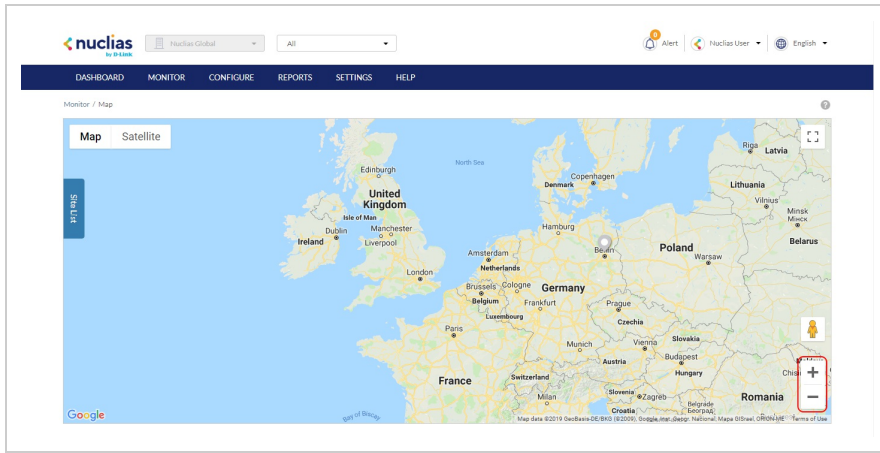
## Navigating the Map

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.

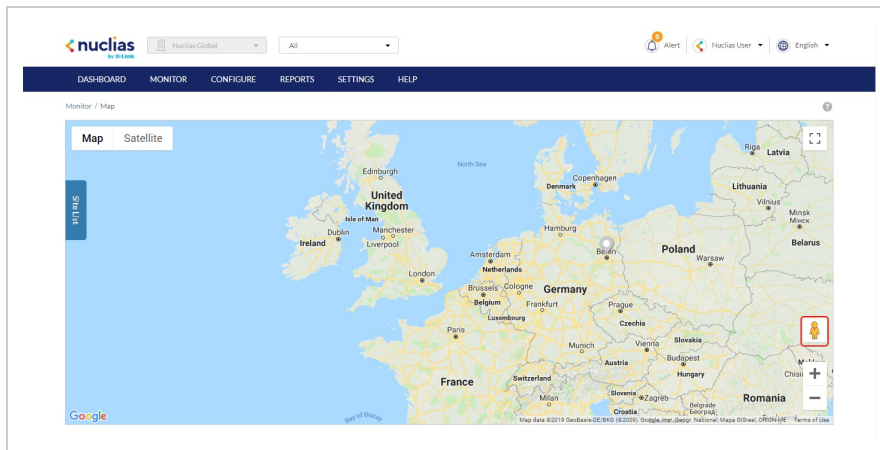
1. Navigate to **Monitor > Map**.
2. Click **Map** or **Satellite** in the top-left corner of the map to switch between the street map and satellite image map.



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 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.



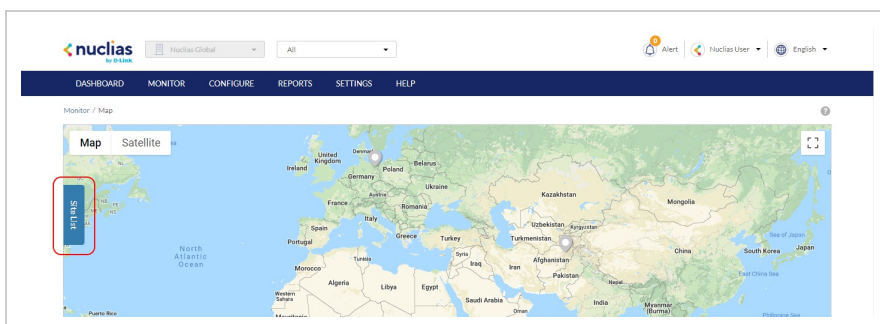
6. Drag and drop the Pegman icon anywhere on the map to open the street view of that location.  
**Note:** When in street view, click the return arrow to return to the map view.



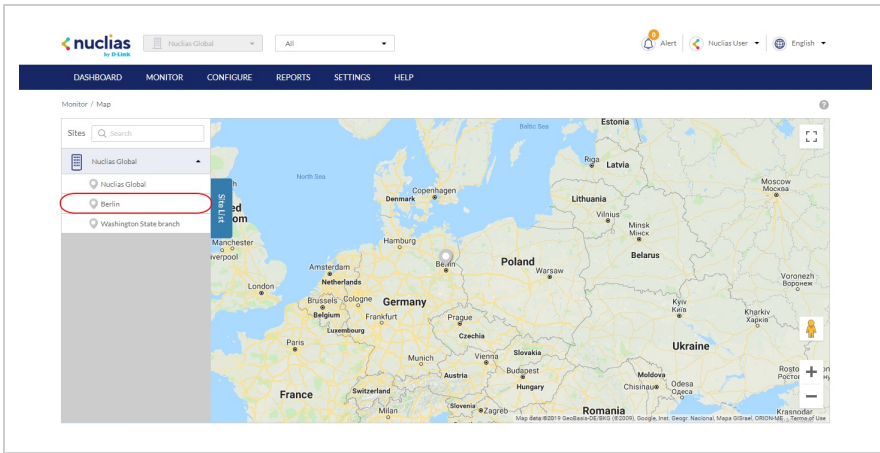
## Navigating Sites on the Map Using the Site List

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 **Monitor > Map**.
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. The map will automatically navigate to the Site's location on the map.



6. Hover the cursor over the Site icon to view basic information.

7. [Optional] Click the Site name in the Site window to open the Dashboard view for that Site.

# Floor Plans

Floor plans offer 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.

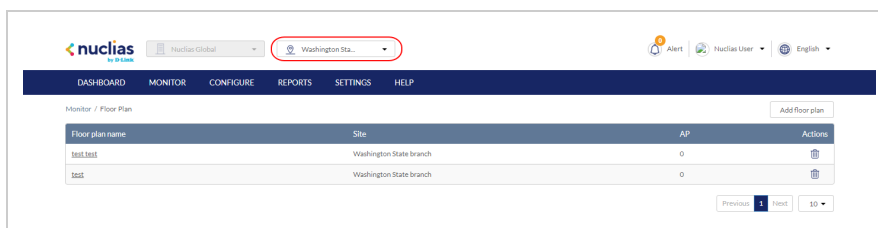
## Adding a Floor Plan

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 **Monitor > Floor Plan**.
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.



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



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

## Editing Floor Plan

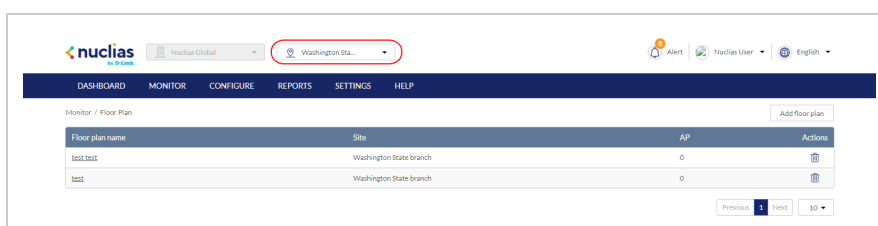
Users can add and remove device icons to floor plans for a visual overview of the device placement, edit the floor plan name, and upload a custom floor plan image.

## 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 **Monitor > Floor Plan**.
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.



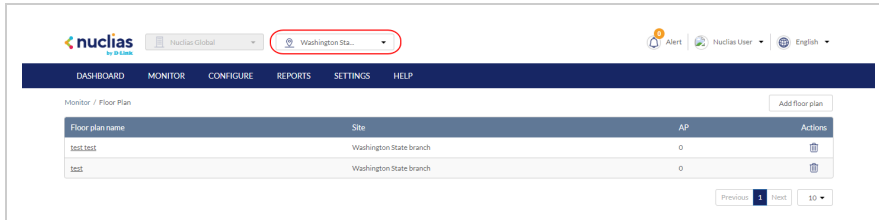
3. From the floor plan list click on the floor plan name.

- Click and drag a device from the Unplaced Devices list onto the floor plan to place it on the floor plan.
- Click **Save**.

## Removing Devices from a Floor Plan

- Navigate to **Monitor > Floor Plan**.
- 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.



- From the floor plan list, click on the floor plan name.
- 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.

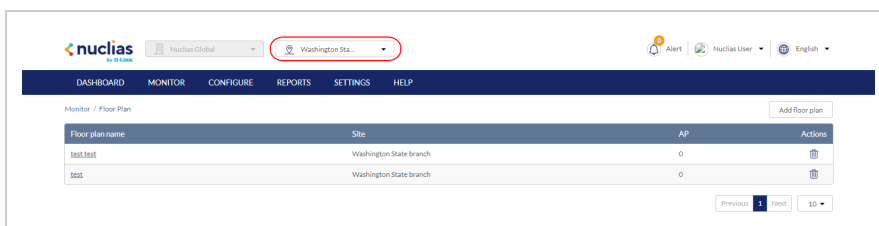


- Click **Save**.

## Editing a Floor Plan Name

- Navigate to **Monitor > Floor Plan**.
- 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.



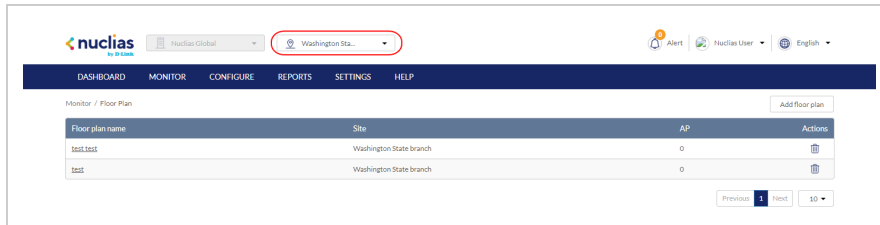
- From the floor plan list, click on the floor plan name.
- Click the floor plan name in the Floor Plan Name field.



# Deleting a Floor Plan

1. Navigate to **Monitor > Floor Plan**.
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.



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



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

# Configure-Access Points

---

From the Configure-Access Points section, users can manage Profiles and devices for the organization.

The following sections provide more detailed information about Profile and device management respectively.

<a href="#">Profiles</a>	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.
<a href="#">Devices</a>	From the Devices section, users can add a single device, or bulk import a group of devices, and configure individual device settings.
<a href="#">IP ACLs</a>	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.
<a href="#">MAC ACLs</a>	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.
<a href="#">Local Authentication</a>	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.
<a href="#">Splash Page Editor</a>	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.
<a href="#">LDAP Servers</a>	From the LDAP Servers page, users can create, manage, and delete LDAP servers that allow for access and maintenance of information services over an IP network, often to used to store, access and share information within an organization.
<a href="#">RADIUS Server</a>	From the RADIUS server page, users can create, edit and delete RADIUS servers that help to maintain and manage a central database to authenticate all users/clients, giving you control over who accesses the network.
<a href="#">Walled Garden</a>	From the Walled Garden page, users can create, edit or delete walled gardens that can either restrict or redirect clients to certain web addresses

# Profiles

---



## 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 **Configure > Access Point > Profiles**.
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**.

## Deleting a Profile

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

## Deleting Multiple Profiles

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

The screenshot shows the Nuclias web interface. At the top, there is a navigation bar with the Nuclias logo and menu items: DASHBOARD, MONITOR, CONFIGURE, REPORTS, SETTINGS, and HELP. Below the navigation bar, there is a breadcrumb trail: Monitor / Access point / Device. A search bar is present with a 'Time frame' dropdown menu set to 'Last 30 days'. Below the search bar is a table with the following columns: #, Status, Name, MAC address, Public IP, Local IP, Model name, Configuration status, and License status. The table contains one row with the following data: # 1, Status (empty), Name TestDevice, MAC address 78:32:18:7D:35:08, Public IP (empty), Local IP (empty), Model name DBA-1510P, Configuration status Up to date, and License status No License. At the bottom of the table, there are pagination controls: Previous, 1, Next, and 10.

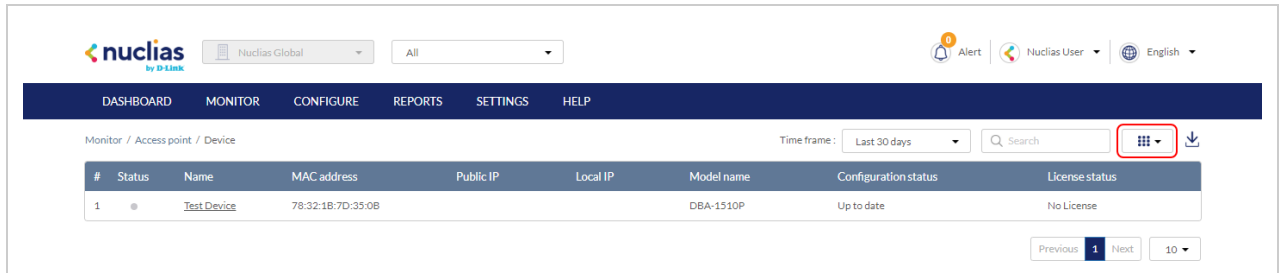
#	Status	Name	MAC address	Public IP	Local IP	Model name	Configuration status	License status
1		TestDevice	78:32:18:7D:35:08			DBA-1510P	Up to date	No License

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

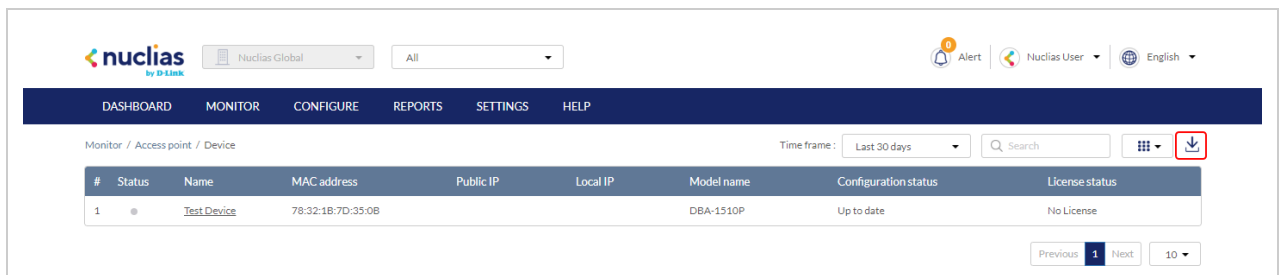
## Creating an SSID

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

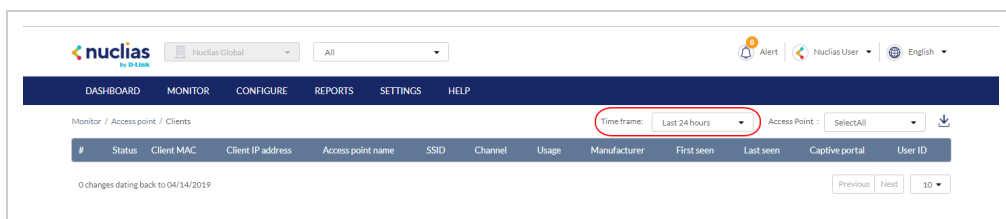
1. Navigate to **Configure > Access Point > Profiles**.
2. From the Profile list, click **SSID** under the Actions column of the Profile you wish to create an SSID for.



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



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



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

## Configuring Basic SSID Settings

### 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 **Configure > Access Point > Profiles**.
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.

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**.

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

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

## Configuring Basic SSID Settings Using WPA, WPA+WPA2 With 802.1X Enterprise (RADIUS) Authentication

1. Navigate to **Configure > Access Point > Profiles**.
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 Authentication Method drop-down menu, select RADIUS.
7. [Optional] If you have no pre-configured 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.

VLAN mode	<p>Select the VLAN type.</p> <p>Tagged: Adds an 802.1Q header to traffic.</p> <p>Untagged: Does not add a tag to traffic.</p>
-----------	---

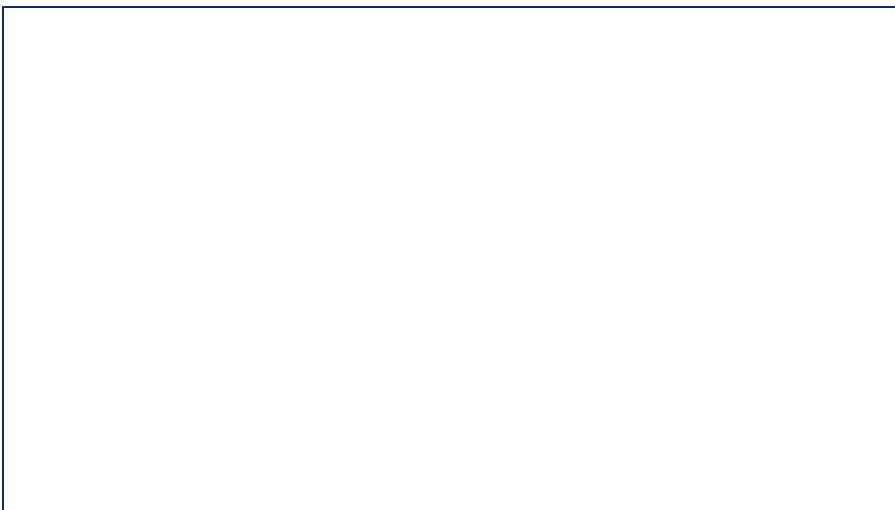
VLAN tag	If the VLAN mode is set to Tagged, specify a VLAN tag. This will segment traffic with the respective VLAN tag.
----------	--

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**.

## Configuring SSID Captive Portal Settings



## 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 **Configure > Access Point > Profiles**.
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**. Refer to [Splash page editor](#) 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**.

## 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 [Local Authentication](#) for more information.

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

## Configuring an SSID Captive Portal With Basic Login Page Using a RADIUS Server

1. Navigate to **Configure > Access Point > Profiles**.
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 for more information.

8. Select **RADIUS** as the Basic Login Page type.
9. [Optional] If you have no pre-configured 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**.

## Configuring an SSID Captive Portal With Third Party Login

1. Navigate to **Configure > Access Point > Profiles**.
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 [Splash Page Editor](#) for more information.
8. Select the required information:

3 <sup>rd</sup> 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**.

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

1. Navigate to **Configure > Access Point > Profiles**.
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 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 [Local Authentication](#) for more information.
11. [Optional] Click **Add authentication users** to create a new local authentication database.
12. Specify the following information:

3 <sup>rd</sup> 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**.

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

1. Navigate to **Configure > Access Point > Profiles**.
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 for more information.
8. Select **RADIUS** as the Basic Login Page type.
9. [Optional] If you have no pre-configured 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:

3 <sup>rd</sup> 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**.

## Configuring SSID Access Control Settings



## Configuring SSID MAC Filtering Settings Using MAC ACL

Using MAC Access Control Lists (ACL), users can 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 **Configure > Access Point > Profiles**.
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 **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 [MAC ACL](#) for more information.
8. [Optional] Click **Add a MAC ACL** to create a new MAC ACL.
9. Click **Save**.
10. Click **Push Configuration**.

## 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 **Configure > Access Point > Profiles**.
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 **Access Control**.
5. In the MAC Filtering section, click **Enable**.
6. Select **RADIUS** as the Filter type
7. [Optional] If you have no pre-configured 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**.

## Configuring SSID IP Filtering Settings Using IP ACL

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

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

## Configuring SSID Schedule Settings



## Configuring Advanced SSID Settings



1. Navigate to **Configure > Access Point > Profiles**.
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:

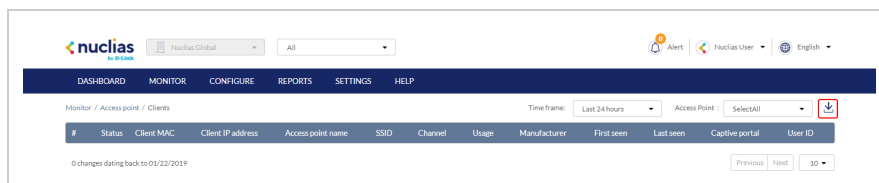
Max Clients	Enter the maximum number of concurrent clients that can connect to the SSID. The maximum is 64.
Max Allowed Client Retries	Enter the maximum amount of times a client can attempt to reconnect to the SSID once the maximum client limit has been reached. After retrying the set amount times, the 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 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 Threshold	Enter the signal strength threshold (in dbm) for clients 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**.

## Deleting an SSID

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



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

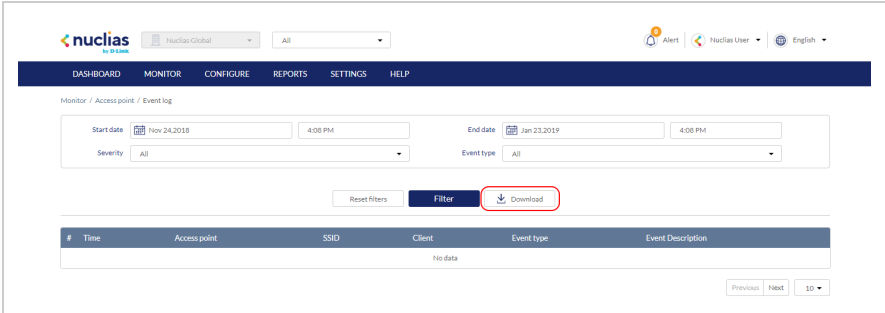
## Configuring Profile Radio Settings



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.

## Configuring Basic Profile Radio Settings

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



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.

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

## Configuring Profile Radio Channel Settings



1. Navigate to **Configure > Access Point > Profiles**.
2. From the Profile list, click **RADIO** under the Actions column of the Profile you wish to edit radio settings for.
3. Select 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 and assign devices.
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. <b>Note:</b> 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**.

## Configuring Advanced Profile Radio Settings



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

## 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 **Configure > Access Point > Profiles**.
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.
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**.

## 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 **Configure > Access Point > Profiles**.
2. From the Profile list, click **Push Configuration** under the Actions column of the Profile you wish to update the configuration settings of.
 

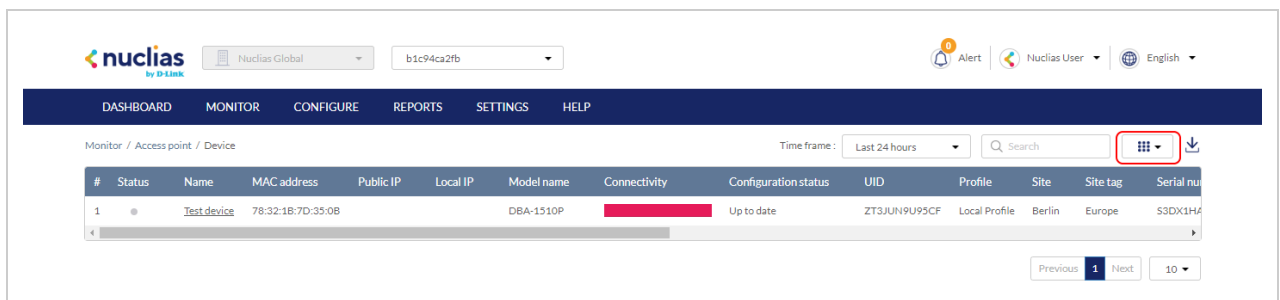
**Note:** A result window will appear providing a summary of the update status.
3. In the Push Configuration Result window, click the **X** icon in the top-right to close the window.

# 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.

## Filtering Device Information

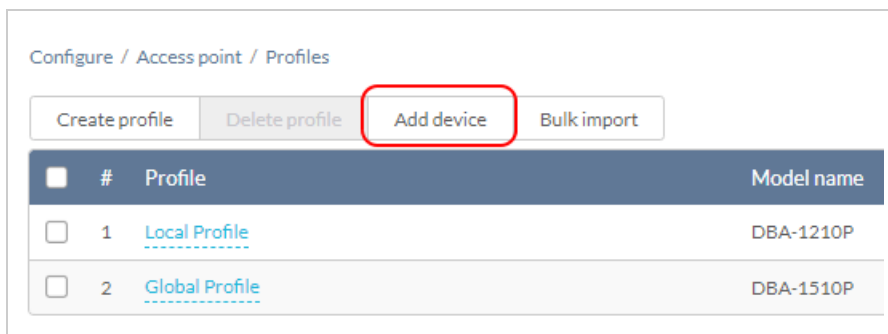
1. Navigate to **Monitor > Access Point > Devices**.
2. Select a time frame from the drop-down menu.
3. Click the filter selection in the top-right.



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

## Adding a Single Device

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



3. Fill out the required information.

Device UID	Enter the device's UID is found on the label printed on the device.  The UID may be listed in the format XXXX-XXXX-XXXX or XXXXXXXXXXXXXXXX. When entering the UID, do not include dashes.
Device name	Enter a name for the device.

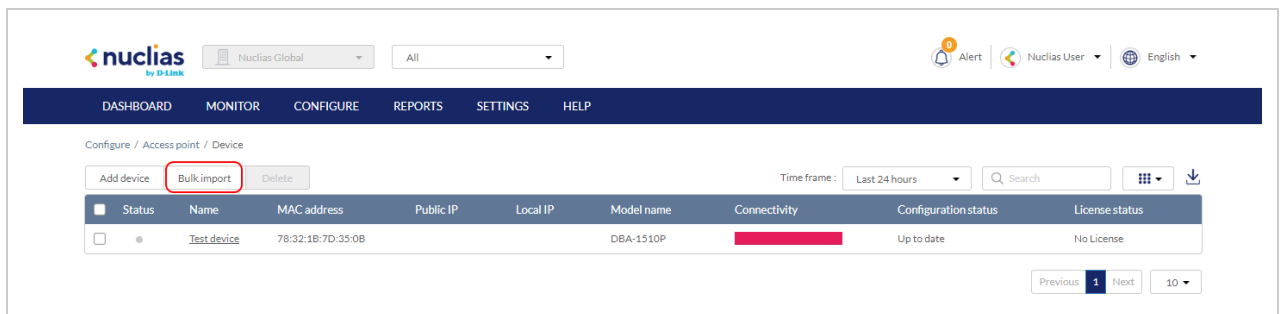
Site	Select a Site to link this device to.
Profile	Select a Profile for this device. The device will use the settings configured in that profile.
License Key	[Optional] Enter the device license key.  Note: Every new device will be issued a one year free license key. Once expired, an additional license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

4. Click **Save**.

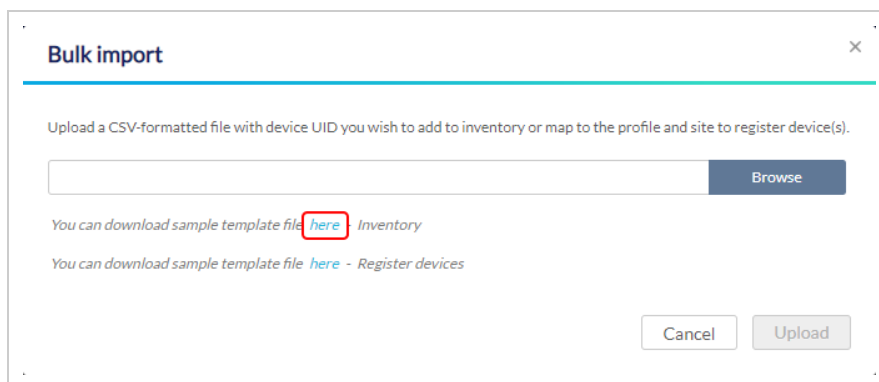
## Bulk Adding Multiple Devices to the Inventory

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 **Configure > Access Point > Devices**.
2. Click **Bulk import**.



3. [Optional] Download the reference sample template.

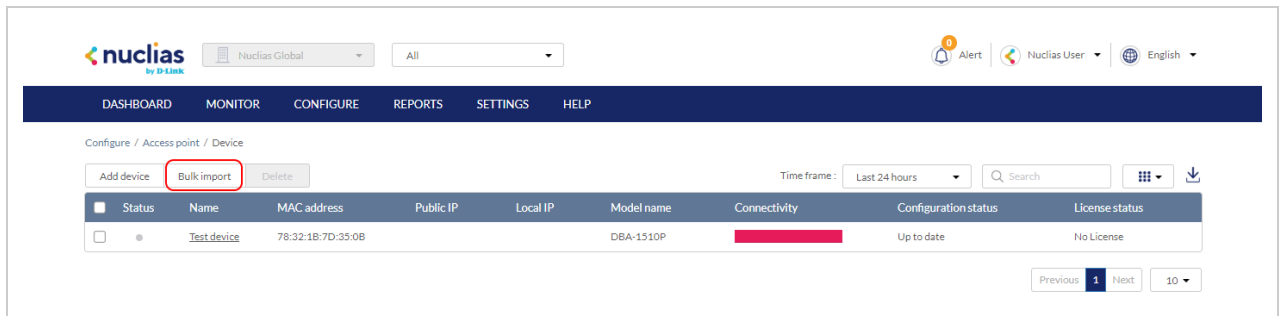


4. Click **Browse**.
5. Locate the CSV-formatted file containing the UIDs of the devices.  
Note: To add devices to the inventory, use the following format:  
[UID]
6. Click **Upload**.

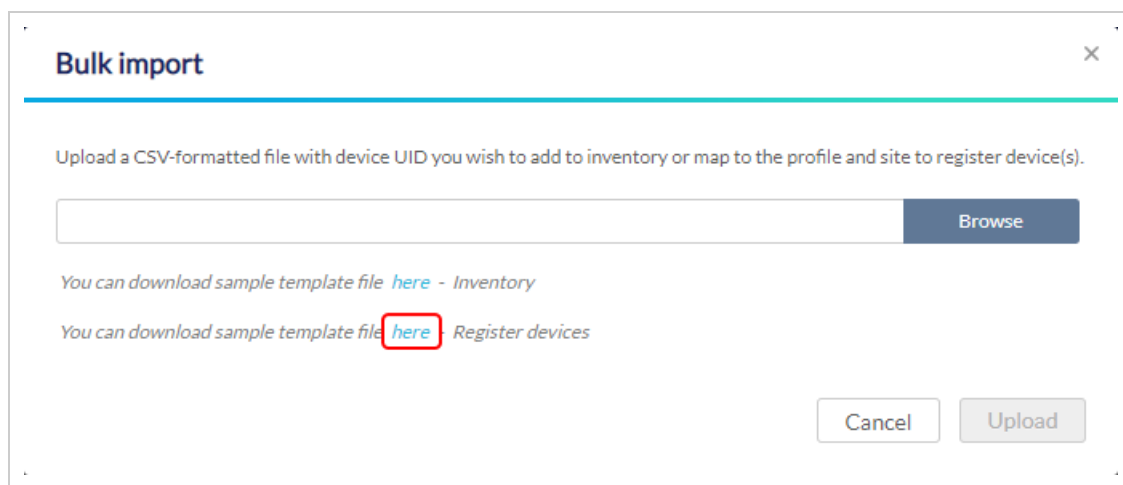
## Bulk Adding and Registering Multiple Devices to a Site

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 **Configure > Access Point > Devices**.
2. Click **Bulk import**.



3. [Optional] Download the reference sample template.



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**.

## Editing a Device

### Editing the Device Name

1. Navigate to **Configure > Access Point > Device**.
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**.

### Changing the Device Site and Profile

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

## 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 **Configure > Access Point > Devices**.
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**.

## 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 **Configure > Access Point > Devices**.
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 DNS server address.

6. Click **Apply**.

## 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 **Configure > Access Point > Devices**.
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 [Profiles](#) for more information on how to configure each section.

## 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 **Configure > Access Point > Devices**.
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](#) for more information on how to configure each section.

## 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 **Configure > Access Point > Devices**.

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**.

## 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 **Configure > Access Point > Devices**.
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**.

## 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 **Configure > Access Point > Devices**.
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.

## Manually Rebooting a Device

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

## Adding a License Key to a Device

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

## Deleting a License Key From a Device

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

# 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 **Configure > Access Point > Devices**.
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.

# Deleting Multiple Devices

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

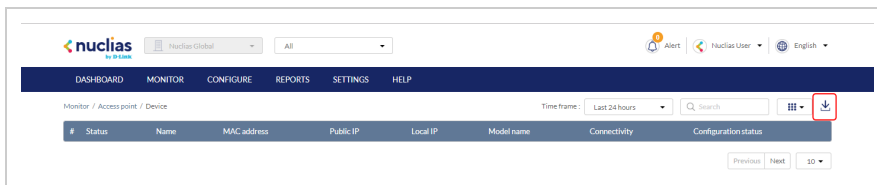
1. Navigate to **Configure > Access Point > Devices**.
2. From the device list, click the checkbox next to the devices you wish to delete.
3. Click **Delete**.
4. When prompted to confirm, click **Yes**.

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

# Download the Device List

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

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



# IP ACLs

## Creating an IP ACL Using Single Entries

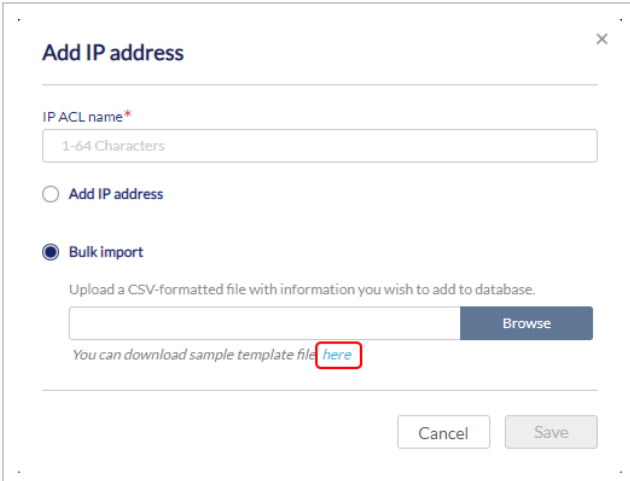
1. Navigate to **Configure > Access Point > IP ACL**.
2. Click **Add IP ACL**.
3. In the Add IP address window, enter a name for the IP ACL.
4. Select **Add IP address**.
5. Specify the following information:

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**.

## Creating an IP ACL Using Bulk Import

1. Navigate to **Configure > Access Point > IP ACL**.
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** [X]

IP ACL name\*  
1-64 Characters

Add IP address

Bulk import

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

[File Input Field] **Browse**

You can download sample template file [here](#)

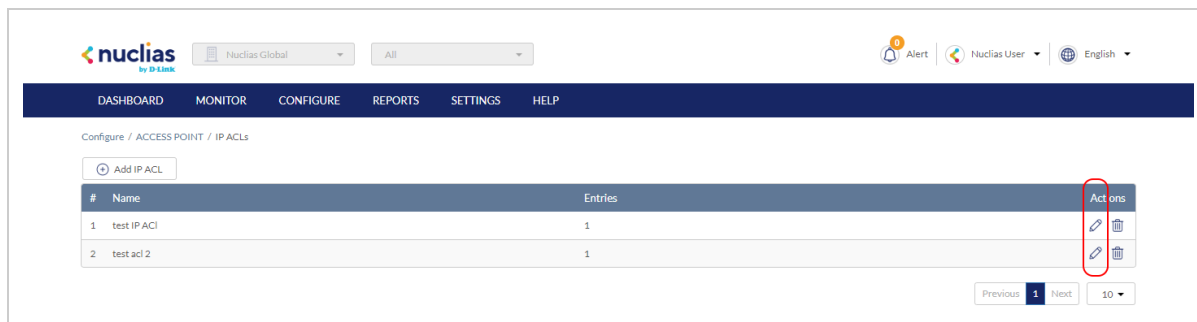
**Cancel** **Save**

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**.

## Editing Existing IP ACLs

### Adding IP Addresses to an Existing IP ACL

1. Navigate to **Configure > Access Point > IP ACL**.
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 **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**.

## Editing an IP Address in an IP ACL

1. Navigate to **Configure > Access Point > IP ACL**.
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**.

## Deleting an IP Address From an Existing IP ACL

1. Navigate to **Configure > Access Point > IP ACL**.
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**.

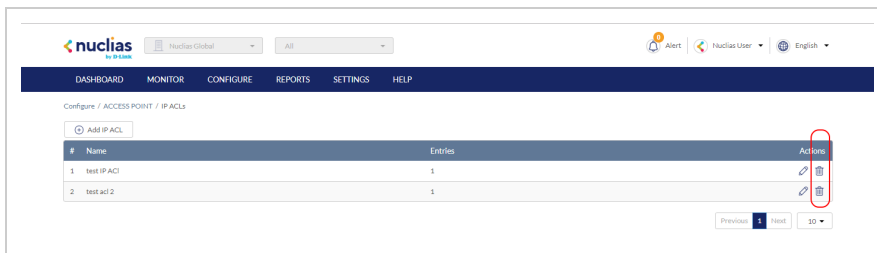
## Exporting an IP ACL

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

1. Navigate to **Configure > Access Point > IP ACL**.
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**.

## Deleting an IP ACL

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



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

# 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.

## Creating a MAC ACL Using Single Entries

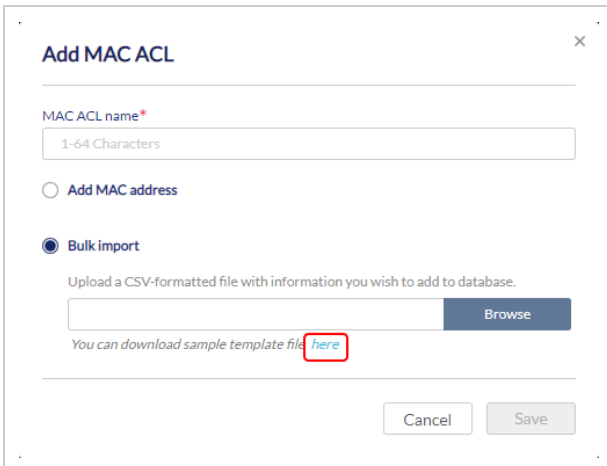
1. Navigate to **Configure > Access Point > MAC ACL**.
2. Click **Add MAC ACL**.
3. In the Add MAC ACL window, enter a name for the MAC ACL.
4. Select **Add MAC address**.
5. Specify the following information:

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**.

## Creating a MAC ACL Using Bulk Import

1. Navigate to **Configure > Access Point > MAC ACL**.
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** [Close]

MAC ACL name\*  
1-64 Characters

Add MAC address

Bulk import

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

[File Input] [Browse]

You can download sample template file [here](#)

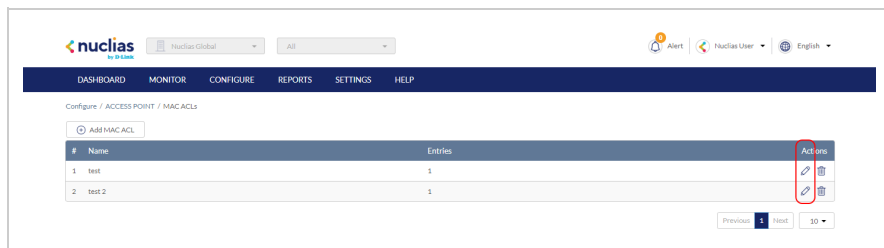
[Cancel] [Save]

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**.

## Editing Existing MAC ACLs

### Adding MAC Addresses to an Existing MAC ACL

1. Navigate to **Configure > Access Point > MAC ACL**.
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 **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**.

## Editing a MAC Address in an Existing MAC ACL

1. Navigate to **Configure > Access Point > MAC ACL**.
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**.

## Deleting a MAC Address From an Existing MAC ACL

1. Navigate to **Configure > Access Point > MAC ACL**.
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**.

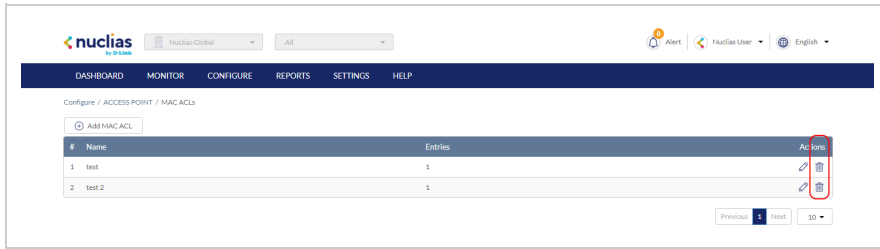
## Exporting a MAC ACL

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

1. Navigate to **Configure > Access Point > MAC ACL**.
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**.

## Deleting a MAC ACL

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



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

# Local Authentication

---

## Creating a Local Authentication Database Using Single Entries

1. Navigate to **Configure > Access Point > Local authentication**.
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**.

## Creating a Local Authentication Database Using Bulk Import

1. Navigate to **Configure > Access Point > Local authentication**.
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.

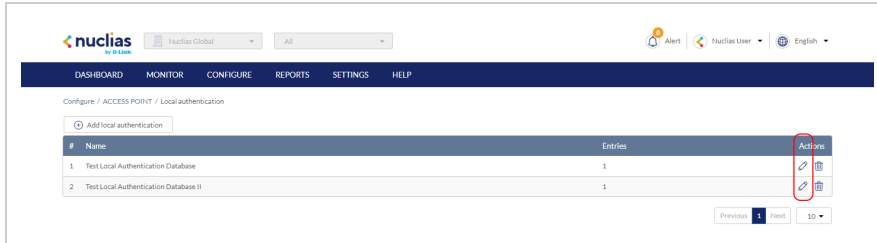
here'. At the bottom are 'Cancel' and 'Save' buttons." data-bbox="121 625 466 813"/>

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**.

## Editing Existing Local Authentication Databases

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

1. Navigate to **Configure > Access Point > Local authentication**.
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 **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**.

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

1. Navigate to **Configure > Access Point > Local authentication**.
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**.

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

1. Navigate to **Configure > Access Point > Local authentication**.

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**.

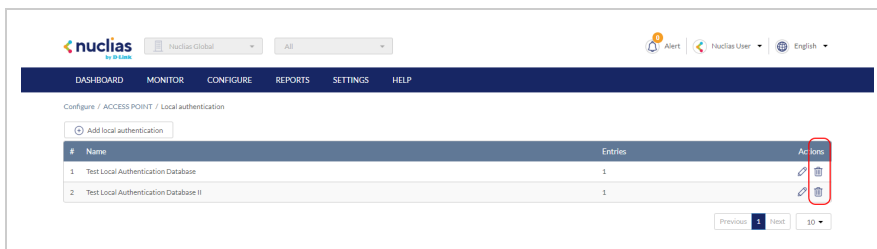
## Exporting a Local Authentication Database

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

1. Navigate to **Configure > Access Point > Local authentication**.
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**.

## Deleting a Local Authentication Database

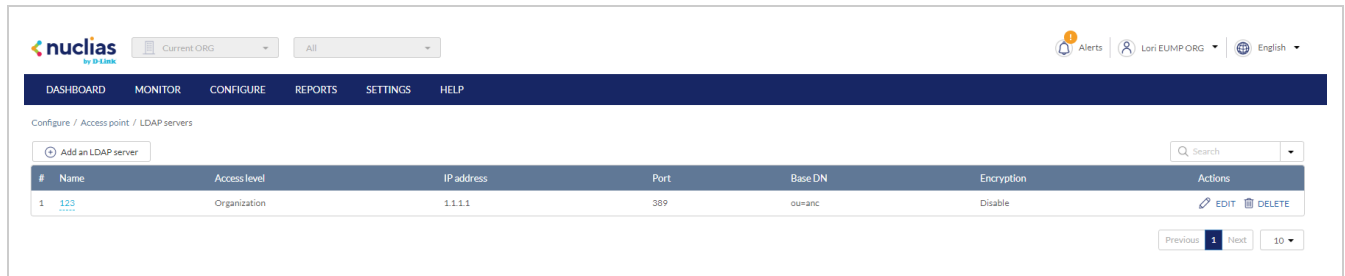
1. Navigate to **Configure > Access Point > Local authentication**.
2. From the local authentication database list, click the trash can icon under the Actions column of the database you wish to delete.



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

# LDAP Servers

Lightweight Directory Access Protocol servers help medium to large-sized companies access and maintain information services over an IP network, often to used to store, access and share information within an organization.



## Add an LDAP Server

### Add an LDAP server

LDAP server name\*  
1-64 Characters

IP address\*  
e.g. 10.90.90.90

Port\*  
389

Base DN\*  
e.g. ou=rdlink,dc=nuclias,dc=com

Encryption  
Disable

Access privilege  
Access level  
Organization

Close Save

1. Navigate to **Configure > Access point > LDAP Server**
2. Click **Add an LDAP server** in the top left.
3. In the Add an LDAP server window, enter the information below:

LDAP server name	Enter a local name for the server.
IP address	Enter a valid IP address.
Port	Enter the port used to connect to the server.
Base DN	Enter the Base DN, which is the point where the server will search for users.
Encryption	Select the type of encryption of the LDAP server from the drop-down menu. You can also choose to disable encryption.
Access level	Select between <b>Organization</b> , <b>Site Tag</b> or <b>Site</b> for the access level from the drop-down menu to restrict who has access to this server.

4. Click **Save**.

## Editing an Existing LDAP Server

1. Navigate to **Configure > Access Point > IP ACL**.
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**.

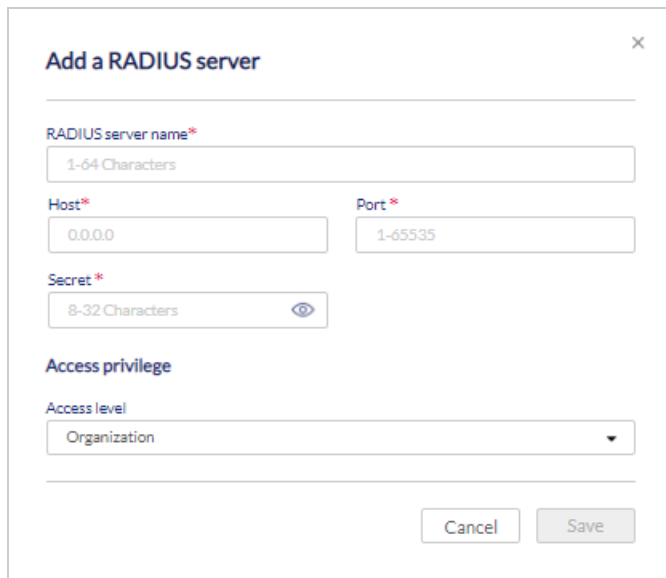
## Deleting an LDAP Server

1. Navigate to **Configure > Access Point > LDAP server**.
2. From the LDAP server list, click the trash can icon under the Actions column of the LDAP server you wish to delete.
3. When prompted to confirm, click **Yes**.

# RADIUS Server

RADIUS servers are a client/server protocol that runs a background process of windows or linux server to maintain and manage a central database to authenticate all users/clients, giving you control over who accesses the network.

## Add a RADIUS Server



1. Navigate to **Configure > Access point > RADIUS Server**
2. Click **Add a RADIUS server** in the top left.
3. In the Add an RADIUS server window, enter the information below:

RADIUS server name	Enter a RADIUS server name.
Host	Enter the host, or physical address of the RADIUS server.
Port	Enter the RADIUS server 16 bit port number.
Secret	Enter the secret text string that serves as a password between hosts.
Access level	Select between Organization, Site Tag or Site for the access level from the drop-down menu to restrict who has access to this server.

## Edit an Existing RADIUS Server

1. Navigate to **Configure > Access point > RADIUS Server**
2. From the RADIUS servers list, click the pencil icon under the Actions column of the server connection you wish to edit.
3. In the Update RADIUS server window, click the pencil icon under the Actions column of the 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.

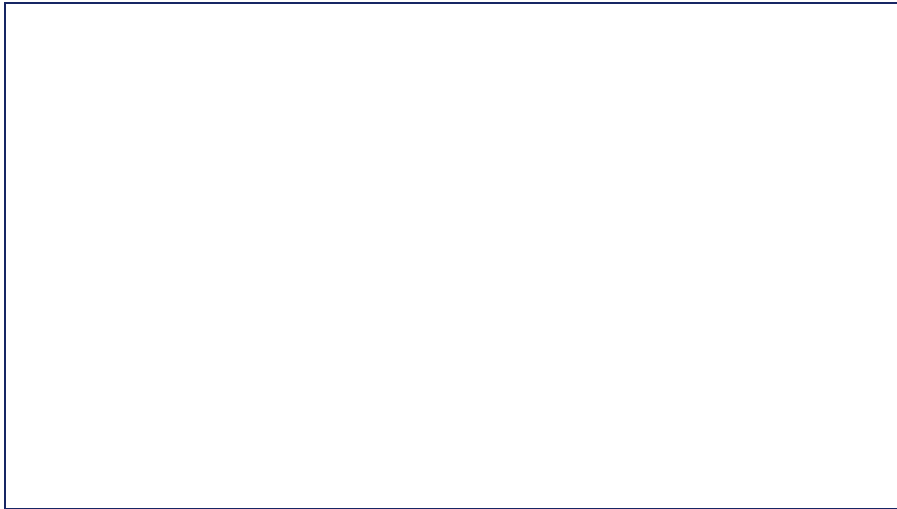
5. Click **Save**.

## Delete a RADIUS Server

1. Navigate to **Configure > Access Point > MAC ACL**
2. From the MAC ACL list, click the trash can icon under the Actions column of the MAC ACL you wish to delete
3. When prompted to confirm, click **Yes**.

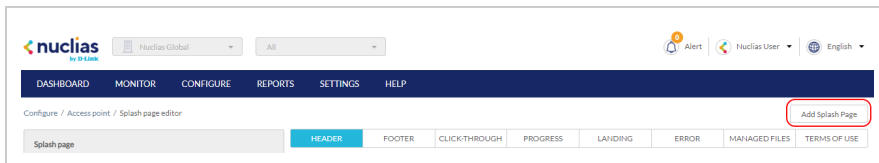
# Splash Page Editor

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.



## Creating a Custom Splash Page

1. Navigate to **Configure > Access Point > Splash Page Editor**.
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 <b>Add Image</b> to navigate to and upload a custom background image.

4. Click **Save**.

## Editing a Splash Page


1. Navigate to **Configure > Access Point > Splash Page Editor**.
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	Edit 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 include logos, icons, and images.
Terms of Use	Edit the Terms of Use content.

4. Click **Save**.

## Deleting a Custom Splash Page

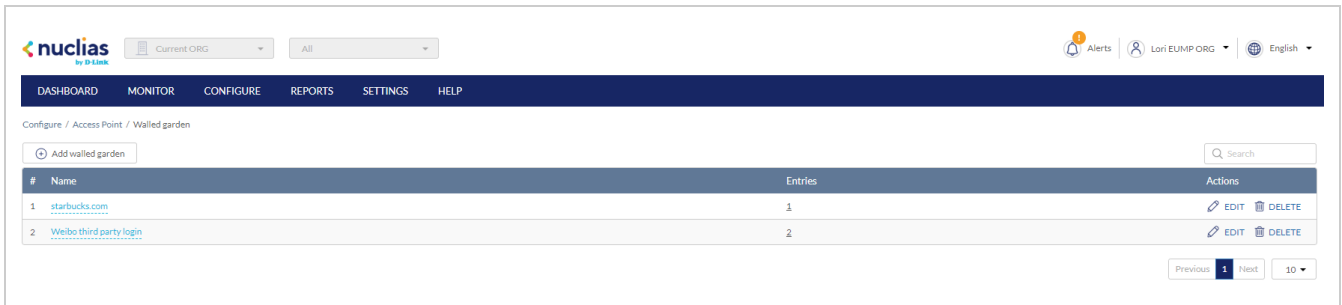
1. Navigate to **Configure > Access Point > Splash Page Editor**.
2. In the Splash page column, click the splash page you wish to delete.  
Note: Default splash pages cannot be deleted.
3. Click the trash can icon.

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.

# Walled Garden

Walled gardens are an internet browsing environment that either restricts from or redirects clients to certain web addresses. These gardens restrict to a particular section of a network and prevent access to other websites.



## Add a Walled Garden

### Add walled garden

Walled garden name  
1-64 Characters

Add walled garden ranges

Range #1\*  
hostname or 10.90.0.0/16

[+](#) Add

[Cancel](#) [Save](#)

1. Navigate to **Configure > Access point > Walled Garden**.
2. Click **Add Walled Garden** in the top left.
3. In the Add an Walled Garden server window, enter the information below:

Walled Garden name	Enter a name for your walled garden.
Walled Garden Ranges	Either enter a hostname or a valid IP address for the range of the walled garden.

4. [Optional] To add multiple ranges for your walled garden, click **Add**.
5. Click **Save**.

## Edit an Existing Walled Garden

### Update walled garden - Weibo third party login ×

<input type="checkbox"/>	#	Walled garden range <span>?</span>	Action
<input type="checkbox"/>	1	<input type="text" value="login.sina.com"/>	<input type="button" value="DELETE"/>
<input type="checkbox"/>	2	<input type="text" value="login.sina.com.cn"/>	<input type="button" value="DELETE"/>

1. Navigate to **Configure > Access Point > IP ACL**.
2. From the Walled Garden list, click the pencil icon under the Actions column of the Walled Garden you wish to edit.
3. From there, edit or delete existing addresses, or add addresses to list of permitted websites.
4. [Optional] Delete multiple entries by clicking the boxes on the left-hand side and then click **Delete**.
5. In the update window, edit the walled garden range (e.g. 192.168.10.100/32 or 10.90.0.0/16, google.com, dlink.com).
6. Click **Save**.

## Delete a Walled Garden

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

# Configure - Switch

---

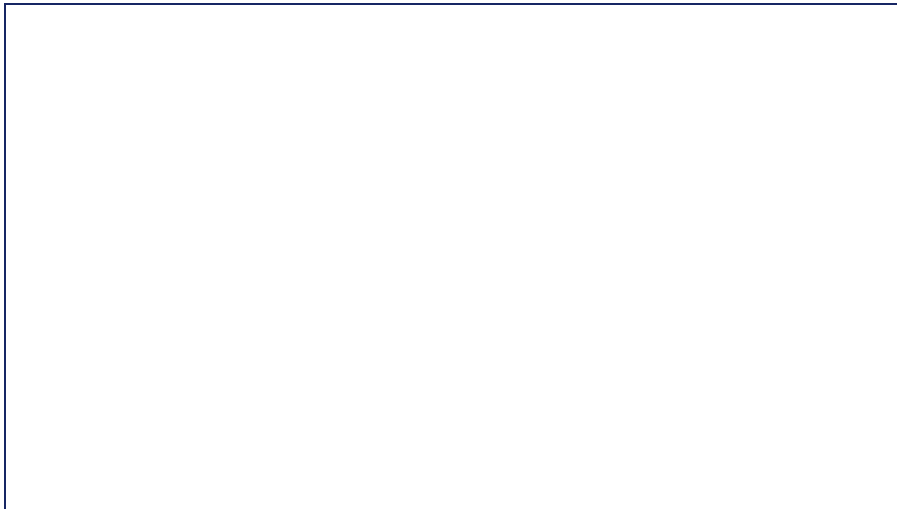
From the Configure section, users can manage profiles and devices for organizations. Because profiles and devices are managed on the organization level and are not shared between organizations, users must select a specific organization from the organization drop-down menu.

The following sections provides more detailed information about Profile and Device management respectively.

<a href="#">Profiles</a>	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 device groups.
<a href="#">Devices</a>	From the Devices section, users can add a single device, or bulk import a group of devices, and configure individual devices.
<a href="#">Switch Ports</a>	From the Switch Ports section, users can configure features on a single port or a group of selected ports.

# Profiles

---



## 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 switch port functionality, port activity schedules, and advanced features including VLAN, Quality of Service, and access control functions.

Note: Profiles are created for individual organizations. In order to configure Profiles, select the organization from the drop-down menu at the top of the page.

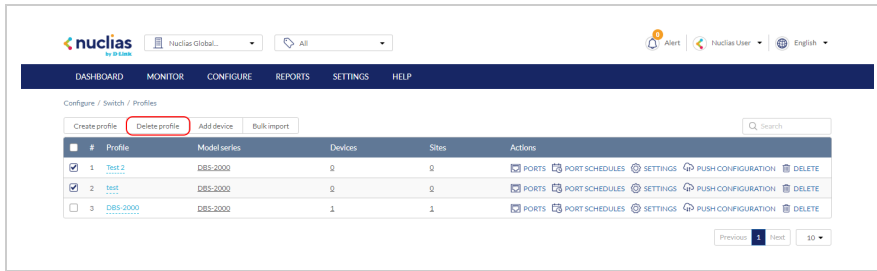
1. Navigate to **Configure > Switch > Profiles**.
2. Click **Create Profile**.
3. Enter a name for the Profile and choose the device model.  
**Note:** The Profile can only be used for the selected device model type.
4. [Optional] Select **Clone from existing profile** and choose a Profile from the drop-down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

## Deleting a Profile

1. Navigate to **Configure > Switch > Profiles**.
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**.

## Deleting Multiple Profiles

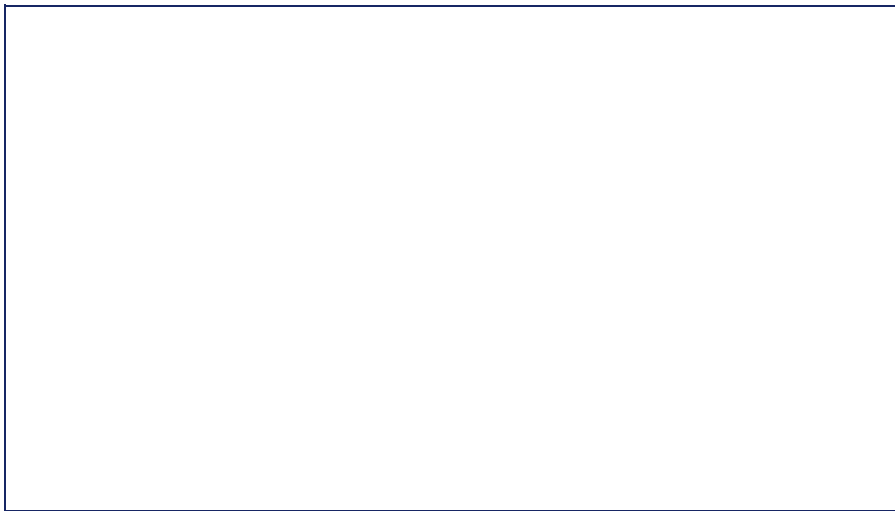
1. Navigate to **Configure > Switch > Profiles**.
2. Click the checkbox next to the Profiles you wish to delete.
3. Click **Delete profile**.



4. When prompted to confirm, click Yes.

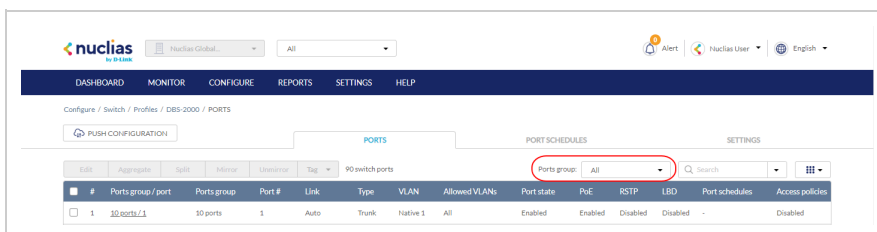
## Configuring Switch Port Settings

From the Ports window, users can configure basic and advanced settings for individual ports or groups of ports. Switch ports are categorized into group ports, with each group referring to the number of ports on the physical switch model. For example, port group 10 configures port settings for 10-port switches. The port settings configured in the profile will only apply to the ports of the corresponding switch type. For example, any port configurations for port group 10 will only apply to corresponding ports on 10-port switch using this profile.

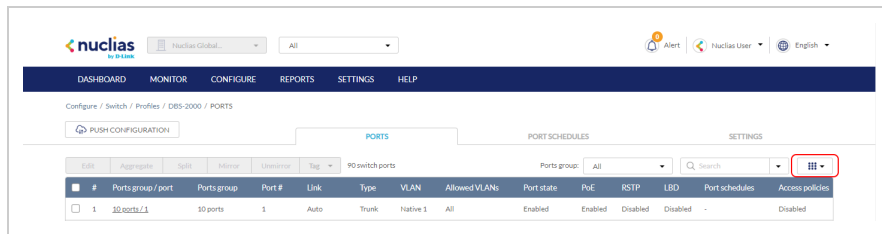


## Customizing the Profile Port Configuration Overview

1. Navigate to **Configure > Switch > Profiles**.
2. From the Profile list, click **Ports** under the Actions column of the Profile you wish to edit.
3. Select a port group from the drop-down menu. This will only display ports for the selected port group profile. For example, selecting port group 28 will only show ports 1 to 28 of the profile used for 28-port switches. Select **All** to show all port groups.



4. Click the filter parameter icon.



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

**Note:** All checked parameters will automatically appear.

## Configuring Profile Port Settings For One or More Switch Ports

Switch port configuration allows administrators to configure extensive port functionality including port availability, port speed, redundancy, VLAN, PoE, and port activity schedules for an individual port or for a group of ports.

1. Navigate to **Configure > Switch > Profiles**.
2. From the Profile list, click **Ports** under the Actions column of the Profile you wish to edit.
3. From the port list, check the box next to the ports you wish to edit.
4. Click **Edit**.
5. Specify the following information:

**Note:** At the top of the edit port window is a list of all selected ports. The changes made will apply to all selected ports.

Port name	Enter a name for the port. If multiple ports are selected, this name will be applied to all ports.
Port state	Choose to enable or disable the port.
RSTP	Choose to enable or disable Rapid Spanning Tree Protocol (RSTP). RSTP prevents data loops by issuing frequent BPDU packets to monitor link status.  Note: RSTP cannot be used in conjunction with LBD.
STP guard	If RSTP is enabled, choose the guard type.  Disabled: Do not use root guard enhancement.  Root guard: Root guard enhancement allows administrators to define the position of the root bridge port in the network.
LBD	Choose to enable or disable Loopback Detection (LBD).  Note: LBD cannot be used in conjunction with RSTP.

Type	<p>Choose the function type of the port.</p> <p>Trunk: Sends and receives tagged data from different VLANs.</p> <p>Access: Only sends and receives untagged data from the VLAN the port belongs to.</p>
Native VLAN	Enter the ID of the native VLAN the port belongs to.
Allowed VLANs	Enter the IDs of the VLANs that can route traffic through this port. Enter <b>All</b> to allow all traffic from all VLANs to pass through this port.
Tags	Enter a descriptive tag for the port. Multiple tags can be entered. If multiple ports are selected, any tags will be applied to all ports.
Link (RJ45)	Choose the maximum link speed of the port. Select Auto to allow the port to auto-negotiate port speed with the partner port or device.
PoE	<p>Choose to enable or disable Power over Ethernet (PoE) functionality on this port.</p> <p>Note: The PoE setting will only apply to ports that support Power over Ethernet.</p>
Port Schedule	Choose a port schedule. Port schedules are separately configured. Refer to the <a href="#">Creating a Switch Port Schedule</a> section.

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

## Aggregating Multiple Switch Profile Ports

Port aggregation allows users to link multiple physical ports together as one logical link to increase port bandwidth and redundancy in the event of a single physical link failure. Ports can be aggregated using either LACP or static link.

**Note:** Port aggregation is not supported if the port type is set to "Access". To configure the port type, refer to the [Configuring Port Settings for One or More Switch Ports](#) section for more information.

1. Navigate to **Configure > Switch > Profiles**.
2. From the Profile list, click **Ports** under the Actions column of the Profile you wish to edit.
3. From the port list, check the box next to the ports you wish to link together.
4. Click **Aggregate**.
5. In the Link Aggregation Setting window, select the aggregation type.

**Note:** Static link requires manual configuration of the ports in the aggregation group. Link Aggregation Control

Protocol (LACP) dynamically queries to listening ports to join the aggregation group.

LACP	LACP (Link Aggregation Control Protocol) allows the switch to automatically detect links in a port trunk group.
Static	Static link aggregation.

## 6. Click **Aggregate**.

**Note:** Aggregated ports can be identified by the combined port number in the Port # column of the port overview.

ID	Ports group/port	Ports group	Port #	Link	Type	VLAN	Allowed VLANs	Port state	PoE	RSTP	LLD	Port schedules	Access Policies
1	10.ports/1	10 ports	3	Auto	Trunk	Native 1	All	Enabled	Enabled	Disabled	Disabled	-	Disabled
2	10.ports/4	10 ports	4	Auto	Trunk	Native 1	All	Enabled	Enabled	Disabled	Disabled	-	Disabled
3	10.ports/2	10 ports	5	Auto	Trunk	Native 1	All	Enabled	Enabled	Disabled	Disabled	-	Disabled
4	10.ports/6	10 ports	6	Auto	Trunk	Native 1	All	Enabled	Enabled	Disabled	Disabled	-	Disabled
5	10.ports/7	10 ports	7	Auto	Trunk	Native 1	All	Enabled	Enabled	Disabled	Disabled	-	Disabled
6	10.ports/8	10 ports	8	Auto	Trunk	Native 1	All	Enabled	Enabled	Disabled	Disabled	-	Disabled
7	10.ports/9	10 ports	9	10Gbps (auto)	Trunk	Native 1	All	Enabled	Disabled	Disabled	Disabled	-	Disabled
8	10.ports/10	10 ports	10	10Gbps (auto)	Trunk	Native 1	All	Enabled	Disabled	Disabled	Disabled	-	Disabled
9	10.ports/1,2	10 ports	1,2	Auto	Trunk	Native 1	All	Enabled	Enabled	Disabled	Disabled	-	Disabled
10	20.ports/1	20 ports	1	Auto	Trunk	Native 1	All	Enabled	Enabled	Disabled	Disabled	-	Disabled

## 7. Click **Push Configuration**.

# Splitting Aggregated Switch Ports

Linked port groups can be split into their respective individual ports. Splitting port groups will undo all aggregation settings applied to the affected ports.

1. Navigate to **Configure > Switch > Profiles**.
2. From the Profile list, click **Ports** under the Actions column of the Profile you wish to edit.
3. From the port list, check the box next to the aggregated port(s) you wish to split.
4. Click **Split**.
  - Note:** This will immediately split the selected aggregated ports.
5. Click **Push Configuration**.

# Mirroring Port Traffic to Another Switch Profile Port

Port Mirroring is a method of monitoring network traffic that forwards a copy of each incoming and/or outgoing packet from one port of the switch to another port, where the packet can be studied. This enables network managers to better monitor network performance.

1. Navigate to **Configure > Switch > Profiles**.
2. From the Profile list, click **Ports** under the Actions column of the Profile you wish to edit.
3. From the port list, check the box next to the port(s) you wish to mirror.
4. Click **Mirror**.
5. Specify the following information:

Source ports	Select the data to mirror from the drop-down menu for each selected port.  Both: Mirror both incoming and outgoing.  Rx: Mirror only data received on the port.  Tx: Mirror only data transmitted by the port.
Destination port	Enter the port number of the destination port. Note: The port number should be in numerical format, for example 28.

6. Click **Create port mirror**.
7. Click **Push Configuration**.

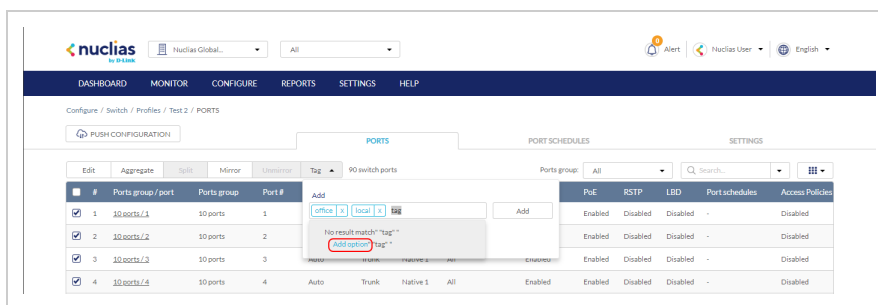
## Undoing Port Traffic Mirroring

1. Navigate to **Configure > Switch > Profiles**.
2. From the Profile list, click **Ports** under the Actions column of the Profile you wish to edit.
3. From the port list, check the box next to the mirrored port(s) you wish to unmirror.
4. Click **Unmirror**.  
**Note:** This will immediately undo the selected mirrored ports.
5. Click **Push Configuration**.

## Adding a Tag to One or More Switch Profile Ports

User can add descriptive tag to ports to identify and filter different ports or groups of ports. Tags are purely informational and do not affect the functionality of the port.

1. Navigate to **Configure > Switch > Profiles**.
2. From the Profile list, click **Ports** under the Actions column of the Profile you wish to edit.
3. From the port list, check the box next to the port(s) you wish to add a tag to.
4. Click **Tag**.
5. In the Add field, enter the tag content. Multiple tags can be entered.  
**Note:** If this is a new tag, click Add option to make this a reusable tag.



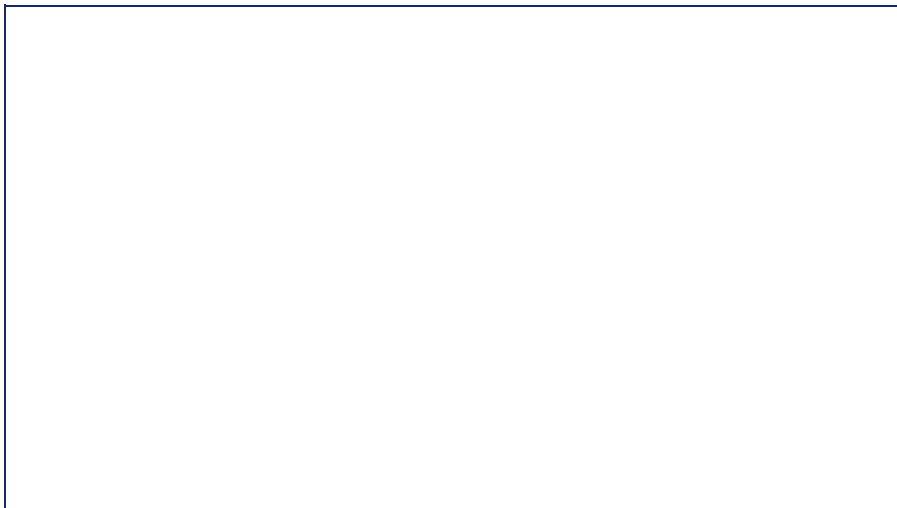
6. Click **Add**.  
**Note:** Any tags associated to a port will be shown in the Tags column.

Ports group	Port #	Link	Type	VLAN	Allowed VLANs	Port state	PoE	RSTP	LED	Port schedules	Access Policies	Mirror	Tags
10 ports	1	Auto	Trunk	Native 1	All	Enabled	Enabled	Disabled	Disabled	-	Disabled	-	office.local
10 ports	2	Auto	Trunk	Native 1	All	Enabled	Enabled	Disabled	Disabled	-	Disabled	-	office.local
10 ports	3	Auto	Trunk	Native 1	All	Enabled	Enabled	Disabled	Disabled	-	Disabled	-	office.local
10 ports	4	Auto	Trunk	Native 1	All	Enabled	Enabled	Disabled	Disabled	-	Disabled	-	office.local
10 ports	5	Auto	Trunk	Native 1	All	Enabled	Enabled	Disabled	Disabled	-	Disabled	-	office.local
10 ports	6	Auto	Trunk	Native 1	All	Enabled	Enabled	Disabled	Disabled	-	Disabled	-	office.local

## Removing a Tag From One or More Switch Ports

1. Navigate to **Configure > Switch > Profiles**.
2. From the Profile list, click **Ports** under the Actions column of the Profile you wish to edit.
3. From the port list, check the box next to the tagged port(s) you wish to remove the tag(s) from.
4. Click **Tag**.
5. In the Delete field, enter the tag name. Alternatively, click the input field to bring up a list with all the associated tags.
6. Click **Remove**.

## Configuring Switch Profile Port Schedules



## Creating a Switch Port Schedule

Users can create customized schedules to configure port activity for each day of the week. Schedules are applied to individual ports.

1. Navigate to **Configure > Switch > Profiles**.
2. From the Profile list, click **Port Schedules** under the Actions column of the Profile you wish to edit.
3. Click **Add port schedule**.

The screenshot shows the 'Add port schedule' dialog box with the following elements:

- A header bar with the Nuclias logo and navigation tabs: DASHBOARD, MONITOR, CONFIGURE, REPORTS, SETTINGS, HELP.
- A breadcrumb trail: Configure / Switch / Profiles / Test2 / PORT SCHEDULES.
- A 'PUSH CONFIGURATION' button.
- A tabbed interface with 'PORTS', 'PORT SCHEDULES', and 'SETTINGS' tabs.
- An 'Add port schedule' button, which is circled in red.
- An input field labeled '# Port schedule name'.
- An 'Actions' button.
- 'Cancel' and 'Save' buttons at the bottom.

4. Enter a name for the schedule.
5. [Optional] Select a predefined schedule template from the drop-down menu.
6. [Optional] Click the 24 HOURS or AM/PM button in the top-right to change the time display format.
7. In the Availability column, select the schedule behavior for each day of the week:

On	The port will be active during the defined time period.
Off	The port will be disabled during the defined time period.

8. 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 port activity period.

9. In the add port schedule window, click **Save**.
10. [Optional] Repeat steps 3 to 9 to create additional schedules.
11. Click **Save**.

## Editing a Switch Port Schedule

1. Navigate to **Configure > Switch > Profiles**.
2. From the Profile list, click **Port Schedules** under the Actions column of the Profile you wish to edit.
3. From the port schedule list, click **Edit** under the Actions column of the port schedule you wish to edit.

4. [Optional] Select a predefined schedule template from the drop-down menu.
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 port will be active during the defined time period.
Off	The port will be disabled during the defined time period.

- 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 port activity period.

- Click **Save**.
- Click **Push Configuration**.

## Deleting a Switch Port Schedule

- Navigate to **Configure > Switch > Profiles**.
- From the Profile list, click **Port Schedules** under the Actions column of the Profile you wish to edit.
- From the port schedule list, click **Delete** under the Actions column of the port schedule you wish to delete.

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

## Configuring Basic Switch Profile Settings

### Configuring Management VLAN Membership

The management VLAN is the primary VLAN to connect to the cloud to configure and manage the network. By default, management VLAN 1 is the default for all switch ports.

- Navigate to **Configure > Switch > Profiles**.
- From the Profile list, click **Settings** under the Actions column of the Profile you wish to edit.
- Click the **Basic** tab.

- In the VLAN Configuration section, select a VLAN ID from the drop-down menu or directly enter an ID into the VLAN ID field.  
Note: Changing the management VLAN ID requires the management port(s) to be assigned to the new management VLAN ID.
- Click **Save**.
- Click **Push Configuration**.

## Configuring Spanning Tree Protocol (STP) Functionality

RSTP is an availability and redundancy feature that prevents redundant backup links between switches and prevents switch loops from forming by shutting down the port causing the loop. If RSTP is enabled under profile settings, this profile's device will be enabled. Users can enable/disable RSTP of individual ports under the Switch Ports page, or at **Configure > Profile > Ports**. **Note:** RSTP must be manually enabled under BOTH Switch Settings of a profile and Switch Ports.

- Navigate to **Configure > Switch > Profiles**.
- From the Profile list, click **Settings** under the Actions column of the Profile you wish to edit.
- Click the **Basic** tab.
- In the STP Configuration section, select **Enable** next to RSTP.
- Click **Add** to add a STP bridge priority.
- In the Set the bridge priority for switches window, specify the following information:

Switch	Enter the name of the switch or click the field and select an available switch from the drop-down menu.
Bridge Priority	Select a priority value from the drop-down menu. Lower values are more likely to act as the root, while higher values are more likely to act as edges.

- [Optional] Click **Add** to add additional bridge priorities.
- Click **Add**.
- [Optional] To delete a bridge priority, check the checkbox next to the switch and click **Delete**.
- Click **Save**.
- Click **Push Configuration**.

## Configuring Internet Group Management Protocol (IGMP) Snooping Functionality

IGMP Snooping allows administrators to configure switches to subscribe to, and receive multicast traffic. If a switch is not added to the IGMP list, it will not receive multicast traffic by default.

- Navigate to **Configure > Switch > Profiles**.
- From the Profile list, click **Settings** under the Actions column of the Profile you wish to edit.
- Click the **Basic** tab.
- In the IGMP Snooping Configuration section, click **Add** to add a switch to the IGMP snooping list.
- In the Set multicast settings for switches window, specify the following information:

Switch	Enter the name of the switch or click the field and select an available switch from the drop-down menu.
--------	---

IGMP Snooping	<p>Select an IGMP policy.</p> <p>Enable: The switch will subscribe to and receive multicast traffic.</p> <p>Disable: The switch will not receive multicast traffic.</p>
---------------	---

6. [Optional] Click **Add** to add switches to the IGMP list.
7. Click **Add**.
8. [Optional] To delete a switch from the list, check the checkbox next to the switch and click Delete.
9. Click **Save**.
10. Click **Push Configuration**.

## Configuring DHCP Server Screening

DHCP screening allows administrators to whitelist DHCP servers to prevent unauthorized DHCP servers and devices from gaining access to the network.

1. Navigate to **Configure > Switch > Profiles**.
2. From the Profile list, click **Settings** under the Actions column of the Profile you wish to edit.
3. Click the **Basic** tab.
4. In the DHCP Server Screening Configuration section, select **Enable** next to DHCP Server Screening.
5. In the Allowed DHCP server field, enter the IP address of the DHCP server to whitelist.
  - Note:** Currently, only one DHCP server can be whitelisted.
6. Click **Save**.
7. Click **Push Configuration**.

## Configuring Voice VLAN Functionality

Voice traffic from IP phones can be assigned to a dedicated VLAN (via Voice VLAN ID setting) and given traffic priority (via Voice VLAN CoS setting).

**Note:** Voice VLAN priority settings overrule any priority settings configured in the Quality of Service section.

**Note:** Voice VLAN is not supported if the port type is set to "Trunk".

1. Navigate to **Configure > Switch > Profiles**.
2. From the Profile list, click **Settings** under the Actions column of the Profile you wish to edit.
3. Click the **Basic** tab.
4. In the Voice VLAN Configuration section, select **Enable** next to Voice VLAN.
5. In the Voice VLAN ID field, enter an ID between 2 and 4094.
6. Select a Voice VLAN Class of Service (CoS) level from the drop-down menu.
  - Note:** The CoS level reflects the priority level of Voice VLAN traffic. A higher value means a high priority, whereas a lower value means a low priority.
7. [Optional] Click **Add** to add a Voice VLAN OUI.
  - Note:** An Organizationally Unique Identifier (OUI) is used to add additional manufacturers to the voice VLAN identification list.
8. In the Add OUIs for switches window, specify the following information:

OUI Address	This field will contain which MAC address range the OUI mask will begin with.
-------------	---

Mask	With the same concept of subnet mask, OUI Mask uses “F” as match, while “0” as any.
Description	Add a description for the OUI.

OUI Address	Mask	Description	Actions
00:01:E3:00:00:00	FF:FF:FF:00:00:00	Siemens	
00:03:4B:00:00:00	FF:FF:FF:00:00:00	Cisco	
00:09:6E:00:00:00	FF:FF:FF:00:00:00	Avaya	
00:0F:E2:00:00:00	FF:FF:FF:00:00:00	Huawei&3COM	
00:60:89:00:00:00	FF:FF:FF:00:00:00	NEC&Philips	
00:D0:1E:00:00:00	FF:FF:FF:00:00:00	Pingtel	
00:E0:75:00:00:00	FF:FF:FF:00:00:00	Veritel	
00:E0:BB:00:00:00	FF:FF:FF:00:00:00	3COM	

9. [Optional] Click **Add** to add additional OUIs.
10. Click **Add**.
11. [Optional] To delete an OUI, check the checkbox next to the OUI and click **Delete**.  
**Note:** Default OUIs cannot be deleted.
12. Click **Save**.
13. Click **Push Configuration**.

## Configuring Jumbo Frame

Enabling Jumbo Frame allows the port to switch frames larger than the standard Ethernet frame and can maximize server-to-server performance.

1. Navigate to **Configure > Switch > Profiles**.
2. From the Profile list, click **Settings** under the Actions column of the Profile you wish to edit.
3. Click the **Basic** tab.
4. In the Jumbo Frame Configuration section, select **Enable** next to Jumbo Frame.
5. Click **Save**.
6. Click **Push Configuration**.

## Configuring Quality of Service Settings

QoS is an implementation of the IEEE 802.1p standard that allows network administrators to reserve bandwidth for important functions that require a larger bandwidth or that might have a higher priority, such as VoIP (voice-over Internet Protocol), web browsing applications, file server applications or video conferencing. By reserving more bandwidth for critical traffic, less critical traffic is deprioritized to ensure that critical data is transmitted smoothly.

The Quality of Service windows displays the status of Quality of Service priority levels of each port, a higher priority means the traffic from this port will be first handled by the switch. For packets that are untagged, the switch will assign the priority depending on your configuration.

1. Navigate to **Configure > Switch > Profiles**.
2. From the Profile list, click **Settings** under the Actions column of the Profile you wish to edit.
3. Click the **Basic** tab.
4. In the Quality of Service section, click **Edit**.
5. In the DSCP to CoS Queue Mapping window, select a Class of Service value between 0 to 7 for each DSCP value. A higher value means a higher priority while a lower value means a lower priority. Traffic from ports with high CoS values are processed first.

DSCP value	Cos Queue Value	Name
0	0	Default
1	0	Default
2	1	Default
3	2	Default
4	3	Default
5	4	Default
6	5	Default
7	6	Default
8	7	Default
9	1	Default
10	1	Default
11	1	Default

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

## Configuring Switch Profile IPv4 ACL Settings

### Creating IPv4 Access Control Policy Rules

IPv4 Access Control Lists (ACL) allow administrators to configure a set of criteria for permitting or denying traffic coming from and to the switch based on IP address.

1. Navigate to **Configure > Switch > Profiles**.
2. From the Profile list, click **Settings** under the Actions column of the Profile you wish to edit.
3. Click the **IPv4 ACL** tab.
4. In the User Defined IPv4 Rules section, click **Add**.
5. In the Add IPv4 rules window, specify the following information:

Policy	<p>Select an access policy.</p> <p>Permit : Traffic with matching parameters will be forwarded.</p> <p>Deny: Traffic with matching parameters will be denied.</p>
Protocol	<p>Select a protocol from the drop-down menu.</p> <p>Any : The rule applies to any protocol traffic.</p> <p>UDP: The rule only applies to traffic with a UDP header.</p> <p>TCP: The rule only applies to traffic with a TCP header.</p>
Source	<p>Enter the source IP address. If the source address is configured as Any, all source traffic will be evaluated according to the conditions of the rule.</p>
Src port	<p>Specify the source port number between 0 and 65535.</p> <p>If the source port is configured as Any, all source ports will be evaluated according to the conditions of the rule.</p>

Destination	Enter the destination IP address. If the destination address is configured as Any, all destination traffic will be evaluated according to the conditions of the rule.
Dst port	Specify the destination port number between 0 and 65535.  If the source port is configured as Any, all source ports will be evaluated according to the conditions of the rule.
Comment	Enter a description for the rule.

6. [Optional] Click **Add** to add additional rules.
7. Click **Add**.
8. Click **Save**.
9. Click **Push Configuration**.

## Editing IPv4 Access Control Policy Rules

1. Navigate to **Configure > Switch > Profiles**.
2. From the Profile list, click **Settings** under the Actions column of the Profile you wish to edit.
3. Click the **IPv4 ACL** tab.
4. In the policy rules list, click **Edit** in the Actions column of the rule you wish to edit.
5. Specify the following information:

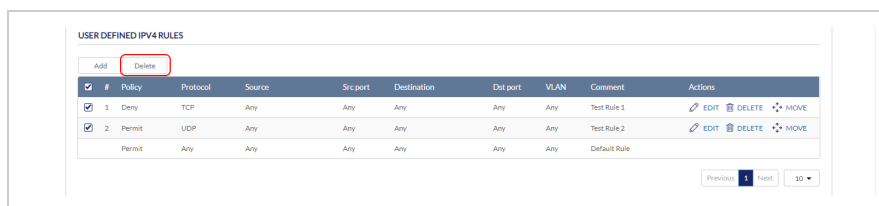
Policy	Select an access policy. Enable : Traffic with matching parameters will be forwarded.  Deny: Traffic with matching parameters will be denied.
Protocol	Select a protocol from the drop-down menu. Any : The rule applies to any protocol traffic.  UDP: The rule only applies to traffic with a User Datagram Protocol (UDP) header.  TCP: The rule only applies to traffic with a Transmission Control Protocol (TCP) header.
Source	Enter the source IP address. If the source address is configured as Any, all source traffic will be evaluated according to the conditions of the rule.
Src port	Specify the source port number between 0 and 65535.  If the source port is configured as Any, all source ports will be evaluated according to the conditions of the rule.
Destination	Enter the destination IP address. If the destination address is configured as Any, all destination traffic will be evaluated according to the conditions of the rule.

Dst port	Specify the destination port number between 0 and 65535.  If the source port is configured as Any, all source ports will be evaluated according to the conditions of the rule.
VLAN	Specify a VLAN to which the rule will apply.
Comment	Enter a description for the rule.

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

## Deleting IPv4 Access Control Policy Rules

1. Navigate to **Configure > Switch > Profiles**.
2. From the Profile list, click **Settings** under the Actions column of the Profile you wish to edit.
3. Click the **IPv4 ACL** tab.
4. In the policy rules list, click the checkbox next to the rule(s) you wish to delete.
5. Click **Delete**.



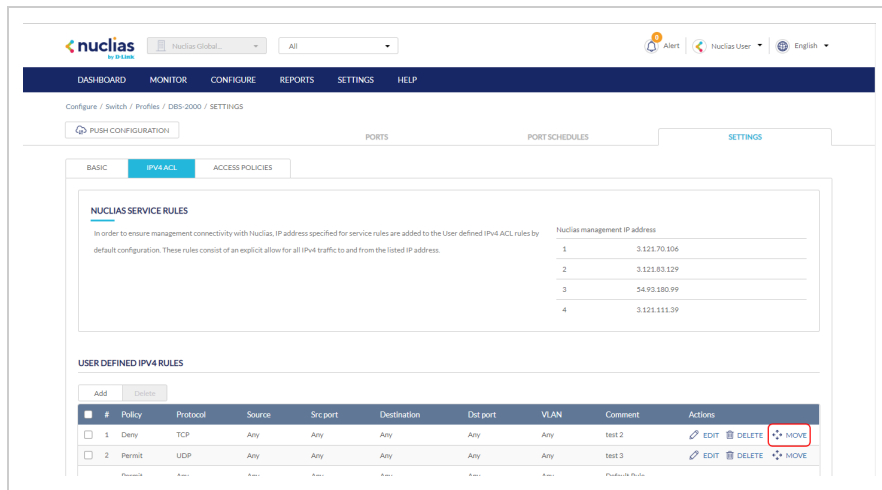
6. When prompted to confirm, click **Yes**.

## Moving IPv4 Access Control Policy Rules

If an IPv4 Access Control List contains multiple rules other than the default rule, rules can be moved around. Moving rules will affect their priority. In the event of a conflict between two rules, the rule listed as #1 will override the rule(s) below it.

**Note:** The index means priority. The lower the index the higher the priority.

1. Navigate to **Configure > Switch > Profiles**.
2. From the Profile list, click **Settings** under the Actions column of the Profile you wish to edit.
3. Click the **IPv4 ACL** tab.
4. In the policy rules list, click and drag the Move icon of the rule you wish to move. Dragging it below another rule will lower its priority, dragging above another rule increases its priority over that rule.



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

## Configuring Access Policies

### Creating an Access Policy

Administrators can configure one or more remote RADIUS servers for port-based or MAC-based authorization and authentication. This ensures that only users with matching credentials have access to the network. Administrators can also configure a Guest VLAN to grant internet access to visitors, while preventing them from accessing the network.

1. Navigate to **Configure > Switch > Profiles**.
2. From the Profile list, click **Settings** under the Actions column of the Profile you wish to edit.
3. Click the **Access Policies** tab.
4. Enter a name for the policy.
5. In the RADIUS servers field, click **Add** to add a new RADIUS server.
6. In the Add RADIUS servers window, 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.
Key	Enter a shared secret.

7. [Optional] Click **Add** to add additional RADIUS servers.
8. Click **Save**.
9. Select an access policy type:

802.1x port-based	This method requires only one user to be authenticated per port by a remote RADIUS server to allow the remaining users on the same port to access the network.
-------------------	--

802.1x MAC-based

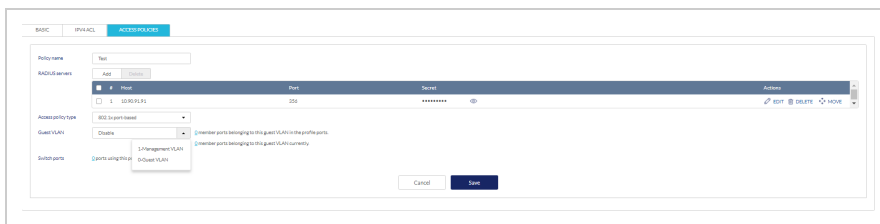
Using this method, the Switch will automatically learn up to a maximum of 448 MAC addresses by port and set them in a list. Each MAC address must be authenticated by the Switch using a remote RADIUS server before being allowed access to the Network.

10. [Optional] Select a VLAN ID from the drop-down menu.
11. Click **Save**.
12. Click **Push Configuration**.

## Configure a Guest VLAN

Administrators can configure one or more Guest VLANs to grant internet access to visitors, while preventing them from accessing the network.

1. Navigate to **Configure > Switch > Profiles**.
2. From the Profile list, click **Settings** under the Actions column of the Profile you wish to edit.
3. Click the **Access Policies** tab.
4. Select a Guest VLAN from the list.
5. Click **Save**.
6. Click **Push Configuration**.



## Pushing Configuration Changes

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

**Note:** Changes made to a Profile's ports, port schedule or settings, will be pushed to all associated devices after the user selects Push Configuration.

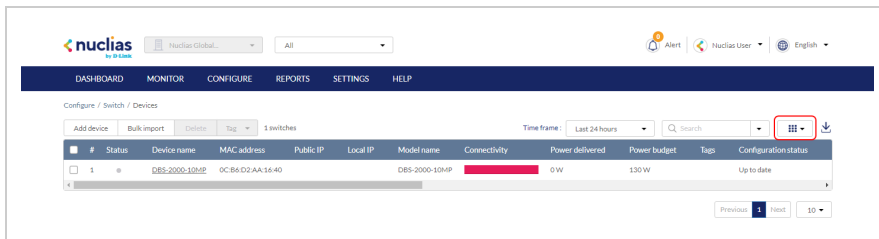
1. Navigate to **Configure > Switch > Profiles**.
2. From the Profile list, click **Push Configuration** under the Actions column of the Profile you wish to update the configuration settings of.  
**Note:** A result window will appear providing a summary of the update status.
3. In the Push Configuration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

# 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.

## Filtering Device Information

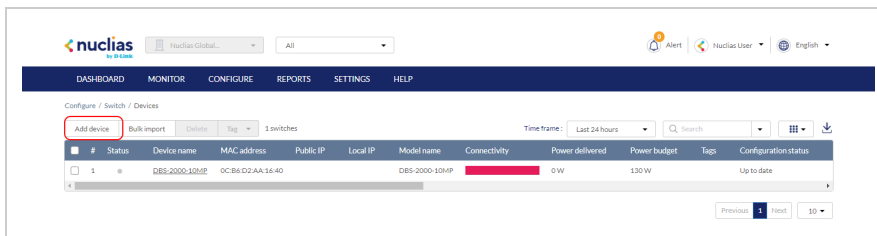
1. Navigate to **Monitor > Switch > Devices**.
2. [Optional] Select a time frame from the drop-down menu.
3. Click the filter selection in the top-right.



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

## Adding a Single Device

1. Navigate to **Configure > Switch > Devices**.
2. Click **Add device**.



3. Fill out the required information.

Device UID	Enter the device's UID found on the label printed on the device. The UID may be listed in the format XXXX-XXXX-XXXX or XXXXXXXXXXXXXX. 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.

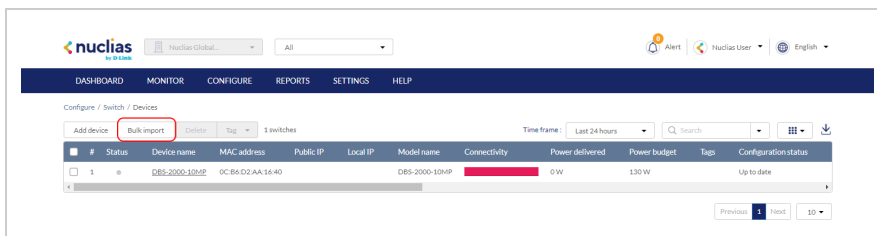
License Key	<p>Enter the device license key.</p> <p>Note: Every new device will be issued a one-year free license key. Once expired, an additional license must be purchased to continue using the device.</p>
-------------	--

4. Click **Save**.

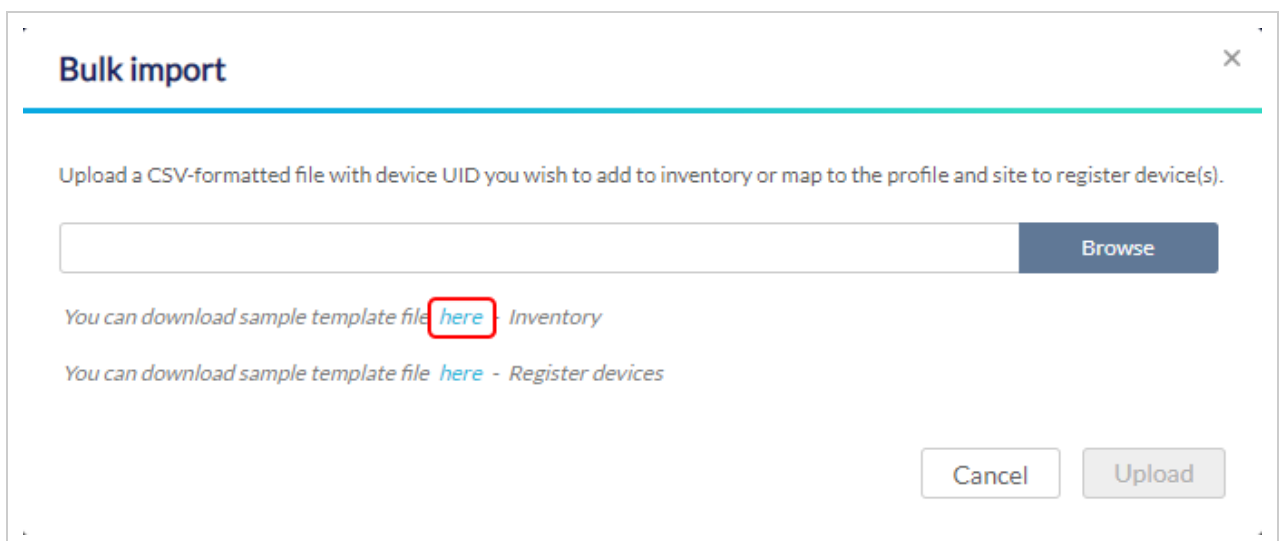
## Bulk Adding Multiple Devices to the Inventory

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 **Configure > Switch > Devices**.
2. Click **Bulk import**.



3. [Optional] Download the reference sample template.

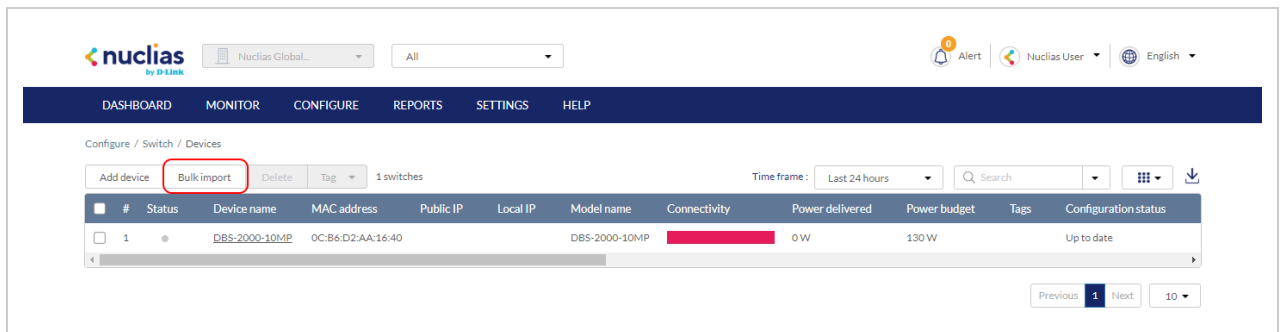


4. Click **Browse**.
5. Locate the CSV-formatted file containing the UIDs of the devices.  
**Note:** To add devices to the inventory, use the following format:  
[UID]
6. Click **Upload**.

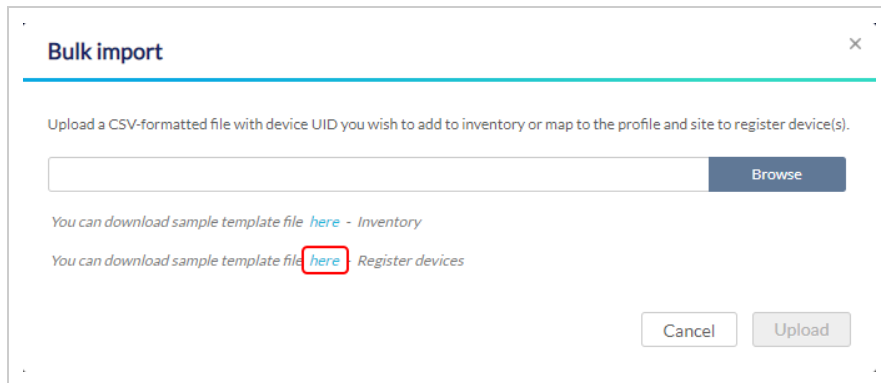
## Bulk Adding and Registering Multiple Devices to a Site

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 **Configure > Switch > Devices**.
2. Click **Bulk import**.



3. [Optional] Download the reference sample template.



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**.

## Adding a Tag to One or More Devices

Users can add descriptive tag to devices to identify and filter different devices or groups of devices. Tags are purely informational and do not affect the functionality of the device.

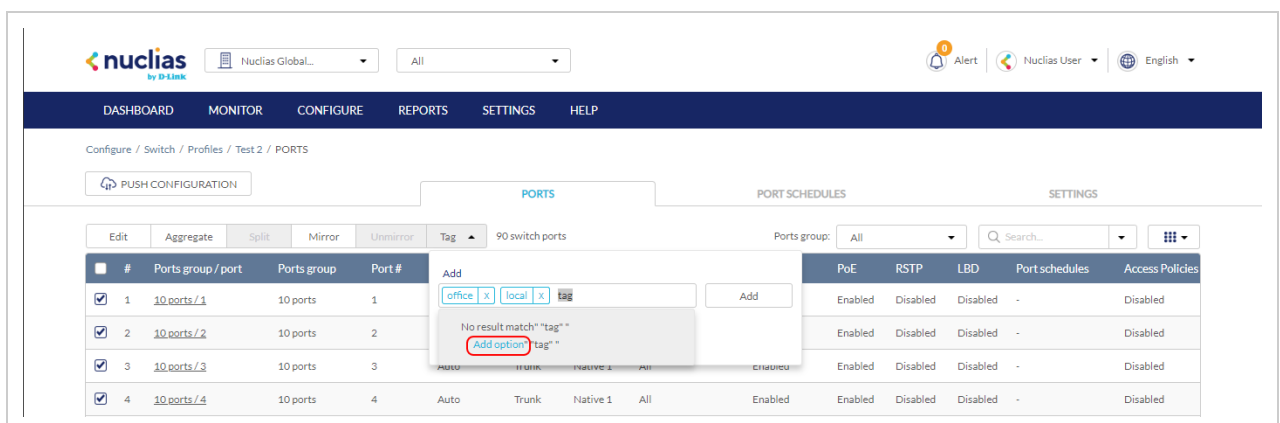
1. Navigate to **Configure > Switch > Profiles**.

2. From the devices list, check the box next to the tagged device(s) you wish to add a tag to.

3. Click **Tag**.

4. In the Add field, enter the tag content. Multiple tags can be entered.

**Note:** If this is a new tag, click **Add option** to make this a reusable tag.



5. Click **Add Tag**.

**Note:** Any tags associated to a device will be shown in the Tags column.

## Removing a Tag From One or More Devices

1. Navigate to **Configure > Switch > Devices**.
2. From the devices list, check the box next to the tagged device(s) you wish to remove the tag(s) from.
3. Click **Tag**.
4. In the Delete field, enter the tag name. Alternatively, click the input field to bring up a list with all the associated tags.
5. Click **Remove**.

## Editing a Device

1. Navigate to **Configure > Switch > Devices**.
2. From the device list, click the device name.
3. In the Device Information section, click the device name in the Name field. You will be navigated to the **Monitor > Switch > Device** page when you select a device from this list. Please refer to Monitor > Switch > Device for a comprehensive guide on how to edit and monitor your switch.

## 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 **Configure > Switch > Devices**.
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.

## 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 **Configure > Switch > Devices**.
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.

## Download the Device List

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

1. Navigate to **Configure > Switch > Devices**.
2. From the device list, click the Download icon in the top-right.

Configure / Switch / Devices

Add device Bulk import Delete Tag 1 switches Time frame: Last 24 hours Search [icon] [download icon]

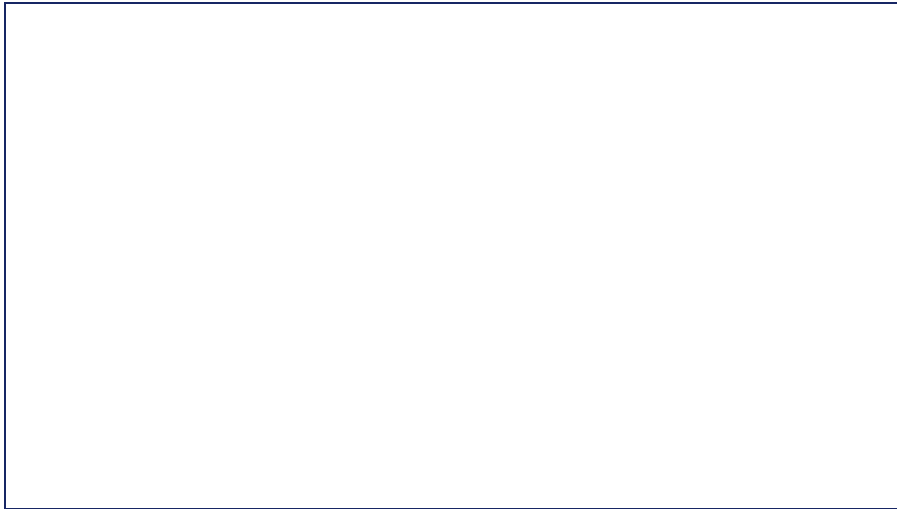
#	Status	Device name	MAC address	Public IP	Local IP	Model name	Connectivity	Power delivered	Power budget	Tags	Configuration status
1		DBS-2000-10MP	0C:B6:D2:AA:16:40			DBS-2000-10MP		0W	130W	test	Up to date

Previous 1 Next 10

# Switch Ports

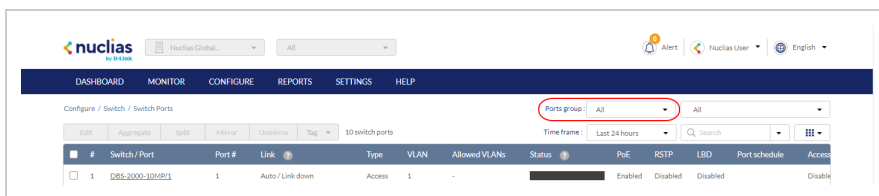
From the Switch Ports section, users can configure individual ports or groups of ports for physical switches. Any settings configured in this window are applied to the physical switch directly and override any overlapping or conflicting settings in the Profile applied to the switch.

Local switch configurations may be useful in cases where one switch in a group of switches requires specialized settings that are not configured in the associated Profile to accommodate a specific application.

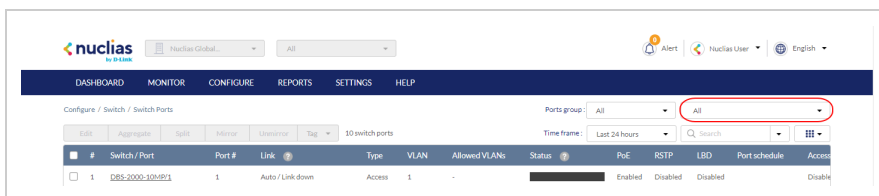


## Customizing the Switch Ports Configuration Overview

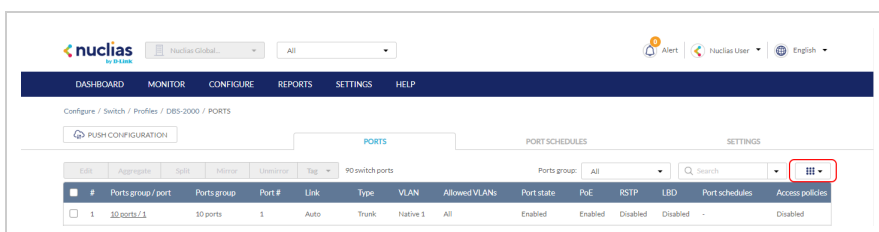
1. Navigate to **Configure > Switch > Switch Ports**.
2. Select a port group from the port groups drop-down menu. This will only display ports for the select port group profile. For example, selecting port group 28 will only show ports 1 to 28 of 28-port switches added to the organization. Select **All** to show all port groups.



3. If the organization has multiple switches of the same port group, for example multiple DBS-2000-10MP switches, select a specific switch from the drop-down menu to only show the ports of that switch.



4. Select a time frame from the time frame drop-down menu.
5. Click the filter parameter icon.



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

**Note:** All checked parameters will automatically appear.

## Configuring Local Port Settings for One or More Switch Ports

Switch port configuration allows administrators to configure extensive port functionality including port availability, port speed, RSTP, VLAN, PoE, and port activity schedules for an individual port or for a group of ports.

**Note:** These local settings will override any conflicting Profile settings associated with the device.

1. Navigate to **Configure > Switch > Switch Ports**.
2. From the port list, check the box next to the ports you wish to edit.
3. Click **Edit**.
4. Specify the following information:

**Note:** At the top of the edit port window is a list of all selected ports. The changes made will apply to all selected ports.

Port name	Enter a name for the port. If multiple ports are selected, this name will be applied to all ports.
Port state	Choose to enable or disable the port.
RSTP	Choose to enable or disable RSTP. <b>Note:</b> RSTP cannot be used in conjunction with LBD. <b>Note:</b> User must enable Profile/Settings/STP Configuration for this port to enable RSTP
STP guard	If RSTP is enabled, choose the guard type. Disabled: Do not use root guard enhancement. Root guard: Root guard enhancement allows administrators to define the position of the root bridge port in the network.
LBD	Choose to enable or disable LBD <b>Note:</b> LBD cannot be used in conjunction with RSTP.
Type	Choose the function type of the port. Trunk: Sends and receives tagged data from different VLANs. Access: Only sends and receives untagged data from the VLAN the port belongs to.
Native VLAN	Enter the ID of the native VLAN the port belongs to.

Allowed VLANs	Enter the IDs of the VLANs that can route traffic through this port. Enter <b>All</b> to allow all traffic from all VLANs to pass through this port.
Tags	Enter a descriptive tag for the port. Multiple tags can be entered. If multiple ports are selected, any tags will be applied to all ports.
Link (RJ45)	Choose the maximum link speed of the port. Select <b>Auto</b> to allow the port to auto-negotiate port speed with the partner port or device.
Link (SFP)	Choose the maximum link speed of the port. Select <b>Auto</b> to allow the port to auto-negotiate port speed with the partner port or device.
PoE	Choose to enable or disable Power over Ethernet (PoE) functionality on this port. <b>Note:</b> The PoE setting will only apply to ports that support Power over Ethernet.
Port Schedule	Choose a port schedule. Port schedules are separately configured. Refer to the <a href="#">Creating a Switch Port Schedule</a> section.

5. Click **Save**.

## Aggregating Switch Ports

Port aggregation allows users to link multiple physical ports together as one logical link to increase port bandwidth and redundancy in the event of a single physical link failure. Ports can be aggregated using either LACP or static link.

**Note:** Aggregated ports must maintain the same settings, otherwise users will not be permitted to aggregate multiple ports in one group.

**Note:** Port aggregation is not supported if the port type is set to "Access".

**Note:** These local settings will override any conflicting Profile settings associated with the device.

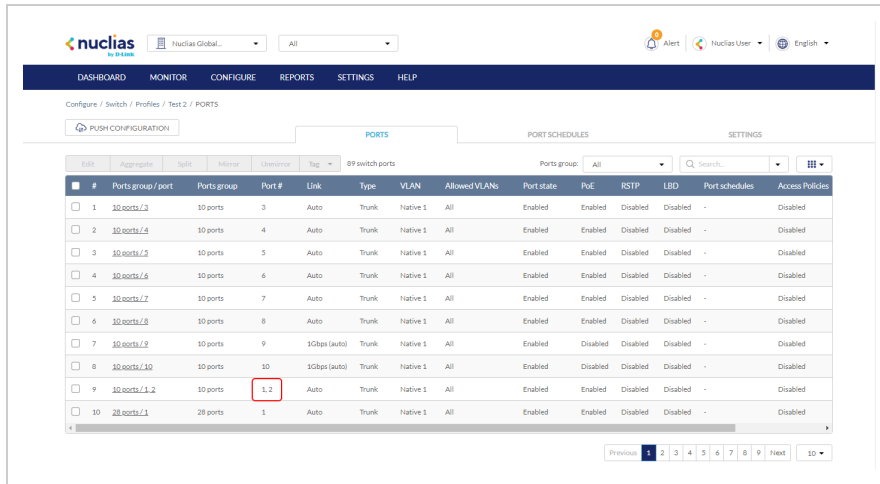
1. Navigate to **Configure > Switch > Profiles**.
2. From the Profile list, click **Ports** under the Actions column of the Profile you wish to edit.
3. From the port list, check the box next to the ports you wish to link together.
4. Click **Aggregate**.
5. In the Link Aggregation Setting window, select the aggregation type.

**Note:** Static link requires manual configuration of the ports in the aggregation group. Link Aggregation Control Protocol (LACP) dynamically queries to listening ports to join the aggregation group.

1. LACP
2. Static

6. Click **Aggregate**.

**Note:** Aggregated ports can be identified by the combined port number in the Port # column of the port overview.



7. Click **Push Configuration**.

## Splitting Aggregated Switch Ports

Linked port groups can be split into their respective individual ports. Splitting port groups will undo all aggregation settings applied to the affected ports.

**Note:** These local settings will override any conflicting Profile settings associated with the device.

1. Navigate to **Configure > Switch > Switch Ports**.
2. From the port list, check the box next to the aggregated port(s) you wish to split.
3. Click **Split**.

**Note:** This will immediately split the selected aggregated ports.

## Mirroring Port Traffic to Another Switch Port

Port Mirroring is a method of monitoring network traffic that forwards a copy of each incoming and/or outgoing packet from one port of the switch to another port, where the packet can be studied. This enables network managers to better monitor network performance.

**Note:** These local settings will override any conflicting Profile settings associated with the device.

1. Navigate to **Configure > Switch > Switch Ports**.
2. From the port list, check the box next to the port(s) you wish to mirror.
3. Click **Mirror**.
4. Specify the following information:

Source ports	Select the data to mirror from the drop-down menu for each selected port.  Both: Mirror both incoming and outgoing.  Rx: Mirror only data received on the port.  Tx: Mirror only data transmitted by the port.
Destination port	Enter the destination port number. <b>Note:</b> The port number should be in numerical format, for example 28.

5. Click **Create port mirror**.

# Undoing Port Traffic Mirroring

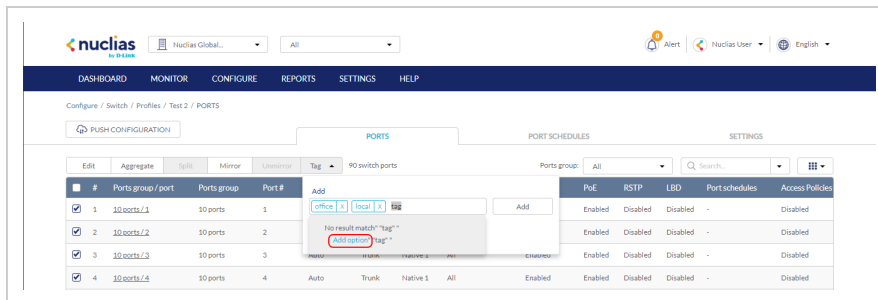
1. Navigate to **Configure > Switch > Switch Ports**.
2. From the port list, check the box next to the mirrored port(s) you wish to unmirror.
3. Click **Unmirror**.  
**Note:** This will immediately undo the selected mirrored ports.
4. Click **Push Configuration**.

# Adding a Tag to One or More Switch Ports

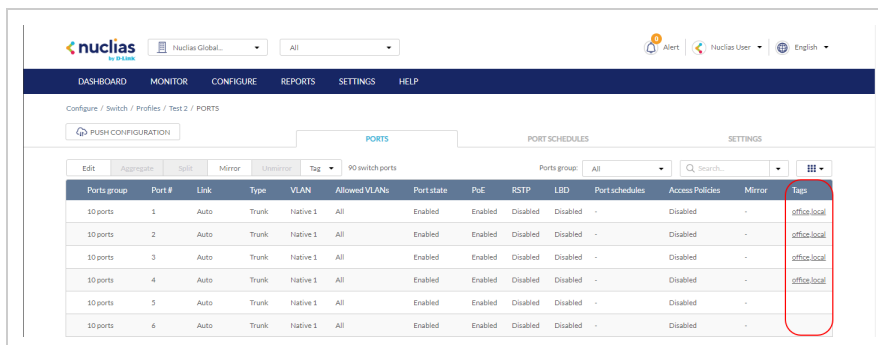
Users can add descriptive tag to ports to identify and filter different ports or groups of ports. Tags are purely informational and do not affect the functionality of the port.

**Note:** These local settings will override any conflicting Profile settings associated with the device.

1. Navigate to **Configure > Switch > Switch Ports**.
2. From the port list, check the box next to the port(s) you wish to add a tag to.
3. Click **Tag**.
4. In the Add field, enter the tag content. Multiple tags can be entered.  
**Note:** if this is a new tag, click Add option to make this a reusable tag.



5. Click **Add**.  
**Note:** Any tags associated to a port will be shown in the Tags column.



# Removing a Tag from One or More Switch Ports

1. Navigate to **Configure > Switch > Switch Ports**.
2. From the port list, check the box next to the tagged port(s) you wish to remove the tag(s) from.
3. Click **Tag**.
4. In the Delete field, enter the tag name. Alternatively, click the input field to bring up a list with all the associated tags.
5. Click **Remove**.

# Reports

---

From the Reports section, users can view and generate detailed reports for changes on the platform such as switch activity, network alerts, and license reports.

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

<a href="#">Change Log</a>	From the Change Log section, users can consult a detailed log of changes occurring on the network.
<a href="#">Access Point</a>	From the access point section, users can view detailed reports about AP activity on the managed network.
<a href="#">Switch</a>	From the switch section, users can view detailed reports about switch activity on the managed network.
<a href="#">Alerts</a>	From the Alerts section, users can view a detailed log of all alerts occurring on the network.
<a href="#">Licenses</a>	From the Licenses section, users can consult a list of detailed information about licenses assigned to the selected organization.

# Change Log

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

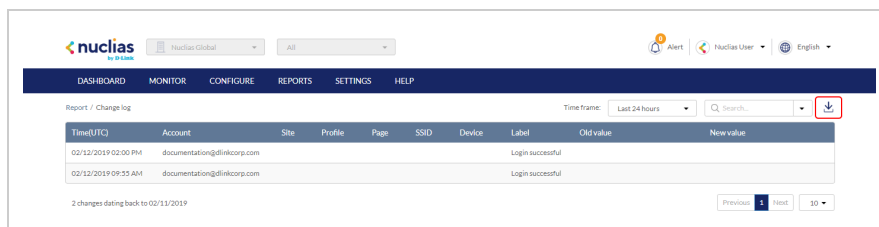
## Searching for Change Events

1. Navigate to **Reports > Change Log**.
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 that 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.

## Downloading Change Logs

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



# Reports-Access Point

---

## Filtering the Access Point Logs

1. Navigate to **Reports > Access Point**.
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**.

## Sending Access Point Logs by Email

1. Navigate to **Reports > Access Point**.
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**.

## Download Archived Access Point Logs

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

1. Navigate to **Reports > Access Point**.
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**.

## Download Access Point Logs

1. Navigate to **Reports > Access Point**.
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**.



# Reports- Switch

---

## Filtering the Switch Logs

1. Navigate to **Reports > Switch**.
2. [Optional] Select a time frame from the drop-down menu.
3. Check the profiles to filter switch logs for from the Device report drop-down menu.
4. Check the devices to filter switch 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 switch 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 switch logs to show from the Customize report drop-down menu. Select **All** to show all report types.
8. Click **Preview**.

## Sending Switch Logs by Email

1. Navigate to **Reports > Switch**.
2. [Optional] Select a time frame from the drop-down menu.
3. Check the profiles to filter switch logs for from the Device report drop-down menu.
4. Check the devices to filter switch 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 switch 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 switch 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 switch log with the selected parameters.
9. Click **Send email**.

## Download Archived Switch Logs

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

1. Navigate to **Reports > Switch**.
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**.

## Download Switch Logs

1. Navigate to **Reports > Switch**.
2. [Optional] Select a time frame from the drop-down menu.
3. Check the profiles to filter switch logs for from the Device report drop-down menu.
4. Check the devices to filter switch 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 switch 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 switch 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 switch log with the selected parameters.
9. Click **Download**.

# Alerts

---

From the Alerts window, users can view a detailed log of all alerts occurring on the network. Alerts are divided into two types: processed and not 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 for more information.

## 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 **Reports > Alerts**.
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.

## 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 **Reports > Alerts**.
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.

## 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 **Reports > Alerts**.
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.

# Searching for Alerts

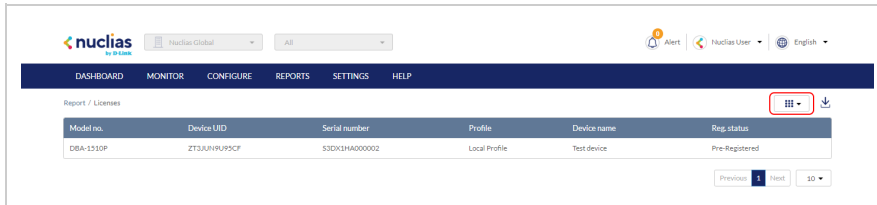
1. Navigate to **Reports > Alerts**.
2. Click the **Not Processed** or **Processed** tab to filter the shown alerts.
3. [Optional] Select a time frame from the drop-down menu.
4. From the alert list, click the Search field.
5. Enter the alert name.  
**Note:** All alerts matching the value entered in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

Device type	Select the device type from the drop-down menu to filter alerts for.
Device name	Enter the name of the device that triggered the alert.
Severity	Select an alert severity level from the drop-down menu.

# Licenses

## Filtering the License Logs

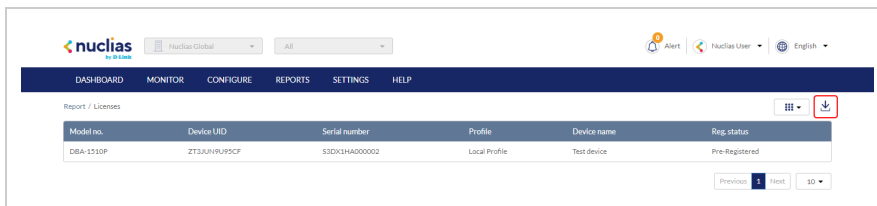
1. Navigate to **Reports > Licenses**.
2. Click the filter selection in the top-right.



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

## Downloading License Logs

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



# Settings

---

<a href="#">Account Management</a>	<p>From the Account Management section, users can view a full overview that includes detailed information of all managed user accounts, invite new users, and edit existing users.</p> <p>Refer to the <a href="#">Account Management</a> section for more information.</p>
<a href="#">Organization Management</a>	<p>From the Organization Management section, users can create and edit Sites and Site Tags, as well as invite users to the organization.</p> <p>Refer to the <a href="#">Organization Management</a> section for more information.</p>
<a href="#">License Management</a>	<p>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.</p> <p>Refer to the <a href="#">License Management</a> section for more information.</p>
<a href="#">Inventory</a>	<p>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.</p> <p>Refer to the <a href="#">Inventory</a> section for more information.</p>
<a href="#">Firmware</a>	<p>From the Firmware section, users can set device upgrade schedules, or manually upgrade a device's firmware.</p> <p>Refer to the <a href="#">Firmware</a> section for more information.</p>
<a href="#">Alert Settings</a>	<p>From the Alert Settings section, users can choose the type of network events that will trigger alert notifications.</p> <p>Refer to the <a href="#">Alert Settings</a> section for more information.</p>
<a href="#">Add Device</a>	<p>From the Add Device section, users can quickly add a new device to the organization.</p> <p>Refer to the <a href="#">Add Device</a> section for more information.</p>

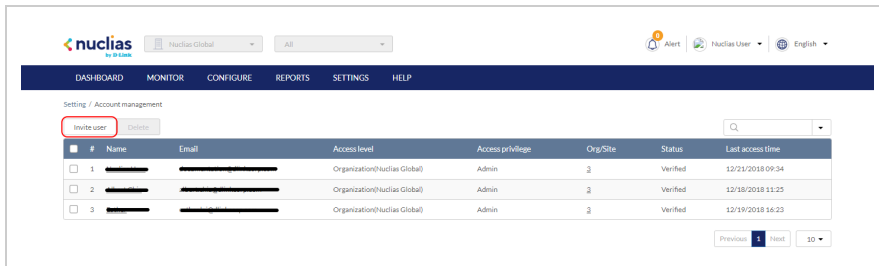
# Account Management

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.

## Inviting a New User

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



3. Specify the following information:

User name	Enter the user's name.
Email address	Enter the user's email address. This is also the user name to log into the Nuclias Portal interface.
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.
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.
Managed Site	This determines which Sites of which the organization can be viewed by the user. Selecting All sites will allow the user to see all Sites under the selected organization.

4. Click **Submit**.

## Editing an Existing User

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

Name	Enter a user name
Role	<p>Select a role for the user. Roles determine the degree of editing and viewing privileges of the user.</p> <p>Admin: Full editing and full viewing rights.</p> <p>Editor: Partial editing and full viewing rights.</p> <p>Monitor: Limited editing and partial viewing rights.</p> <p>Viewer: Limited viewing rights.</p>
Managed Site	<p>This determines which Sites of which the organization can be viewed by the user. Selecting All sites will allow the user to see all Sites under the selected organization.</p>

4. Click **Save change**.

## Searching for a User

1. Navigate to **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.

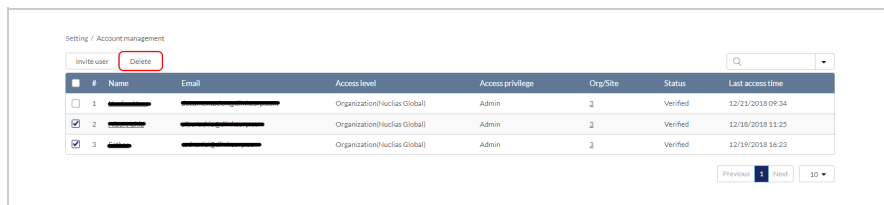
## Deleting a User

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 **Settings > Account Management**.

- From the user account list, click the checkbox next to the user account(s) you wish to delete.
- Click **Delete**.



- 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.
- Click **Yes**.  
**Note:** The deleted user will receive a notification email to confirm the account was deleted.

# Organization Management

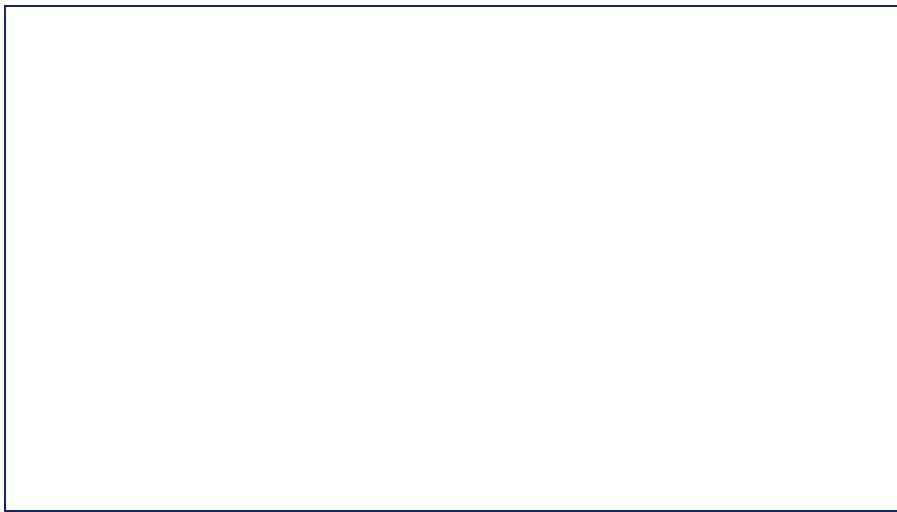
---

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.

## Creating a New Organization

Organization creation is only available for MSP-level users. Normal user accounts cannot create additional organizations.

## 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 **Settings > Organization Management**.
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**.

## Adding A Site Tag to an Organization

1. Navigate to **Settings > Organization Management**.
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**.

## 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 **Settings > Organization Management**.
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 <b>All</b> will allow the user to see all Sites under the selected organization.
Role	<p>Select a role for the user. Roles determine the degree of editing and viewing privileges of the user.</p> <p>Admin: Full editing and full viewing rights.</p> <p>Editor: Partial editing and full viewing rights.</p> <p>Monitor: Limited editing and partial viewing rights.</p> <p>Viewer: Limited viewing rights.</p>

4. Click **Save**.

## Deleting an Organization

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

# 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.



## Adding a License Key

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

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

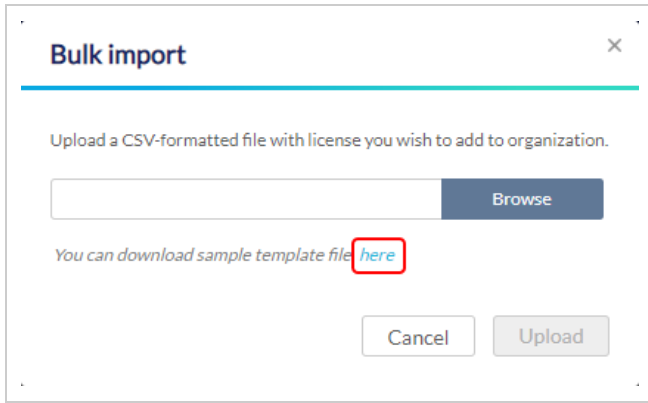
License Key	Enter a valid license key.
-------------	----------------------------

4. Click **Add**.

## Bulk Adding Multiple Licenses

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

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



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

## Searching for a License Key

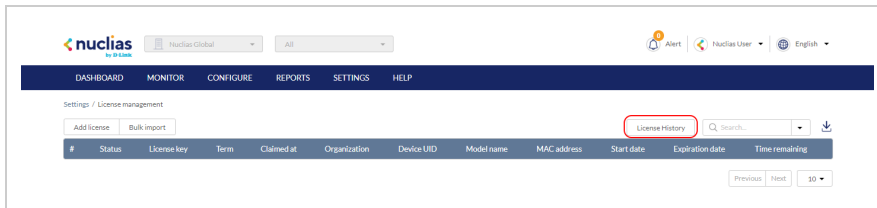
1. Navigate to **Configure > License Management**.
2. From the license key list, click the Search field.
3. Enter the license key number.  
**Note:** All license keys matching the value entered in the search field will automatically appear.
4. [Optional] Click the filter drop-down menu and enter the 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.

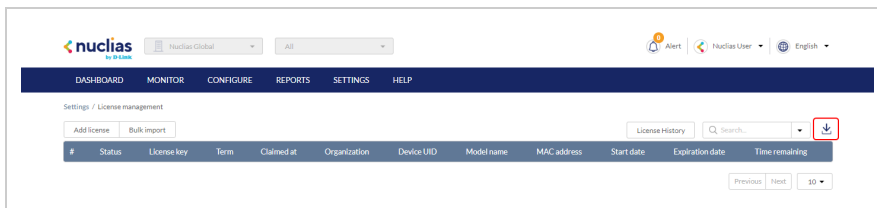
## Viewing the License History

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



## Downloading License Key List

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



# Inventory

---

From the Inventory window, 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.

## 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 **Settings > Inventory**.
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 XXXXXXXXXXXXXXX. When entering the UID, do not include dashes.
Device Name	Enter a name for the device.

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

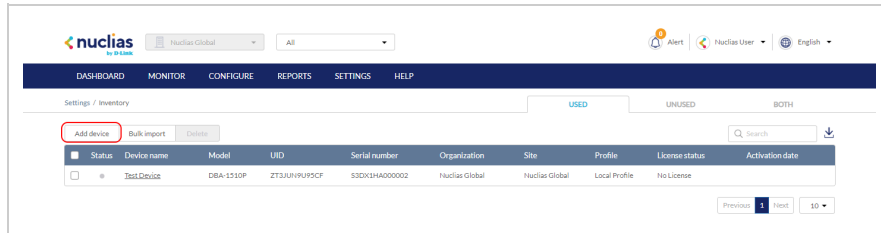
Site	Select a Site to link this device to.
Profile	Select a Profile for this device. The device will use the settings configured in that profile.
License Key	[Optional] Enter the device license key.  Note: Every new device will be issued a one-year free license key. Once expired, an additional license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

6. Click **Save**.

## 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 **Settings > Inventory**.
2. Click **Add device**.



3. Specify the following information:

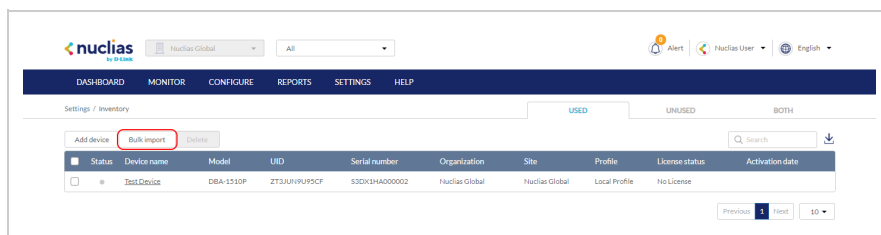
Device UID	Enter the device's Unique Identifier (UID) found on the label printed on the device. The UID may be listed in the format XXXX-XXXX-XXXX or XXXXXXXXXXXXXXX. When entering the UID, do not include dashes.
Device Name	Enter a name for the device.

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

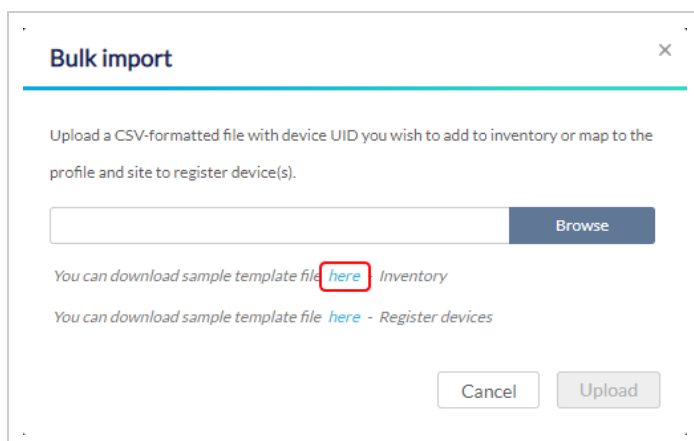
## Bulk Adding Multiple Devices to the Inventory

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 **Settings > Inventory**.
2. Click **Bulk import**.



3. [Optional] Download the reference sample template.

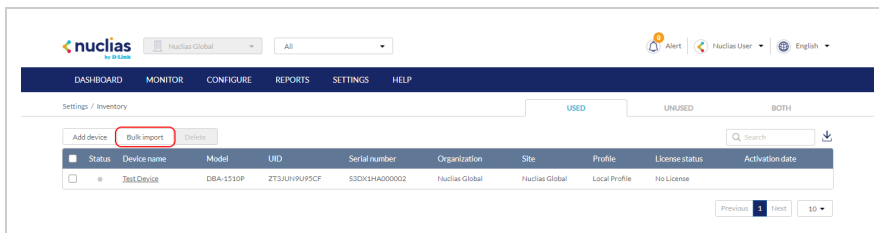


4. Click **Browse**.
5. Locate the CSV-formatted file containing the UIDs of the devices.  
Note: To add devices to the inventory, use the following format:  
[UID]
6. Click **Upload**.

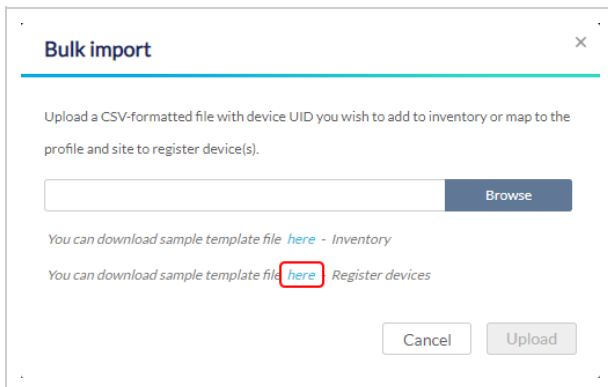
## Bulk Adding and Registering Multiple Devices to a Site

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 **Settings > Inventory**.
2. Click **Bulk import**.



3. [Optional] Download the reference sample template.

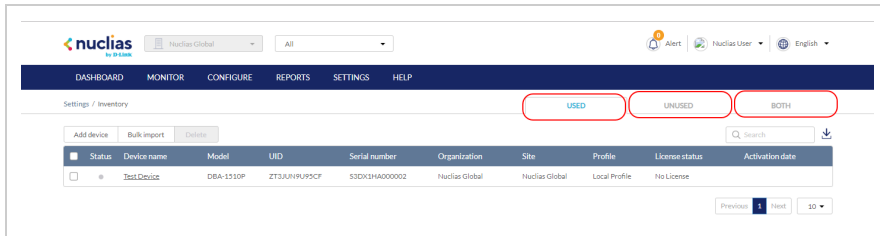


4. Click **Browse**.
5. Locate the CSV-formatted file containing the UIDs of the devices.  
Note: To directly register devices to a Site, use the following format:  
[UID][Device Name][Profile Name][Site][License Key]
6. Click **Upload**.

## 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.

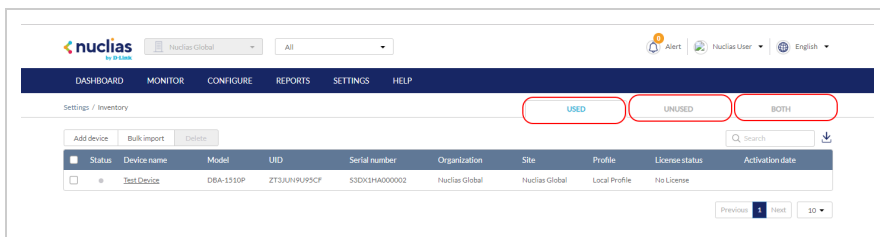
1. Navigate to **Settings > Inventory**.
2. Click the tab of the inventory list to filter shown devices.



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**.

## Searching for a Device

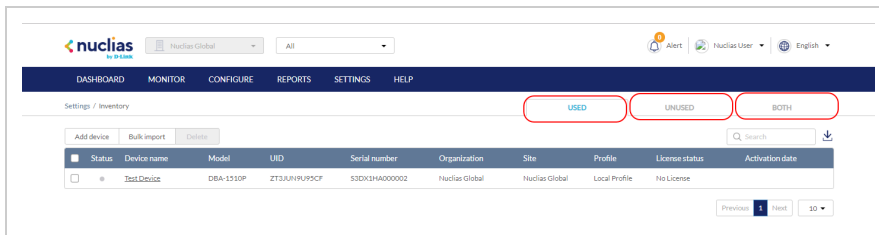
1. Navigate to **Configure > Inventory**.
2. Click the tab of the inventory list to filter shown devices.



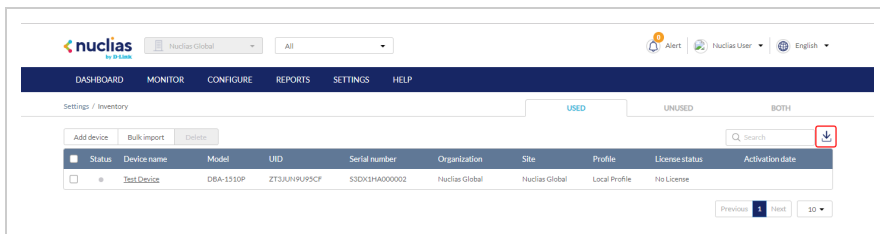
3. From the device list, click the Search field.
4. Enter the device name.  
**Note:** All devices matching the value entered in the search field will automatically appear.

## Exporting the Inventory List

1. Navigate to **Settings > Inventory**.
2. Click the tab of the inventory list you wish to export.  
**Note:** Each tab exports a separate inventory list for the respective tab.

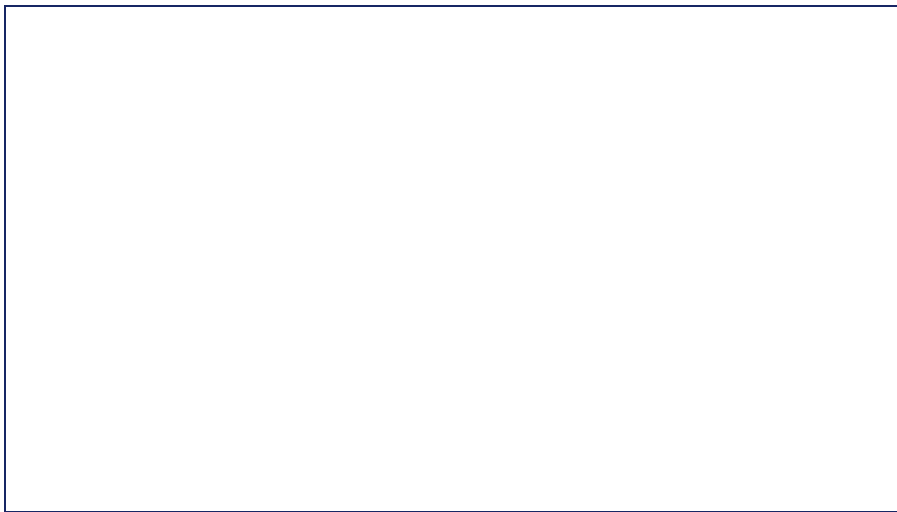


3. From the device list, click the **Download** icon in the top-right.



# Firmware

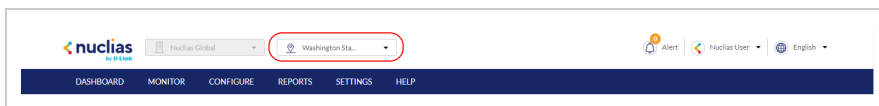
From the Firmware window, users can view basic firmware information, and set up a firmware upgrade schedule. Firmware upgrades are managed at the Site level and configured per device type, which means that all devices of the same type that are linked to that Site will use the same firmware upgrading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



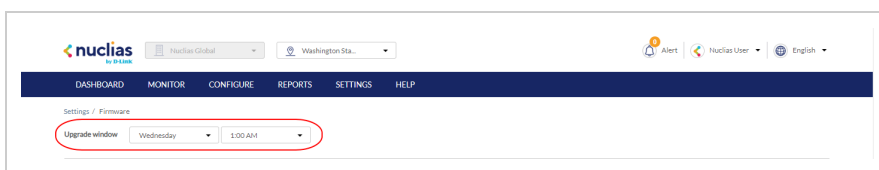
## Setting an Automatic Upgrade Window

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.

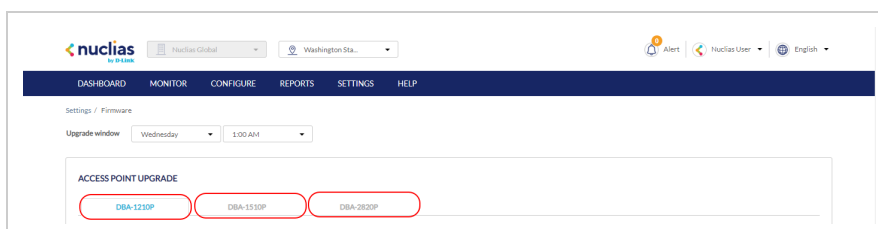
1. Navigate to **Settings > Firmware**.
2. Select a Site from the Site menu in the top of the screen.



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



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.

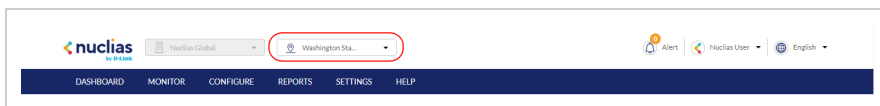


5. Select Follow upgrade window.
6. Click **Save**.

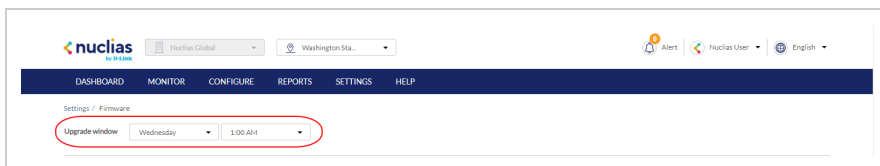
## Setting a Custom Device Upgrade Time

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

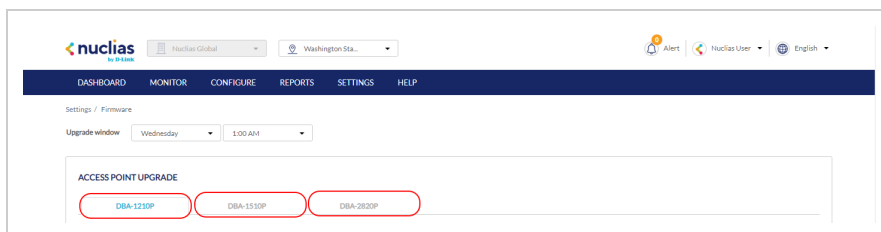
1. Navigate to **Settings > Firmware**.
2. Select a Site from the Site menu in the top of the screen.



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



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.

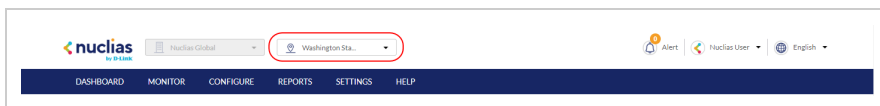


5. Select **Reschedule the upgrade to**.
6. Click the date field to choose a date and select a time from the drop-down menu.
7. Click **Save**.

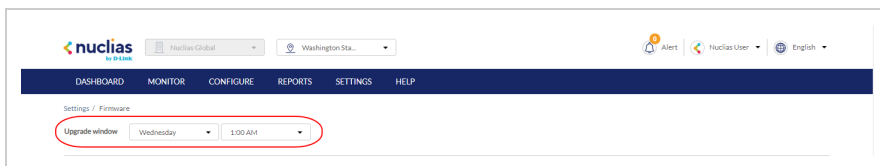
## Performing a Manual Firmware Upgrade

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

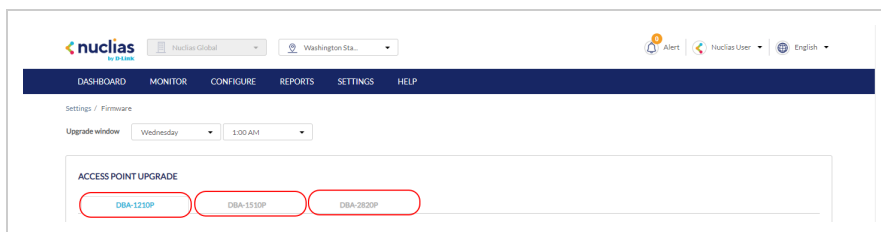
1. Navigate to **Settings > Firmware**.
2. Select a Site from the Site menu in the top of the screen.



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



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.



5. Select **Perform the upgrade now**.
6. Click **Upgrade now**.
7. When prompted to confirm, click **Yes**.

# Alert Settings

---

## 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 **Settings > Alert Settings**.
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 successfully upgraded.
Firmware upgrade failed	Sends an alert notification when a device firmware upgrade failed.
Device added to profile	Sends an alert notification when a device has been 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, select a time (in minutes) from the drop-down menu, and check the respective checkbox to receive notifications by email or through the app whenever the device goes offline for longer than the selected time period.
4. In the Switch section, select a time (in minutes) from the drop-down menu, and check the respective checkbox to receive notifications by email or through the app whenever the device goes offline for longer than the selected time period.
5. Select **Any port** or a specific from the drop-down menu, select a time (in minutes) from the drop-down menu, and check the respective checkbox to receive notifications by email or through the app whenever the selected port(s) are down for longer than the selected time period.
6. Click **Save**.

# Add Device

---

1. Navigate to **Settings > Add device**.

**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 <b>XXXX-XXXX-XXXX</b> or <b>XXXXXXXXXXXXXX</b> . 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**.

# Help

---

## 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.

### Contacting Nuclias Support

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

Name	Click to enter a sender name. The recipient will see this name. By default, this is the username.
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 <b>Add</b> 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**.

# Nuclias Cloud Mobile App

---

The Nuclias Cloud App is D-Link's mobile cloud-based networking solution. With the Nuclias App, organizations can deploy, configure, manage and monitor networks, all from the convenience of your mobile device.

## Download the Nuclias Cloud App

The Nuclias Cloud App is currently available for iOS smart devices. Go to the App Store and search for Nuclias, or scan the QR code below:



## Logging into your Nuclias Cloud Account

After you have downloaded and installed the Nuclias Cloud app from the app store, open the application and you will be prompted to enter your Nuclias Cloud account's email and password.

Note: It is recommended you first register, set up and configure your account from the your desktop, then login using your existing account.

# Access Points

---



**DBA-1210P**

Nuclias Cloud Managed AC1300 Wave 2 Access Point



**DBA-1510P**

Nuclias Cloud Managed AC1750 Access Point



**DBA-1520P**

Nuclias Cloud Managed AC1750 Wave 2 Access Point

---



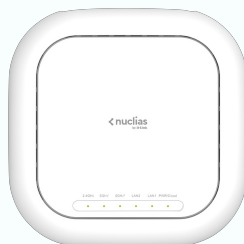
**DBA-2520P**

Nuclias Cloud Managed AC1900 Wave 2 Access Point



**DBA-2620P**

Nuclias Cloud Managed AC1300 Wave 2 Access Point



**DBA-2720P**

Nuclias Cloud Managed AC1300 Wave 2 Access Point



**DBA-2820P**

Nuclias Cloud Managed AC2600 Wave 2 Access Point

---



**DBA-3620P**

Nuclias Cloud Managed AC1300 Wave 2 Outdoor Access Point



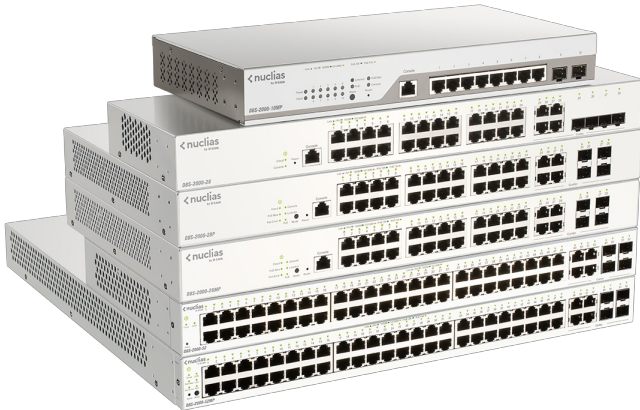
DBA-3621P

Nuclias Cloud Managed AC1300 Wave 2 Outdoor Access Point

---

# Switches

---



## DBS-2000 Series



### [DBS-2000-10MP](#)

10-Port Nuclias Cloud-Managed PoE Switch



### [DBS-2000-28](#)

28-Port Nuclias Cloud-Managed Switch



[DBS-2000-28MP](#)

**28-Port Nuclias Cloud-Managed PoE Switch**

---



[DBA-2000-28P](#)

**28-Port Nuclias Cloud-Managed Switch**

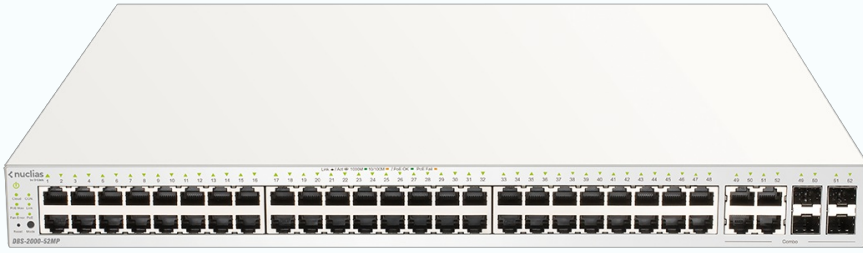
---



[DBA-2000-52](#)

**52-Port Nuclias Cloud-Managed Switch**

---



[DBS-2000-52MP](#)

52-Port Nuclias Cloud-Managed PoE Switch