D-Link

2023 | Business Class

NUCLIAS CLOUD

User Manual

V 2.0

nuclias CLOUD

Getting Started with Nuclias

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 network functions with recommended settings.

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

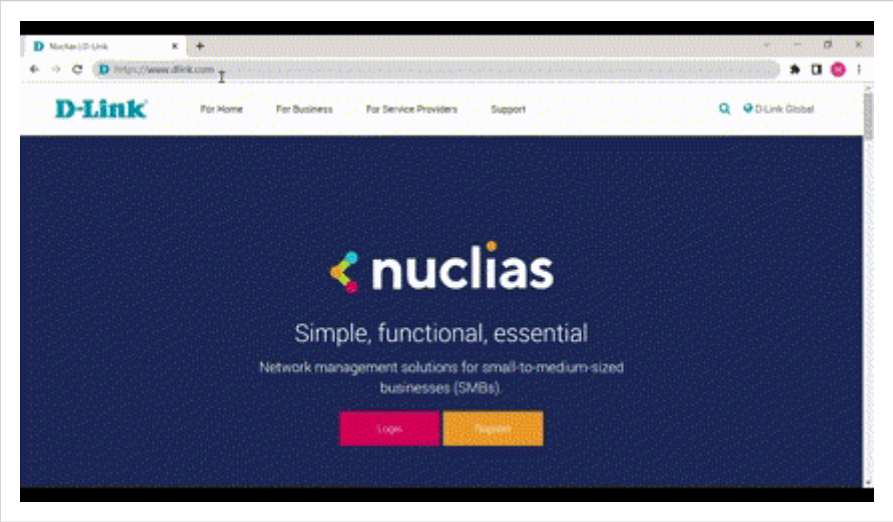
Creating an Account

Logging in to Nuclias Cloud

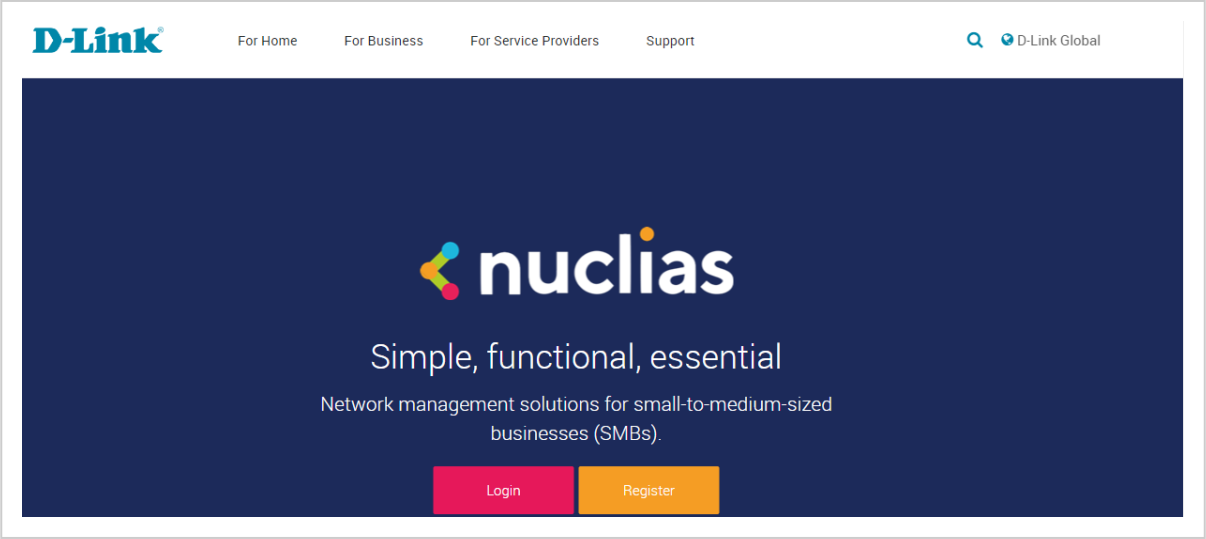
Adding Devices

Creating an Account

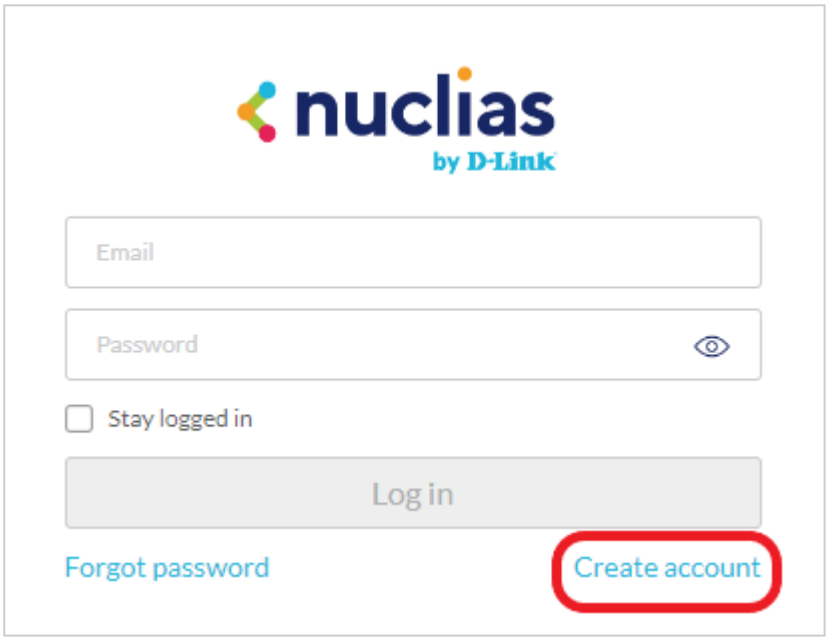
Access to the D-Link Nuclias Cloud can be obtained by signing up for a free Nuclias account.



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



2. Click **Create Account**.



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

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

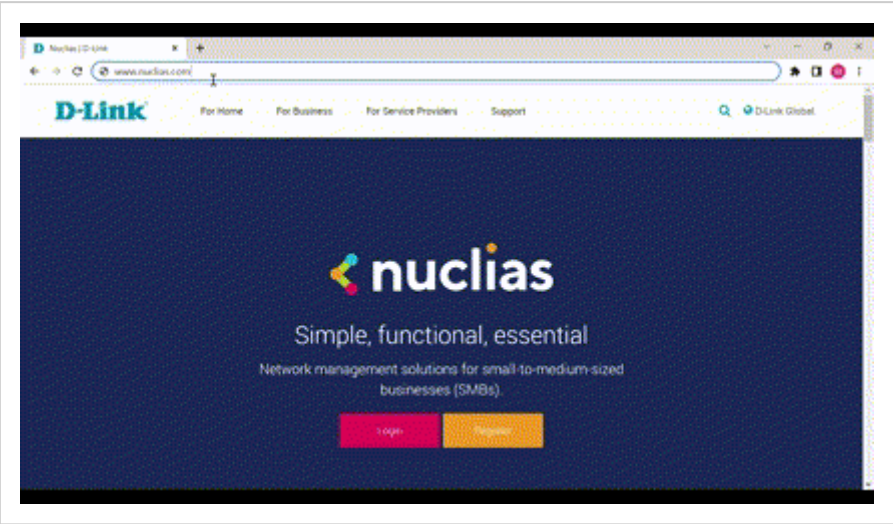
4. Fill out the required information:

Email	Enter your email address. This is also your username to log into the Nuclias Portal interface and it must be unique.
Full Name	Enter your full name
Password	Enter your account password.
Confirm Password	Confirm your password.

Organization Name	Enter your organization name. This will automatically create an organization with this name.
Country	Select a country. This will automatically create a Site using this country and operating the legit channels for your wireless devices.
Timezone	Select a time zone.
Address	Enter your address. This will automatically create a Site using this address that be managed on the Map in the Nuclias portal.

5. Click **I have read and agree to the Terms and Privacy** to continue.
6. Click **Create Account**.
7. 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 www.nuclias.com and click **Login**.
2. Enter your registration email address and password.
3. Click **Log In**.

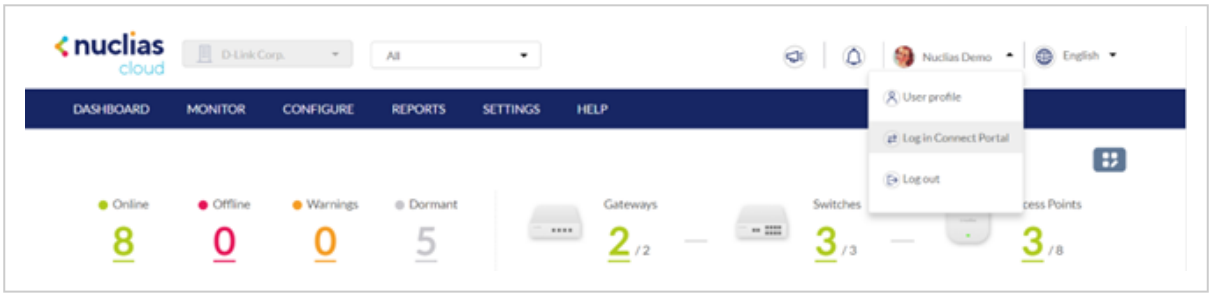
Log Out

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

Log in to Connect Portal

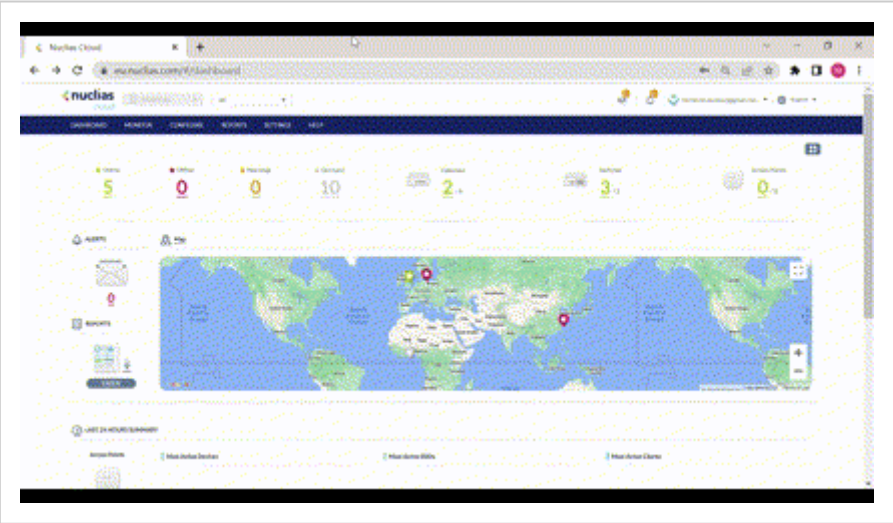
You can directly log in to Nuclias Connect portal from the Nuclias Cloud portal using the Single Sign On function (SS0).

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


nuclias
cloud
D-Link Corp.
All
Nuclias Demo
English
DASHBOARD
MONITOR
CONFIGURE
REPORTS
SETTINGS
HELP
User profile
Log in Connect Portal
Log out
Online
8
Offline
0
Warnings
0
Dormant
5
Gateways
2 / 2
Switches
3 / 3
3 / 8

Adding Devices

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

For first time users, simply go to **Settings > Add device** to add your device with a default profile and site information for quick setup.

You may also go to **Settings > Inventory** (only available to users with the access privilege to all sites) to add devices or to bulk import devices that can be registered later with selected license terms or assign devices to a Site and Profile.

Alternatively, with all the Site and Profile set, devices can be added directly to your Organization or Site by device category. Devices are assigned to a specific Site and Profile to automatically apply the configurations once connected to Nuclias Cloud.

To add a device:

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



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 **XXXXXXXXXXXX**.
Device Name	**[Optional]** Enter a name for the device.
Site	Select a Site to assign this device to.
Profile	Select a Profile for this device to apply that Profile's configuration settings. Click on the drop-down menu to display a list of available profiles for your model (the system will automatically detect the device model if the UID is entered correctly) .
License Key	**[Optional]** Enter the license key. Click on the drop-down menu to display a list of available licenses for this device type. **Note:** Every new device will be issued a one year complimentary license key. You may add more license keys to extend the period of use.

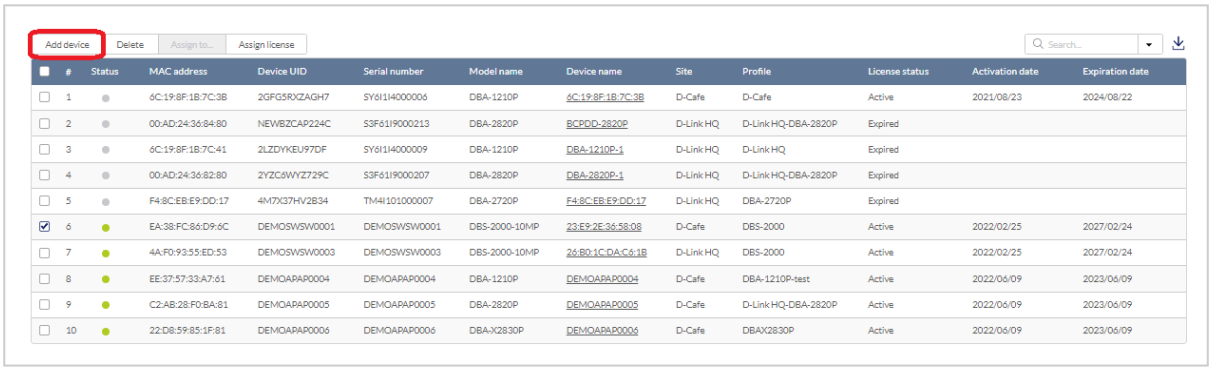
	Once expired, an additional license must be purchased to continue using this device.

Click **Save** when you are done.

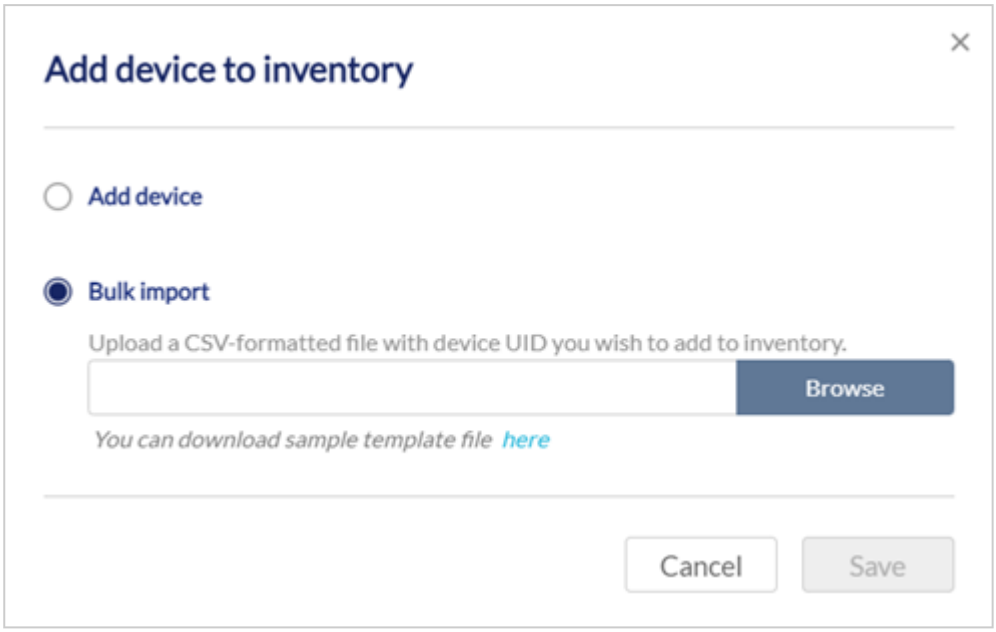
Adding Devices to the Inventory

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

1. Navigate to **Settings > Inventory** and select the **Devices** tab. Then click **Add device** to add devices to the inventory by entering the UID. Or click **Bulk import** to import multiple devices.



2. [Optional] Download the reference sample template to bulk import devices to the Inventory.



3. Click **Browse**.

4. Locate the CSV-formatted file containing the UIDs of the devices as shown in the following example:



5. Click **Save**.

Bulk Assigning Devices with Configuration

Devices can be bulk imported to the Inventory with basic configuration and registration information.

1. Navigate to **Settings > Bulk import devices**.
2. [Optional] Download the reference sample template.
3. Click **Browse**.
4. Locate the CSV file containing the UIDs and other required information such as Site and Time Zone (you can also enter Profile assignment and License keys for device registration) as shown in the following example:

UID	Device name	Site	Time Zone	Profile	License-1	License-2	License-3
FFFFEEEE0001	DBS	Taipei	Asia/Taipei				
FFFFEEEE0002	DBA	Hsinchu	Asia/Taipei				
FFFFEEEE0003	DBG	Hsinchu	Asia/Taipei				

5. Click **Upload**.

Portal

Portal - Overview

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

Introduction

Interface Overview

Dashboard

Monitor

Configure

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

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

Terms and Concepts

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

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 Service Provider (SP) or Managed Service Provider (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, and small to medium sized offices.

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

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

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

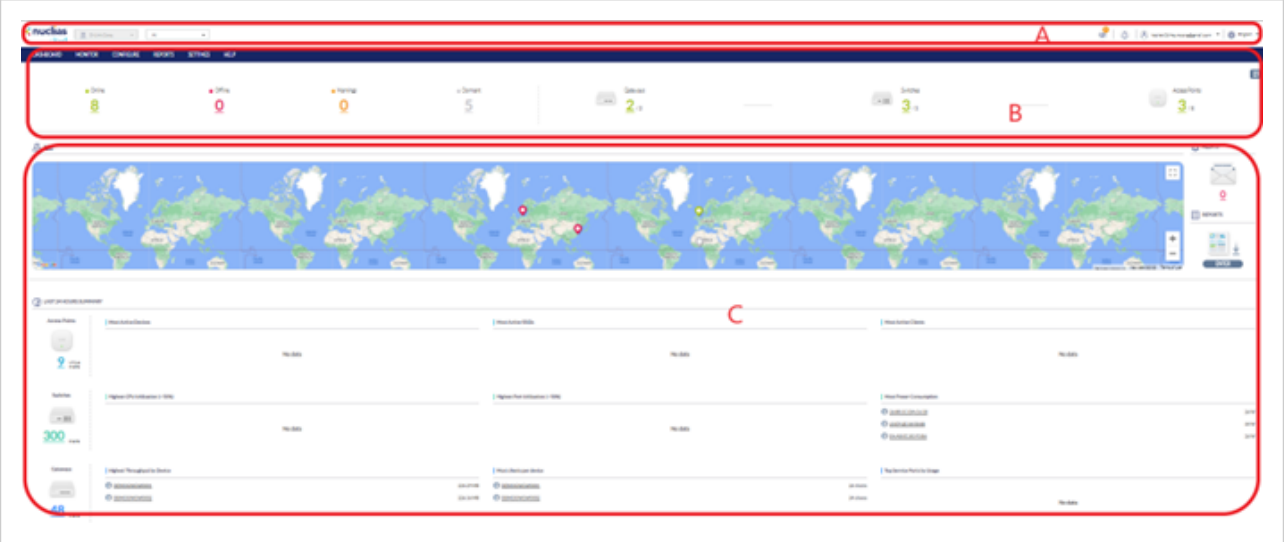
Privileges: Privileges determines to what extent a user can actively manage, ranging from full access to viewing only. Some elements of the Portal interface may be locked depending on the selected privilege. Refer to the overview below for a list of all available privileges.

Admin	An administrator has full access to all elements of the Portal interface and has full management capabilities.

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

Interface

Interface Overview



Section	Item	Description
A	Global Toolbar	Provides access to the organization and site selection menu as well as alerts, user account, and language menu.
B	Management Toolbar	Provides access to the various device management and information, report, and inventory sections.
C	Dashboard	The interactive dashboard to manage and configure through the Nuclias Portal. The 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

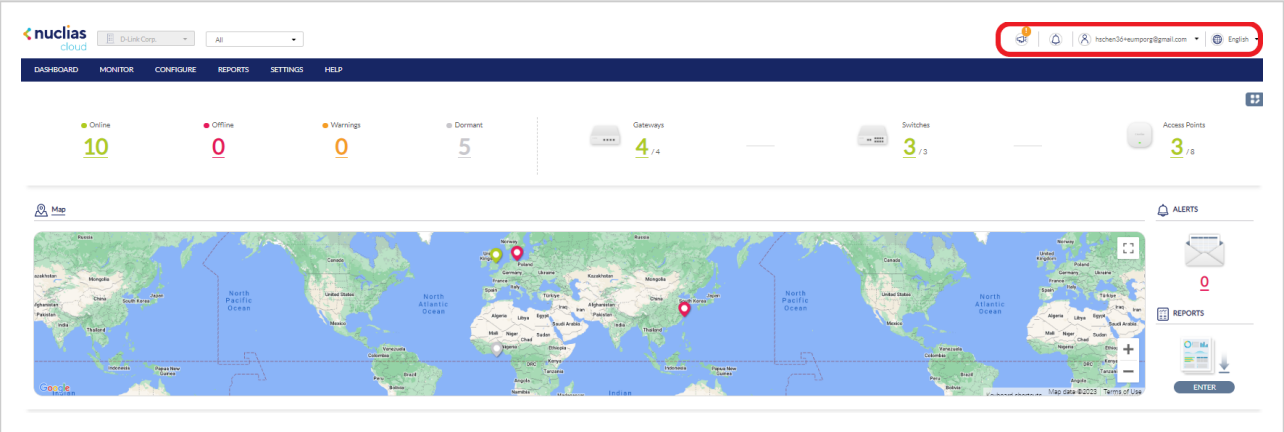
By selecting a specific Site, you can view network activity and client information associated with the devices of the Site and the Map for the selected Site. Certain management features such as alerts and reports are also handled on the Site-level.

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.

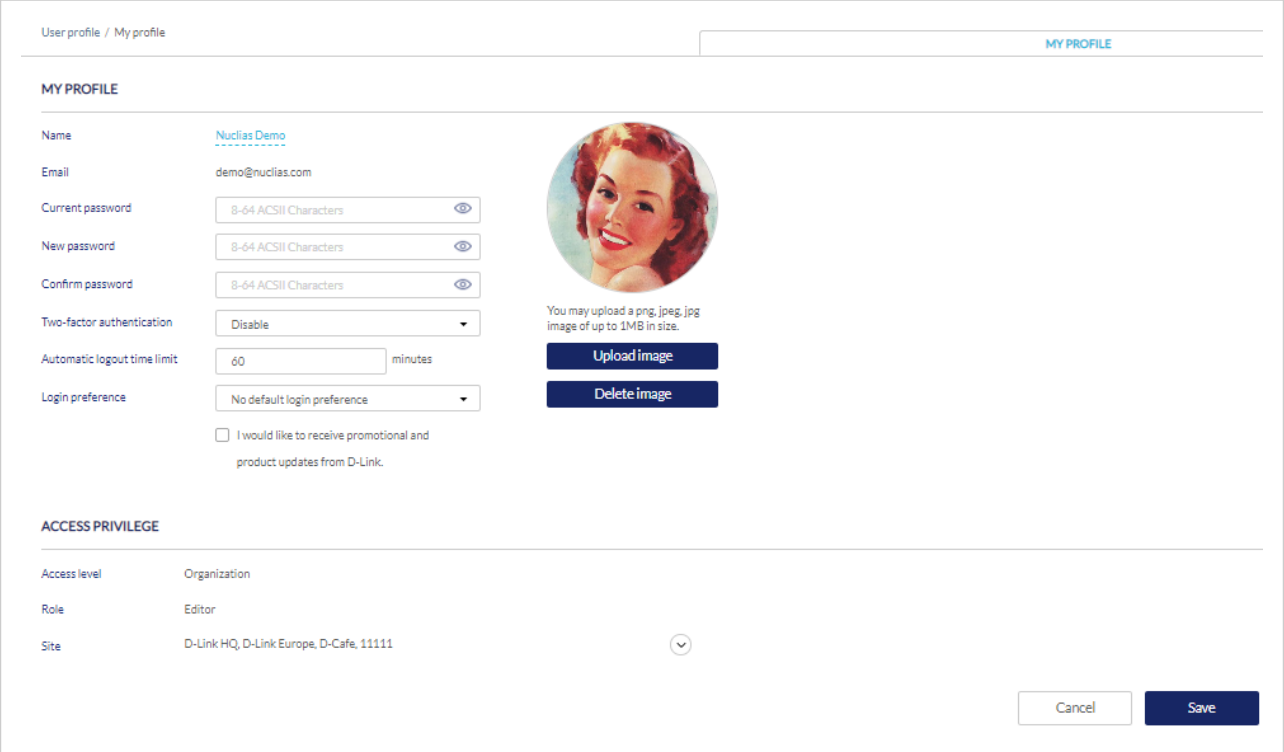
Account Menu

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 current 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 **Upload image** to add a profile image.
2. In the Upload Image window click **Browse** and navigate to the image you want to use.
3. Click **Upload**.

To delete a profile image, click **Delete image**.

d. **Email user information**

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

e. **Two-factor authentication**

Select to disable or use an additional authentication method from the drop down menu. If you select **Google Authenticator**, add your Nuclias account to your Google Authenticator by scanning the QR code below.

f. **Automatic logout time limit**

Enter the time in minutes that this user will be logged out when inactive.

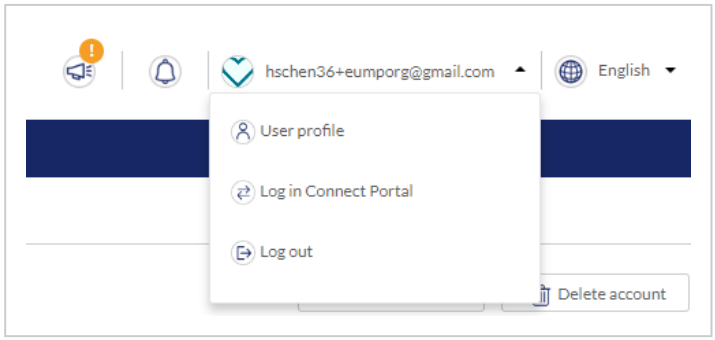
g. **Login preference**

Select none or use either **Cloud Portal** or **Connect Portal** as the default login portal.

4. Click **Save.**

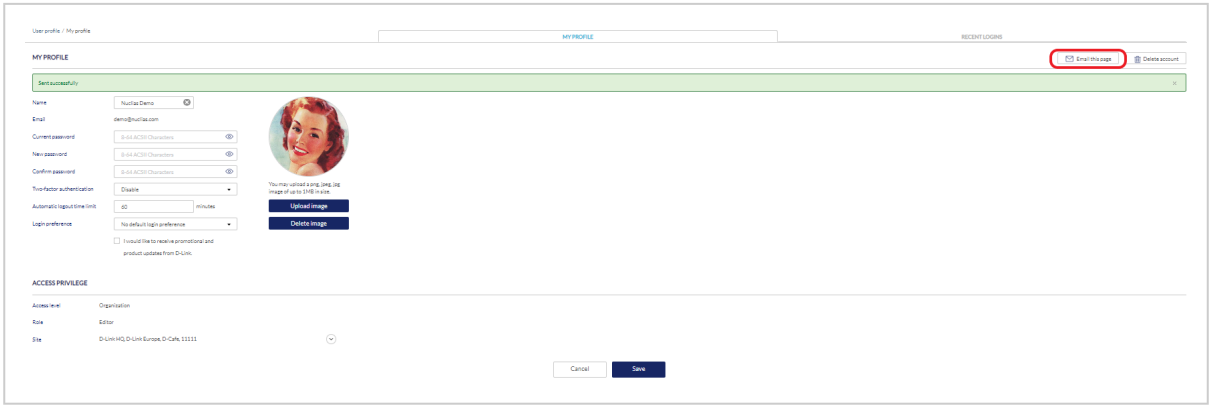
Sending A User Profile Snapshot by Email

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



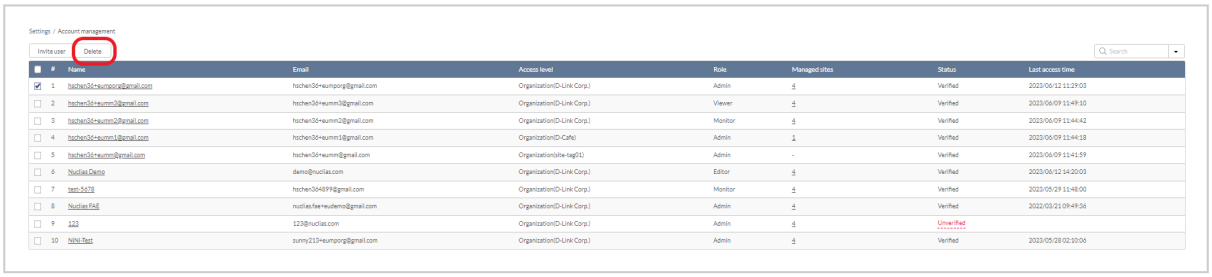
2. Select **User Profile**.
3. Click **Email this page**.
   Note: This will immediately send a snapshot of the user profile page to the email address

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 you 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.

Management Toolbar

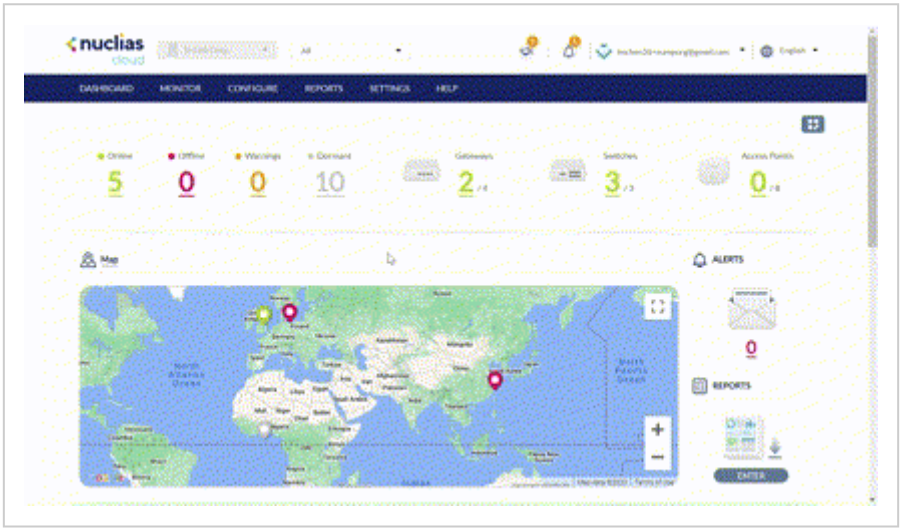
From the Management toolbar, you can access the various management features of the Nuclias Cloud platform, including Profiles and device management, device and network reports, organization and account management, firmware upgrade and alert settings, and the device and license inventory.

Dashboard	The Dashboard offers you a real time overview of the status of the network, including device utilization and performance statistics. The information on the Dashboard can be summarized as a report for download via the Reports section. Refer to the Dashboard section for more information.
Monitor	The Monitor section grants access to detailed device related information, including neighbor AP for wireless networks and associated client information, bandwidth usage and availability of the entire network, and event logs as well as the interactive map and floor plan tools. Refer to the Monitor section for more information.
Configure	The Configure section grants access to the main configuration section, including Profiles and individual device settings as well as settings for system-wide configuration such as Schedule policies and Splash pages. Refer to the Configure section for more information.
Reports	The Reports section grants access to detailed reports for changes on the platform, device activity, system alerts and a summary of registered devices with active licenses. Refer to the Reports section for more information.
Settings	The Settings section grants access to organization and user management, the device and license inventory, and firmware and certificate management as well as other settings pertinent to the global operation of the Nuclias Cloud such as

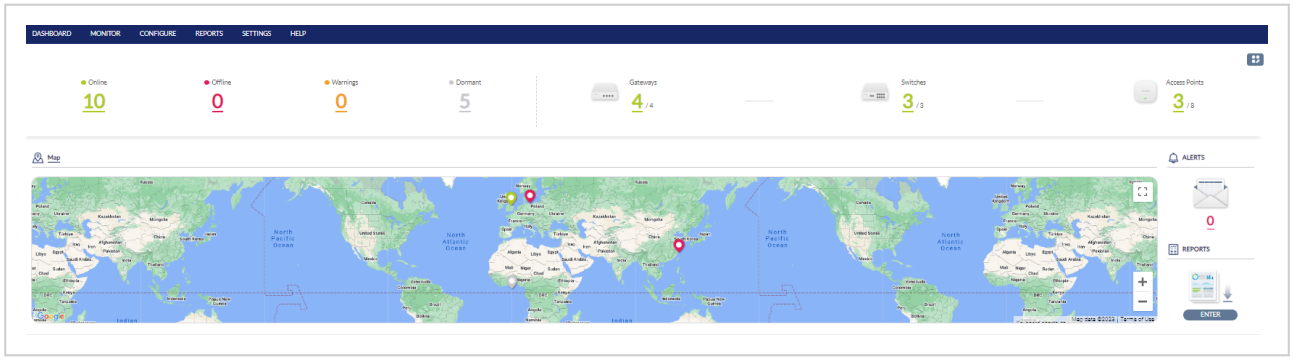
	SAML and Syslog. It also provides menu for quick import of devices and device registration. Refer to the Settings section for more information.
Help	The Help section offers you a platform to submit support tickets and provide feedback. Refer to the Help section for more information.

Dashboard

The Dashboard page is the default window that is displayed after logging in to the Nuclias Cloud Portal interface. It can also be reached by clicking the Dashboard tab in the tool bar. It provides an overview of the devices belonging to the selected site, connected clients of the devices, and device statistics for the selected site. You can also customize the dashboard by selecting the widgets and rearranging them to suit your needs.



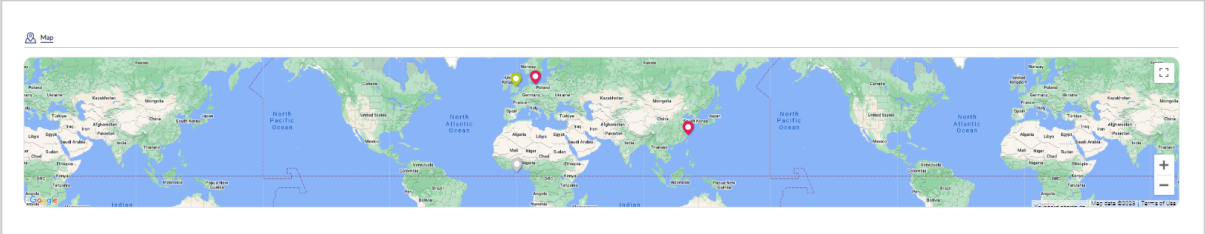
Customizing the Overview



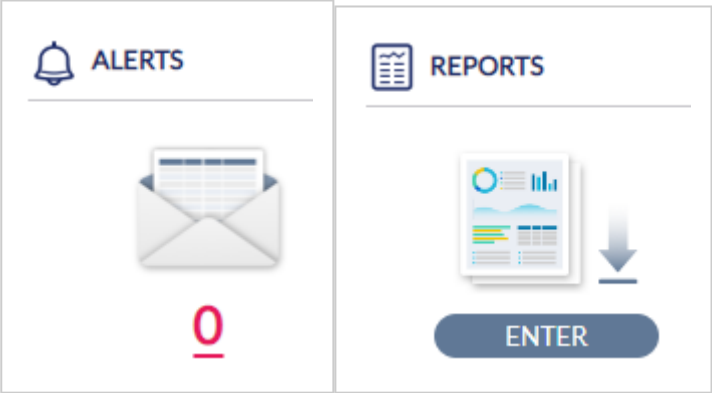


1. Navigate to the Dashboard page
2. Select a Site from the Site menu.
   Note: Selecting a Site will only show device and utilization information for the selected Site.

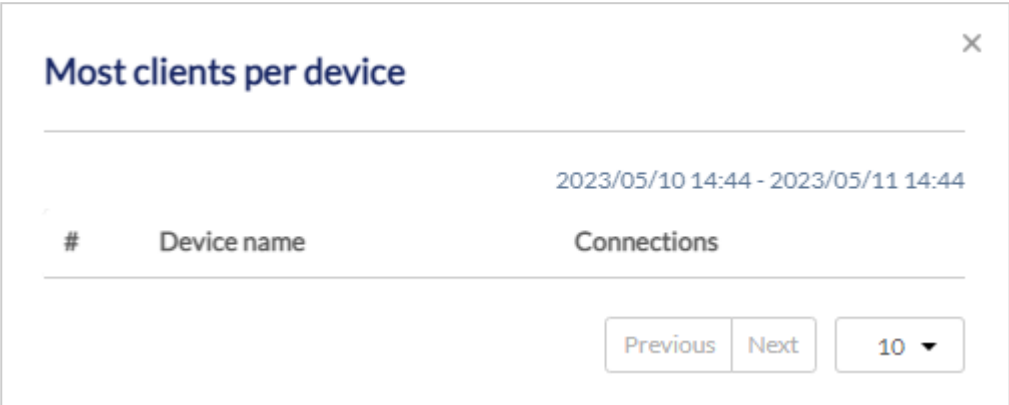
3. The top widget shows the the online/total (devices) for each product category.
4. The Map widget shows the site information as well as the device status. Click a site on the map to display such information.



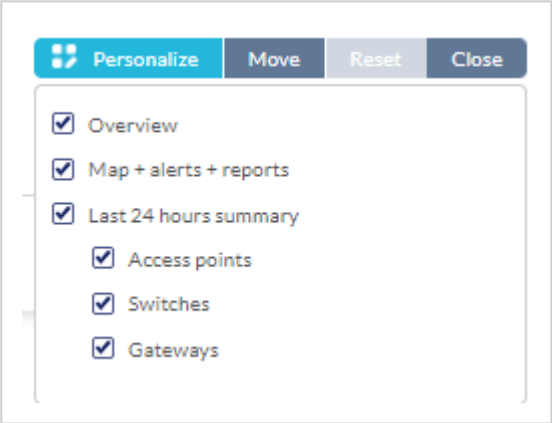
- The Alert and Report next to the map provides links to the Alerts and Summary Report page of the **Reports** menu.



- In the Last 24 Hours Summary section, click the title of the reports to obtain the ranks in different statistic category. For example, click **Most clients per device** to show the top devices with the most clients in the past 24 hours.



- Click the layout icon  at the top right to customize the statistic widgets to be displayed. For example, deselect the **Map** widget to hide geolocation information of sites and their devices. Click **Move** to arrange the widget blocks on the page. You can click **Reset** to reset the display and then click **Close** to close the layout customization control.


Personalize
Move
Reset
Close
Overview
Map + alerts + reports
Last 24 hours summary
Access points
Switches
Gateways

Monitor

Overview

From the Monitor menu, you can view detailed device monitoring reports and access the device availability and bandwidth usage information as well as map and floor plan windows .

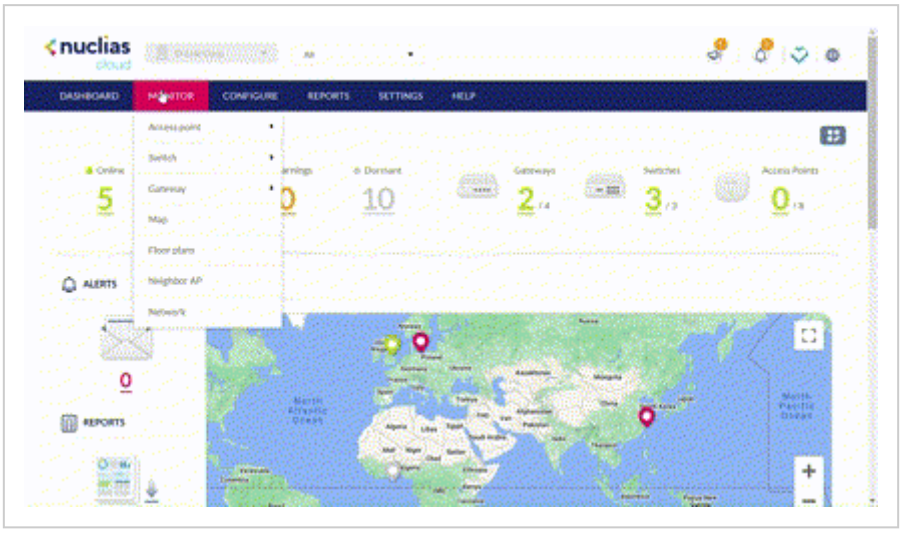
Access Point	The Access Point section provides detailed logs for AP devices, connected clients, and events. Refer to the Access Point section for more information.
Switch	The Switch section provides detailed logs for switch devices, connected clients, and events. Refer to the Switch section for more information.
Gateway	The Gateway section provides detailed logs for gateway devices, connected clients, and events. Refer to the Gateway section for more information.
Map	The Map section provides you with an interactive map that offers a geographical overview of the organization's Sites. Refer to the Map section for more information.
Floor Plans	The Floor Plans section allows you to create, edit, manage, and delete floor plans. Refer to the Floor Plans section for more information.
Neighbor AP	The Neighbor AP section provides information about APs in the neighborhood to help detect rogue devices and solve signal issues.

	Refer to the Neighbor AP section for more information.
Network	The Network section provides the availability of the devices and their client information, the bandwidth usage, and channel utilization. Refer to the Network section for more information.

Monitor - Access Point

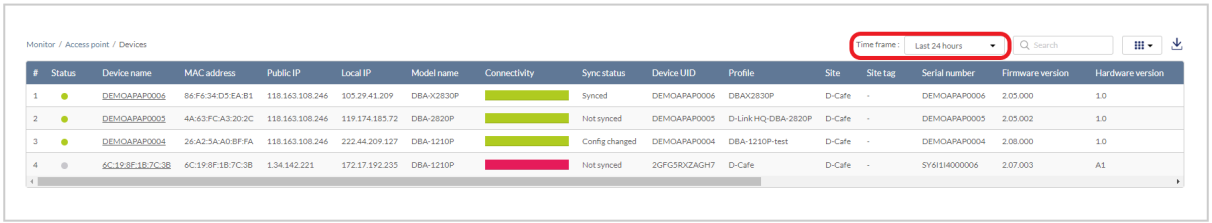
Devices

From the Devices window, you can view the AP devices with detailed information such as IP addresses, model name, firmware version, and license information .

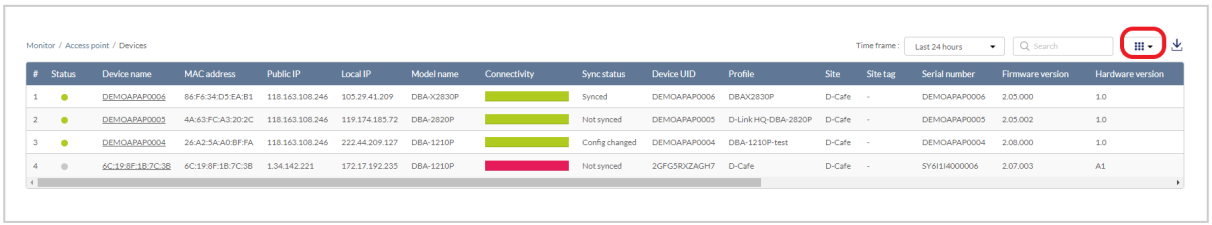


Customizing the Device Monitor Overview

1. Navigate to **Monitor > Access Point > Devices**.
2. Select a time frame from the time frame drop-down menu to set the duration for connectivity information.



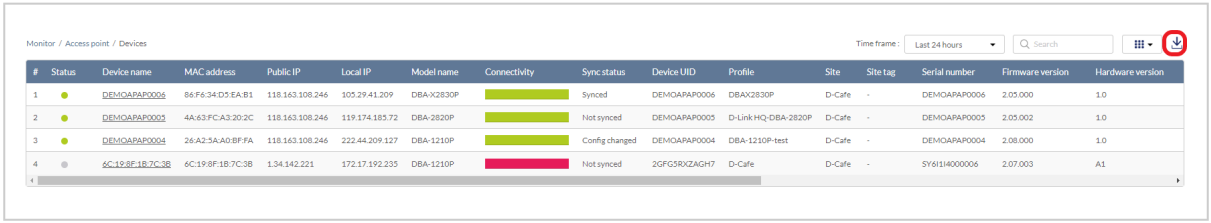
3. Click the filter parameter icon to filter the table properties.



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 > Devices**.
2. From the device list, click the **Download** icon in the top-right.

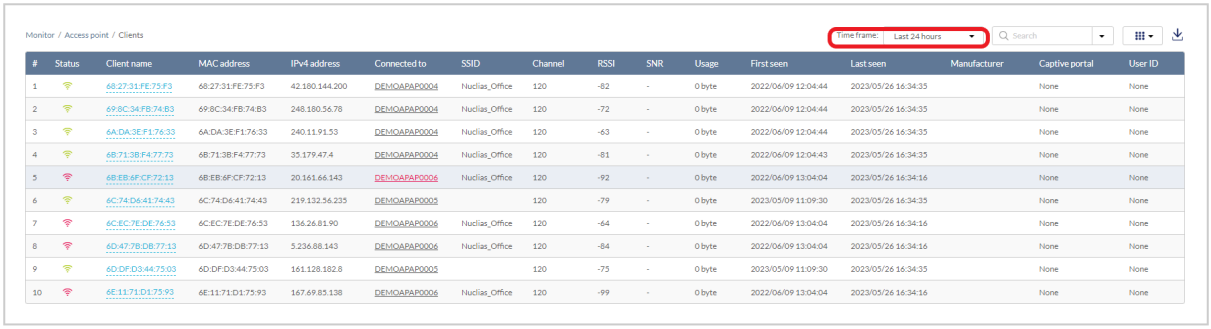


Clients

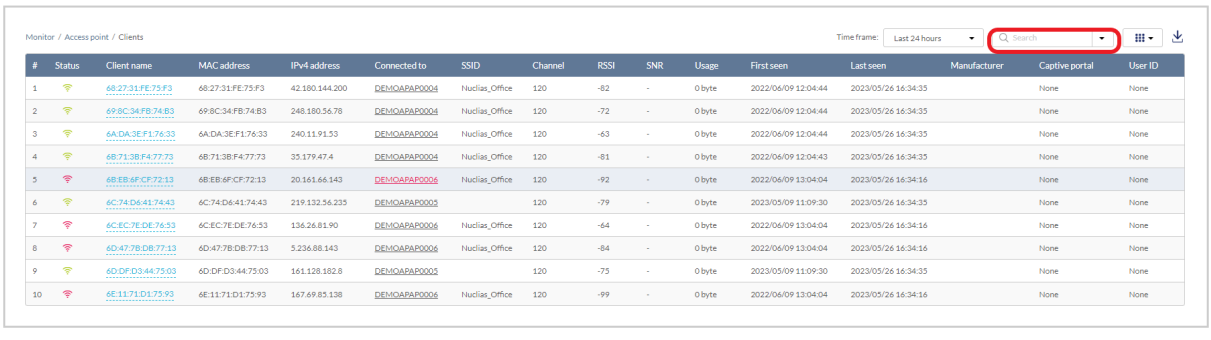
From the Clients window, you can consult a detailed overview of all currently connected clients with additional information such as SSID, channel, and signal strength information.

Customizing the Client Monitor Overview

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

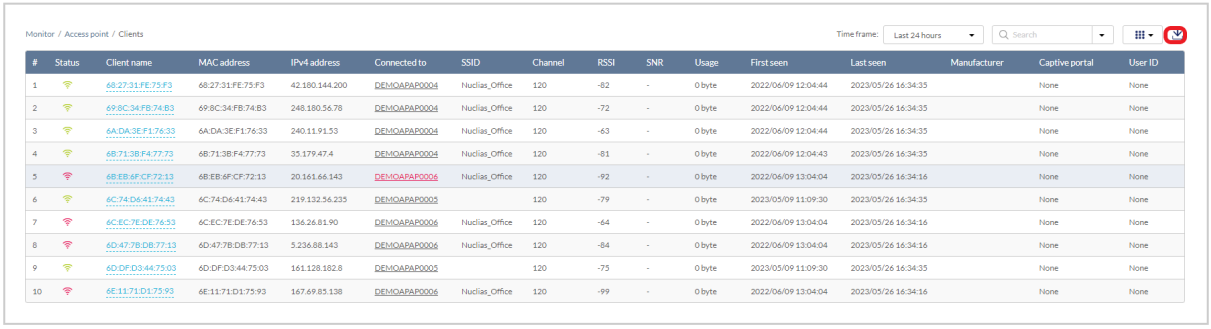


3. Select the criteria from the search drop-down menu to filter the list. You can also enter a keyword to search for all fields.



Downloading Client Monitoring Logs

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



#	Status	Client name	MAC address	IPv4 address	Connected to	SSID	Channel	RSSI	SNR	Usage	First seen	Last seen	Manufacturer	Captive portal	User ID
1		68:27:31:FE:75:F3	68:27:31:FE:75:F3	42.160.144.200	DEMOAPAP0004	Nuclias_Office	120	-82	-	0 byte	2022/06/09 12:04:44	2023/05/26 16:34:35		None	None
2		69:8C:34:FB:74:B3	69:8C:34:FB:74:B3	248.180.56.78	DEMOAPAP0004	Nuclias_Office	120	-72	-	0 byte	2022/06/09 12:04:44	2023/05/26 16:34:35		None	None
3		6A:DA:3E:F1:76:33	6A:DA:3E:F1:76:33	240.11.91.53	DEMOAPAP0004	Nuclias_Office	120	-63	-	0 byte	2022/06/09 12:04:44	2023/05/26 16:34:35		None	None
4		6B:71:3B:F4:77:73	6B:71:3B:F4:77:73	35.179.47.4	DEMOAPAP0004	Nuclias_Office	120	-81	-	0 byte	2022/06/09 12:04:43	2023/05/26 16:34:35		None	None
5		6B:EB:6F:CF:72:13	6B:EB:6F:CF:72:13	20.161.66.143	DEMOAPAP0006	Nuclias_Office	120	-92	-	0 byte	2022/06/09 13:04:04	2023/05/26 16:34:16		None	None
6		6C:74:D6:41:74:43	6C:74:D6:41:74:43	219.132.56.235	DEMOAPAP0005		120	-79	-	0 byte	2023/05/09 11:09:30	2023/05/26 16:34:35		None	None
7		6C:EC:7E:DE:76:53	6C:EC:7E:DE:76:53	136.26.81.90	DEMOAPAP0006	Nuclias_Office	120	-64	-	0 byte	2022/06/09 13:04:04	2023/05/26 16:34:16		None	None
8		6D:47:7B:DB:77:13	6D:47:7B:DB:77:13	5.236.88.143	DEMOAPAP0006	Nuclias_Office	120	-84	-	0 byte	2022/06/09 13:04:04	2023/05/26 16:34:16		None	None
9		6D:DF:D3:44:75:03	6D:DF:D3:44:75:03	161.128.182.8	DEMOAPAP0005		120	-75	-	0 byte	2023/05/09 11:09:30	2023/05/26 16:34:35		None	None
10		6E:11:71:D1:75:93	6E:11:71:D1:75:93	167.69.85.138	DEMOAPAP0006	Nuclias_Office	120	-99	-	0 byte	2022/06/09 13:04:04	2023/05/26 16:34:16		None	None

Event Log

From the Event Log window, you can consult a detailed log of events occurring on the network. You can define event filter parameters, including event type and time period.

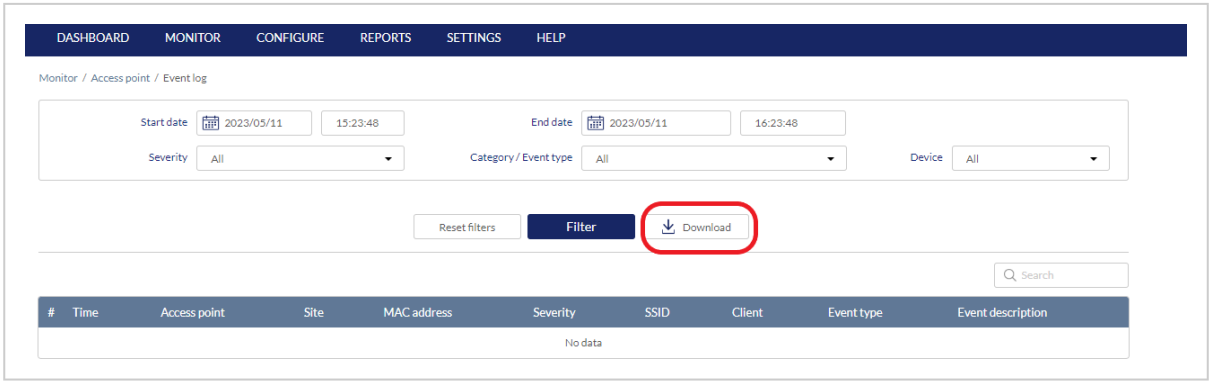
Filtering Event Log Parameters

1. Navigate to **Monitor > Access Point > Event Log**.
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. The severity has 3 states: Critical- Indicates major configuration changes or offline/online status changes, Warning - Indicates system reboot events following scheduled firmware upgrade, Information- Indicates device clients association and disassociation events.
5. Click the Event type drop-down menu and select the event types to display.
6. Click the Device drop-down menu and select the desired device to filter the results.
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 > Access Point > Event Log**.

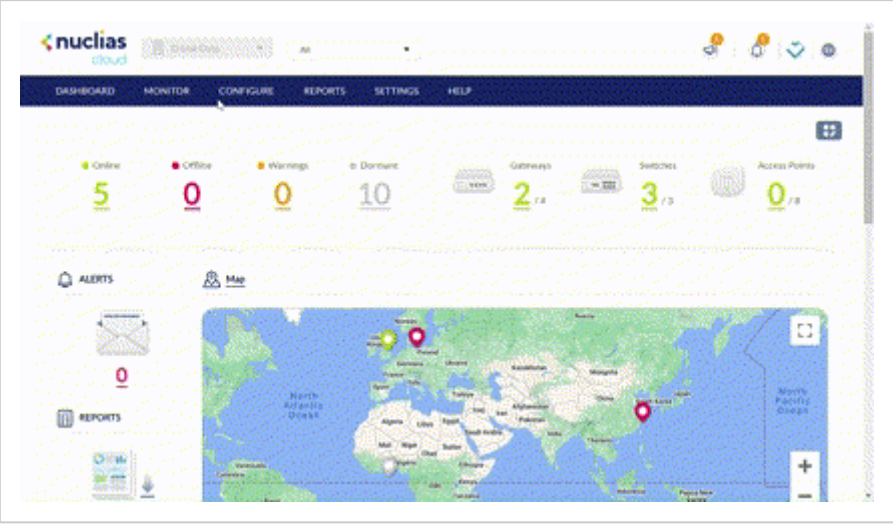
2. From the event log list, click **Download** icon in the center.



Monitor - Switch

Devices

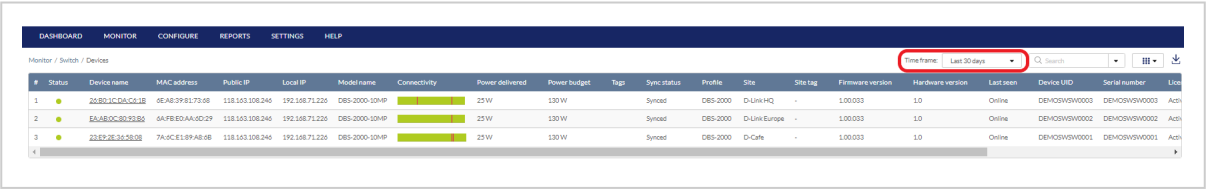
From the Devices window, you can consult a detailed log of events occurring on the network. You can also filter events using specific event filter parameters, including event type and time period.



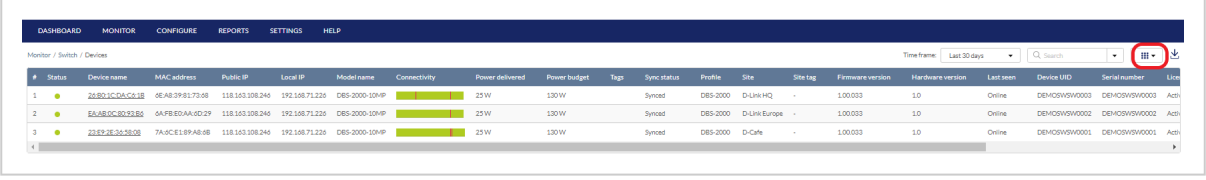
The Device Monitor

Customizing the Device Monitor Overview

1. Navigate to **Monitor > Switch > Devices**.
2. Select a time frame from the drop-down menu to set the duration for connectivity information.



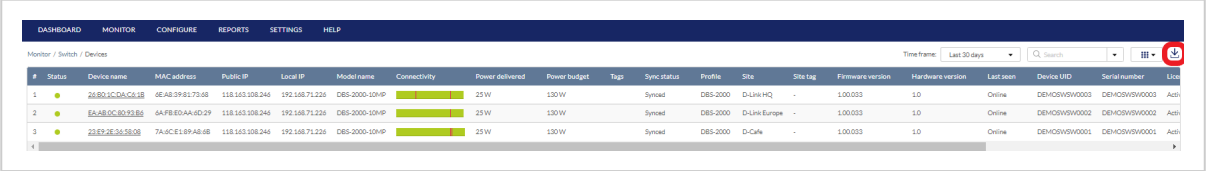
3. Click the filter parameter icon.



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 > Devices**.
2. From the device list, click the **Download** icon in the top-right.



Device Basic Settings

Changing the Device Site and Profile

1. Navigate to **Monitor > Switch > Devices** and select a device from the list.
2. Select the **Basic** tab at the top.
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 > Devices** and select a device from the list.
2. Select the **Basic** tab at the top.
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's 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 > Devices** and select a device from the list.
2. Select the **Basic** tab at the top.
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.
Management VLAN	Select a VLAN to be the management VLAN. This segments management traffic. Make sure that at least one member port belongs to the management VLAN to allow access to the management functions of the switch.
Subnet Mask	Enter the Subnet Mask.
Gateway	Enter the default gateway address.
DNS #1	Enter a primary DNS address.
DNS #2	[Optional] Enter a secondary DNS server address.
DNS #3	[Optional] Enter a tertiary DNS server address.
Proxy	[Optional] Enable or disable the use of DNS proxy. If enabled, enter the proxy host's IP address or domain name and port number (1-65535).

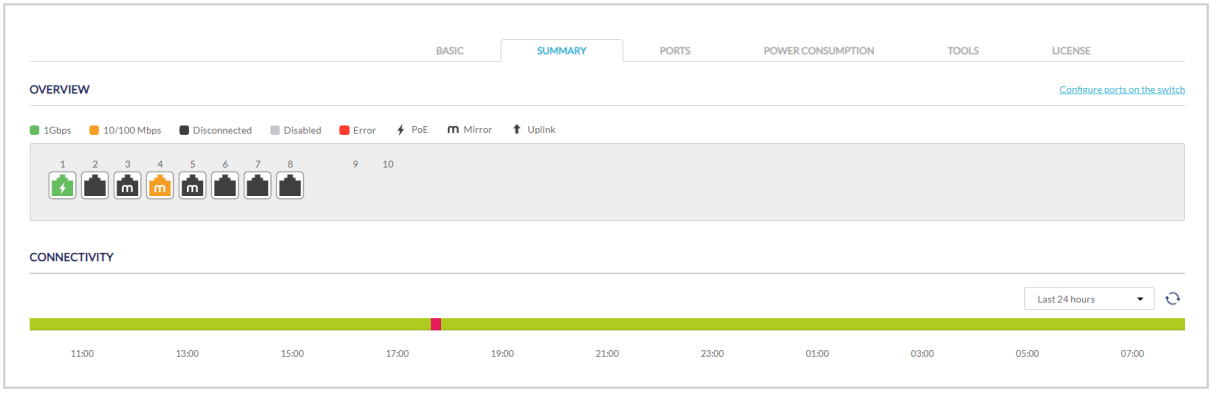
6. Click **Apply**.

The Performance Summary

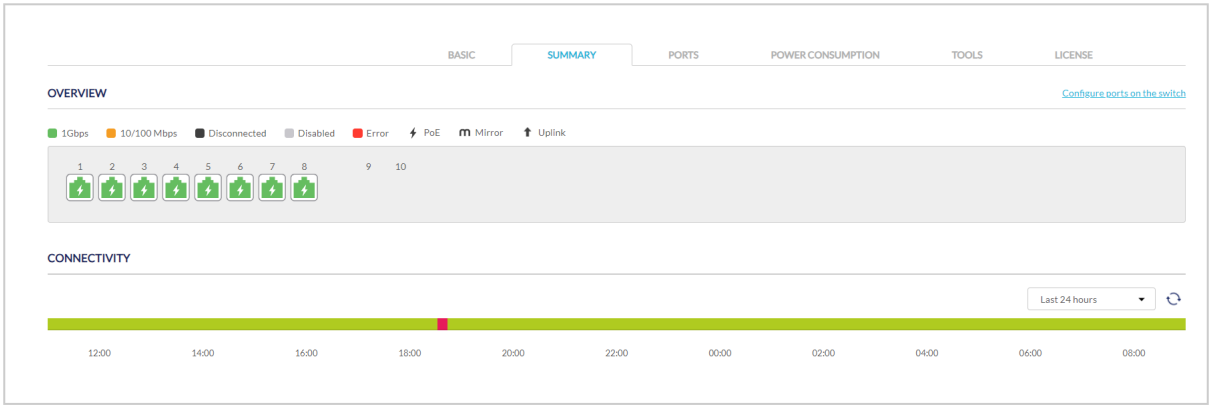
Viewing and Customizing the Switch Performance Summary

1. Navigate to **Monitor > Switch > Devices** and select a device from the list.
2. Select the **Summary** tab at the top.
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.



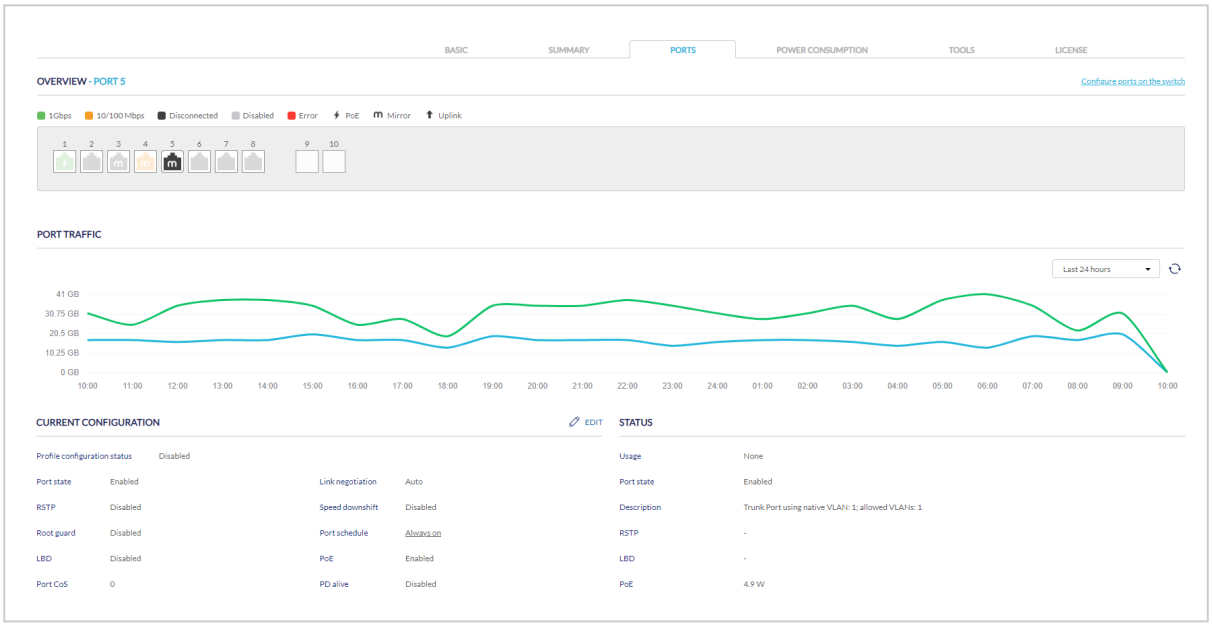
5. [Optional] Click **Configure ports on the switch** to go to the switch port configuration window. Refer to the Switch Ports section for more information.



Ports Status

Viewing and Customizing the Switch Port Status Overview

1. Navigate to **Monitor > Switch > Devices** and select a device from the list.
2. Select the **Ports** tab at the top.



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. **Note**: 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. Note: LBD cannot be used in conjunction with RSTP.
Port CoS	Select a value for Cos value (0-7).
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 if the Trunk type is selected.
Allowed VLANs	Enter the IDs of the VLANs that can route traffic through this port if the Trunk type is selected. Enter **All** to allow all traffic from all VLANs to pass through this port.
Access VLAN	Enter the ID of the VLAN the port belongs to if the Access type is selected.
Access Policy	Select the Access Policy for this port if the Access type is selected. The options include Disabled, MAC Whitelist, Port Security Delete-on-Time Mode, and Port Security Permanent Mode. MAC Whitelist: Allows only the specified MAC addresses in the Static Whitelisted MACs. Port Security Delete-on-Time Mode: All learned MAC addresses have a limited lifetime and will be erased when the lifetime is reached. Port Security Permanent Mode: Allows the MAC addresses learned through this port. The number of allowed addresses is set by Dynamic Whitelist Size Limit. When the number of Dynamic Whitelisted MACs reaches this limit, new devices will be denied access to this port.

Static Whitelisted MACs	Enter the MAC addresses that can access this port to restrict access to this port to devices with specific MAC addresses. If entering multiple MAC addresses, enter only one address per line.
Dynamic Whitelist Size Limit	Enter the maximum number of allowed MAC addresses that the device should learn dynamically for the Port Security Delete-on-time Mode or Port Security Permanent Mode.
Dynamic Whitelisted MACs	Display the learned MAC addresses for the Port Security Delete-on-time mode and Port Security Permanent Mode.
Tags	Enter a descriptive tag for the port. Multiple tags can be entered. If multiple ports are selected, 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.
Link (SFP)	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.
Speed Downshift	Enables/disables automatic speed downshift on the supported interface when the designated maximum speed cannot be established.
PoE	Choose to enable or disable Power over Ethernet (PoE) functionality on this port. **Note**: The PoE setting will only apply to ports that support Power over Ethernet.
PD Alive	Enable or disable the automatic detection of the Powered Devices status.
PD IP Address	Enter the IP address of the Powered Device.

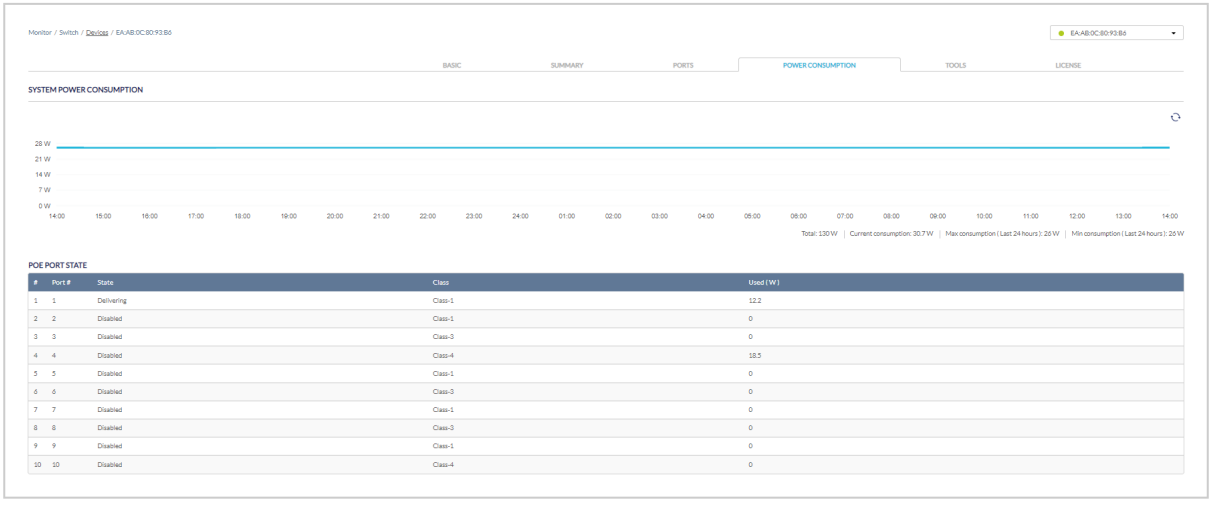
Port Schedule	Choose a pre-configured schedule policy. Go to **Configure > Schedule policies** to access the configured schedules.
Traffic Segmentation	Enable or disable traffic segmentation on this port to further restrict traffic flow in your network. If enabled, select the forward ports.
Forward Ports	Select the forward ports if traffic segmentation is enabled.
Flow Control	Enable or disable the flow control on the port to regulate the data transfer rate between two devices.

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 different packet types (e.g. broadcast , CRC error, or collision) for the selected time period.

Power Consumption

Viewing and Customizing the Switch Power Consumption Overview

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



Tools

Performing a Device Ping Test

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

Performing a MAC Forwarding Table Test

1. Navigate to **Monitor > Switch > Devices** 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 > Devices** 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. Separate multiple port numbers with "," and use "-" for port range, for example, 1,5,7-10.
   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 > Devices** 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 port cycle. Separate multiple port numbers with "," and use "-" for port range, for example, 1,5,7-10.
4. Click **Test**.

Performing a Locate Device Test

1. Navigate to **Monitor > Switch > Devices** 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 > Devices** 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**.

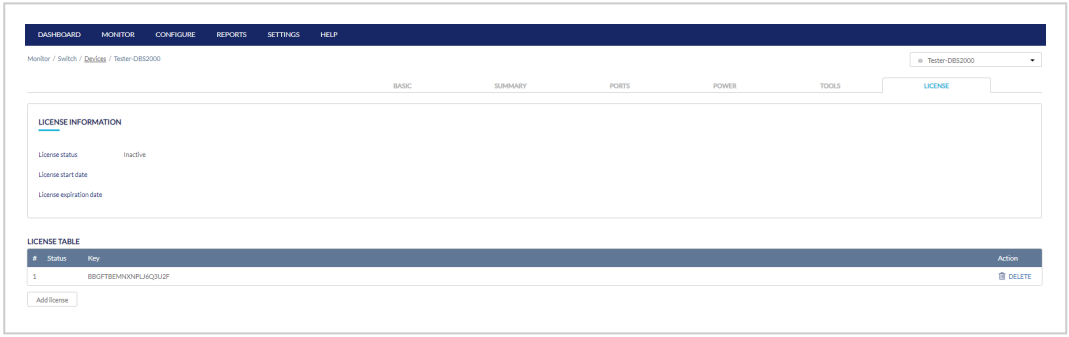
Adding a License Key to a Device

1. Navigate to **Monitor > Switch > Devices** 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 > Devices** 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 reclassify it as unused in the license management inventory until it is reassigned to another device.

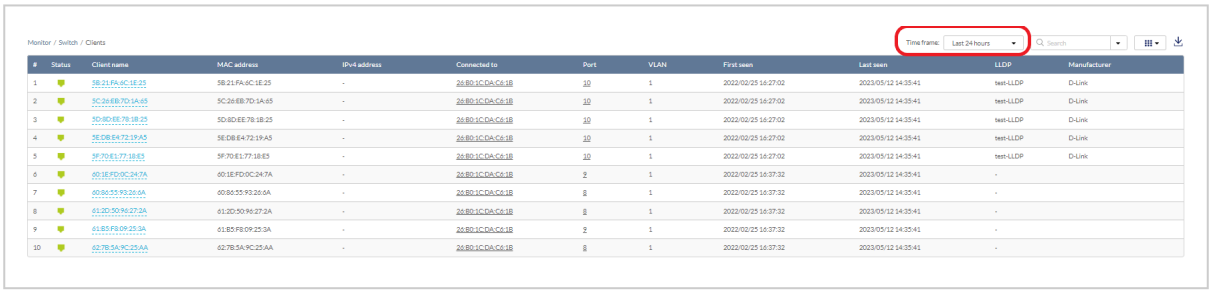


Clients

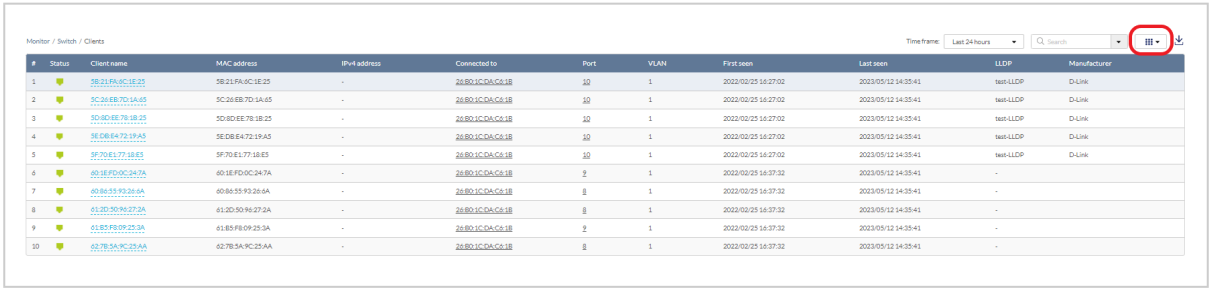
From the Clients window, you can consult a detailed overview of all currently connected devices with additional information including connected ports, VLAN, and other information such as MAC addresses and LLDP setting.

Customizing the Client Monitor Overview

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



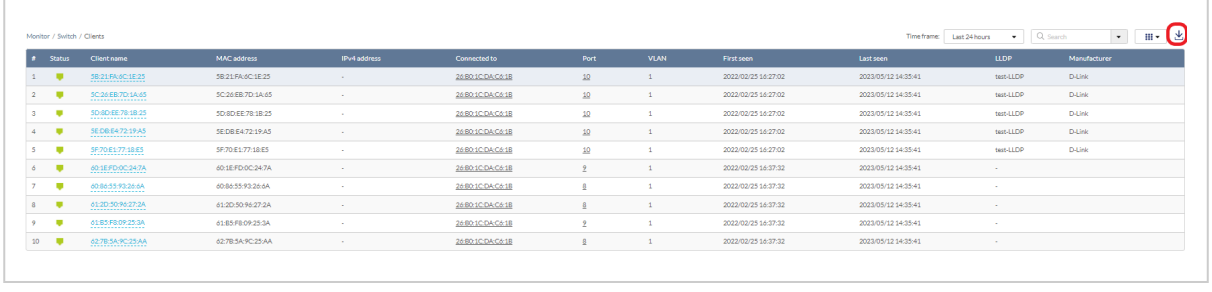
3. Click the parameter filter icon.



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 Log

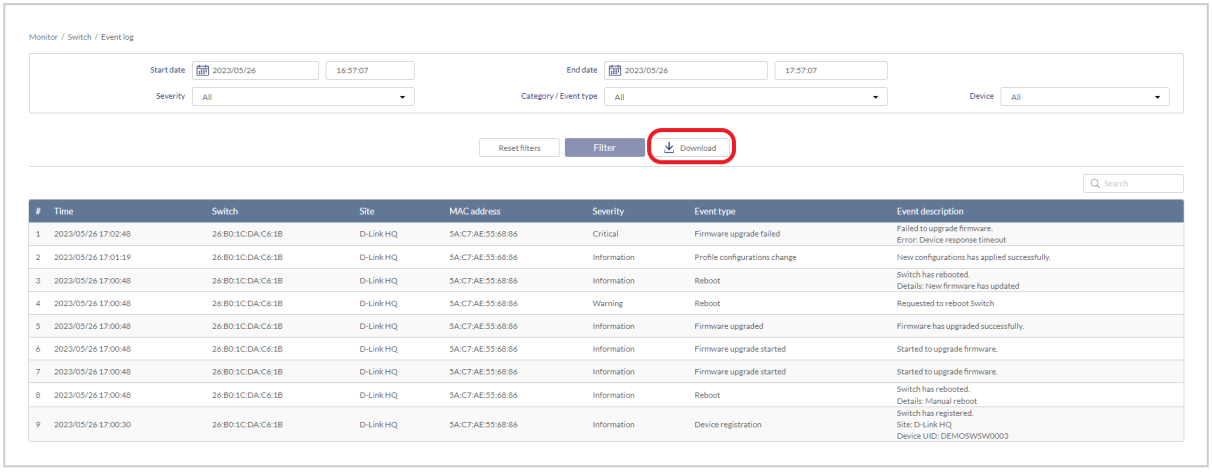
From the Event Logs window, you can consult a detailed log of events occurring on the network. You can define event filter parameters, including event type and time period.

Filtering Event Log Parameters

1. Navigate to **Monitor > Switch > Event Log**.
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. The severity is classified in 3 states: Critical- Indicates major configuration changes or offline/online status changes, Warning - Indicates system reboot events following scheduled firmware upgrade, Information- Indicates device clients association and disassociation events.
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 to filter the results.
   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

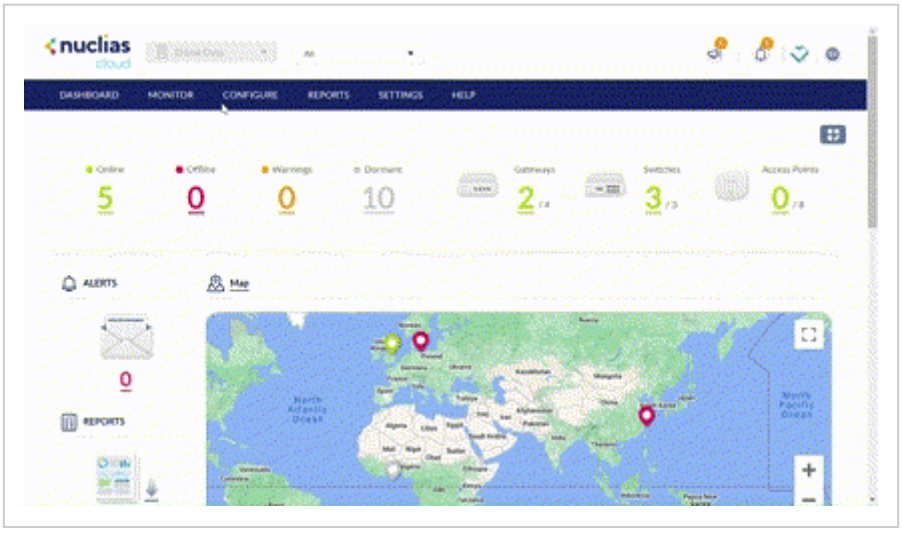
1. Navigate to **Monitor > Switch > Event Log**.
2. From the event log list, click **Download**.



Devices

Devices

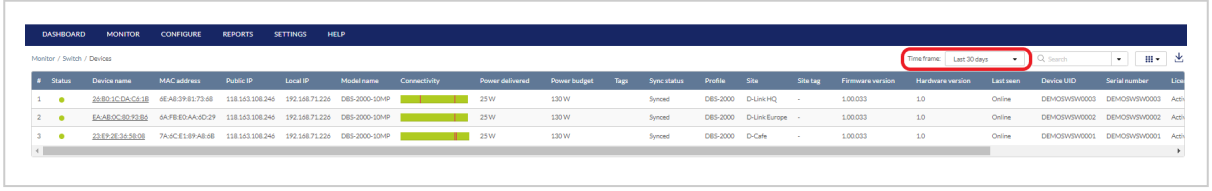
From the Devices window, you can consult a detailed log of events occurring on the network. You can also filter events using specific event filter parameters, including event type and time period.



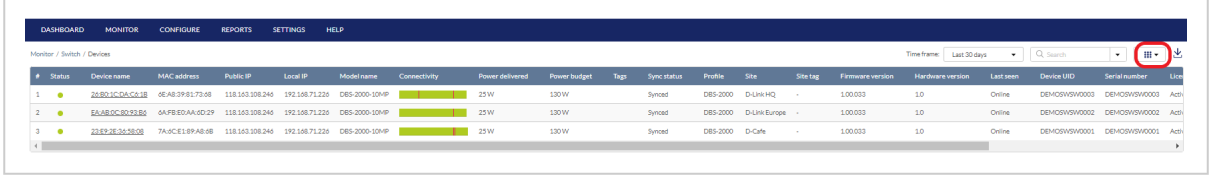
The Device Monitor

Customizing the Device Monitor Overview

1. Navigate to **Monitor > Switch > Devices**.
2. Select a time frame from the drop-down menu to set the duration for connectivity information.



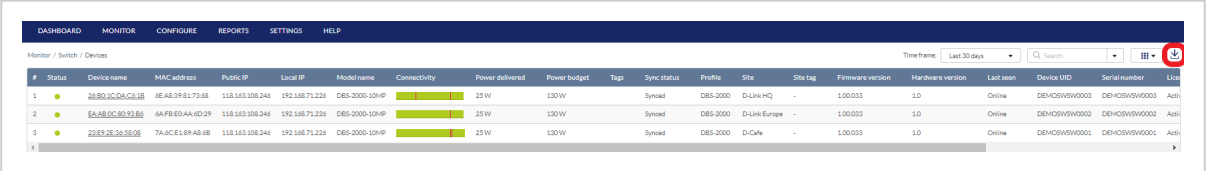
3. Click the filter parameter icon.



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 > Devices**.
2. From the device list, click the **Download** icon in the top-right.



Device Basic Settings

Changing the Device Site and Profile

1. Navigate to **Monitor > Switch > Devices** and select a device from the list.
2. Select the **Basic** tab at the top.
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 > Devices** and select a device from the list.
2. Select the **Basic** tab at the top.
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's 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 > Devices** and select a device from the list.
2. Select the **Basic** tab at the top.
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.
Management VLAN	Select a VLAN to be the management VLAN. This segments management traffic. Make sure that at least one member port

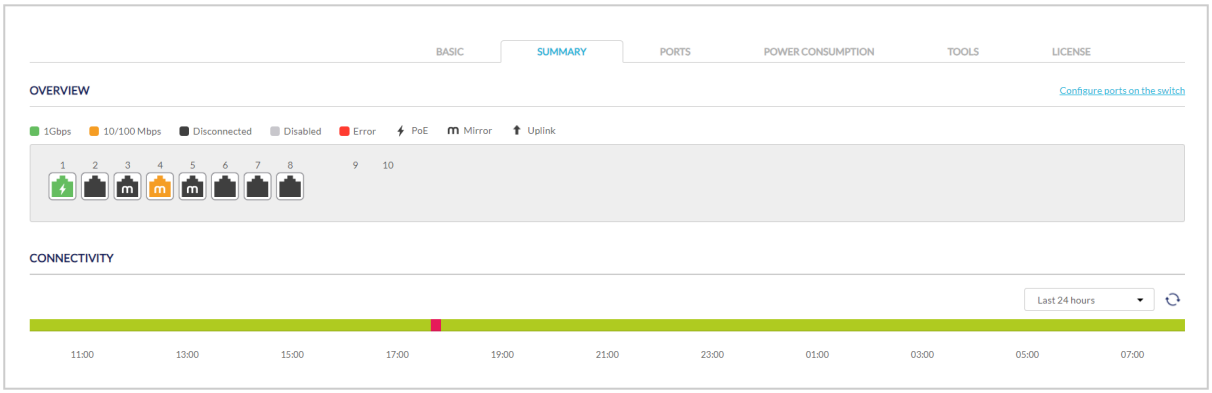
	belongs to the management VLAN to allow access to the management functions of the switch.
Subnet Mask	Enter the Subnet Mask.
Gateway	Enter the default gateway address.
DNS #1	Enter a primary DNS address.
DNS #2	[Optional] Enter a secondary DNS server address.
DNS #3	[Optional] Enter a tertiary DNS server address.
Proxy	[Optional] Enable or disable the use of DNS proxy. If enabled, enter the proxy host's IP address or domain name and port number (1-65535).

6. Click **Apply**.

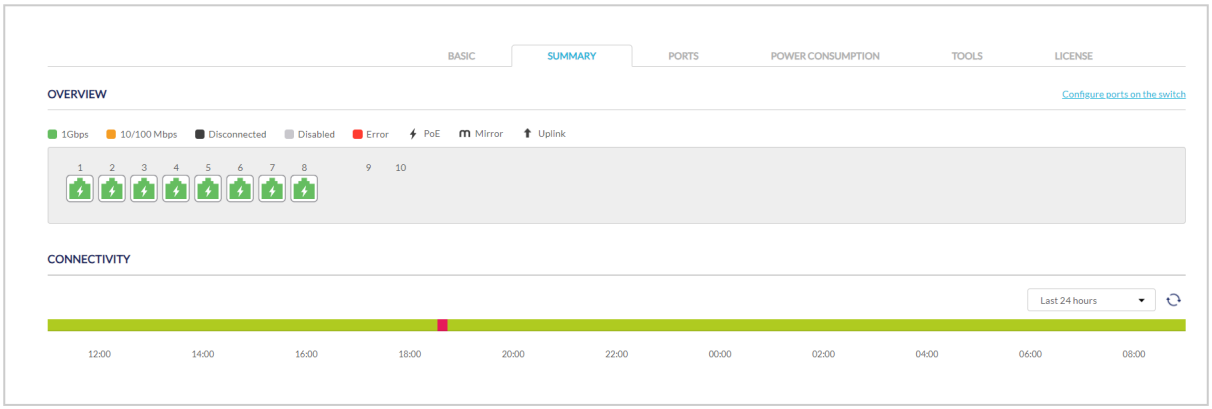
The Performance Summary

Viewing and Customizing the Switch Performance Summary

1. Navigate to **Monitor > Switch > Devices** and select a device from the list.
2. Select the **Summary** tab at the top.
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.



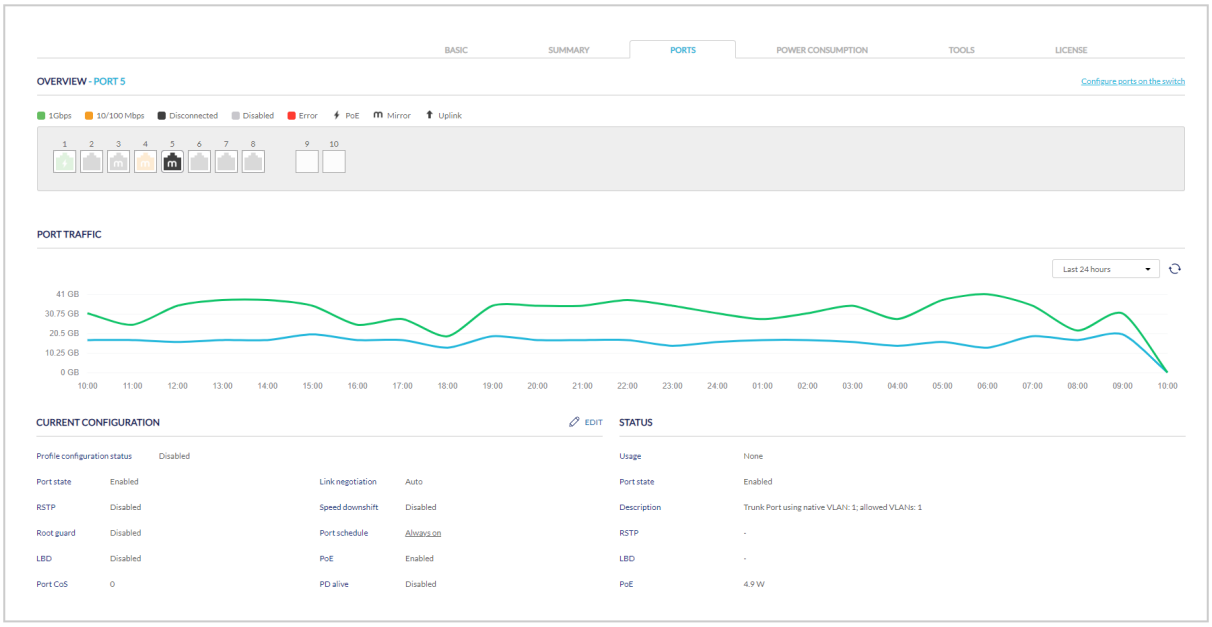
5. [Optional] Click **Configure ports on the switch** to go to the switch port configuration window. Refer to the Switch Ports section for more information.



Ports Status

Viewing and Customizing the Switch Port Status Overview

1. Navigate to **Monitor > Switch > Devices** and select a device from the list.
2. Select the **Ports** tab at the top.



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. **Note**: 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. Note: LBD cannot be used in conjunction with RSTP.
Port CoS	Select a value for Cos value (0-7).
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 if the Trunk type is selected.
Allowed VLANs	Enter the IDs of the VLANs that can route traffic through this port if the Trunk type is selected. Enter **All** to allow all traffic from all VLANs to pass through this port.
Access VLAN	Enter the ID of the VLAN the port belongs to if the Access type is selected.
Access Policy	Select the Access Policy for this port if the Access type is selected. The options include Disabled, MAC Whitelist, Port Security Delete-on-Time Mode, and Port Security Permanent Mode. MAC Whitelist: Allows only the specified MAC addresses in the Static Whitelisted MACs. Port Security Delete-on-Time Mode: All learned MAC addresses have a limited lifetime and will be erased when the lifetime is reached. Port Security Permanent Mode: Allows the MAC addresses learned through this port. The number of allowed addresses is set by Dynamic Whitelist Size Limit. When the number of Dynamic Whitelisted MACs reaches this limit, new devices will be denied access to this port.

Static Whitelisted MACs	Enter the MAC addresses that can access this port to restrict access to this port to devices with specific MAC addresses. If entering multiple MAC addresses, enter only one address per line.
Dynamic Whitelist Size Limit	Enter the maximum number of allowed MAC addresses that the device should learn dynamically for the Port Security Delete-on-time Mode or Port Security Permanent Mode.
Dynamic Whitelisted MACs	Display the learned MAC addresses for the Port Security Delete-on-time mode and Port Security Permanent Mode.
Tags	Enter a descriptive tag for the port. Multiple tags can be entered. If multiple ports are selected, 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.
Link (SFP)	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.
Speed Downshift	Enables/disables automatic speed downshift on the supported interface when the designated maximum speed cannot be established.
PoE	Choose to enable or disable Power over Ethernet (PoE) functionality on this port. **Note**: The PoE setting will only apply to ports that support Power over Ethernet.
PD Alive	Enable or disable the automatic detection of the Powered Devices status.
PD IP Address	Enter the IP address of the Powered Device.

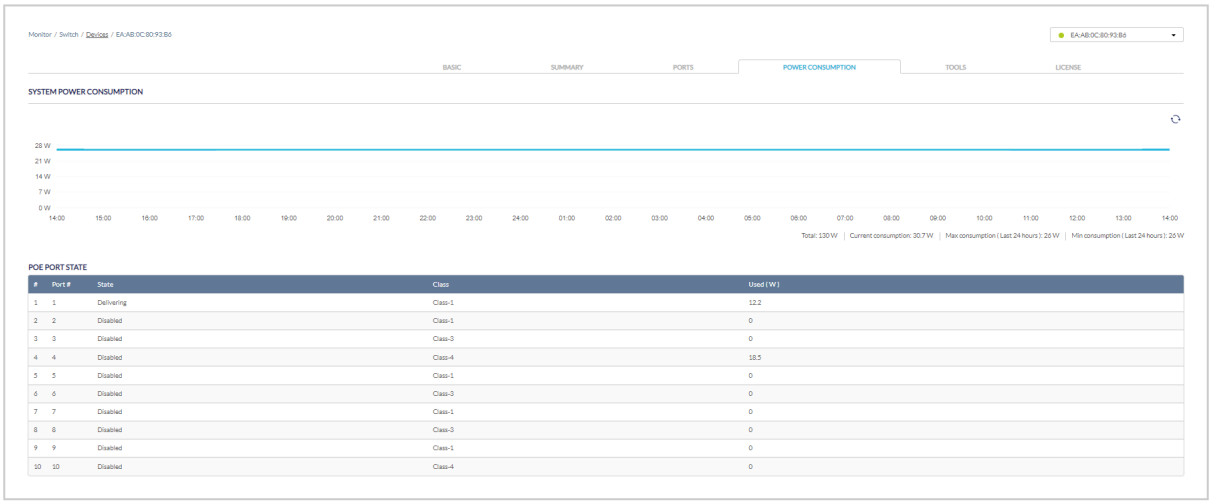
Port Schedule	Choose a pre-configured schedule policy. Go to **Configure > Schedule policies** to access the configured schedules.
Traffic Segmentation	Enable or disable traffic segmentation on this port to further restrict traffic flow in your network. If enabled, select the forward ports.
Forward Ports	Select the forward ports if traffic segmentation is enabled.
Flow Control	Enable or disable the flow control on the port to regulate the data transfer rate between two devices.

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 different packet types (e.g. broadcast , CRC error, or collision) for the selected time period.

Power Consumption

Viewing and Customizing the Switch Power Consumption Overview

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



Tools

Performing a Device Ping Test

1. Navigate to **Monitor > Switch > Devices** and select a device from the list.

2. Select the **Tools** tab in the top-right of the screen.
3. In the IP address/FQDN field in the Ping section, enter a valid IP address or FQDN.
4. Click **Ping**.

Performing a MAC Forwarding Table Test

1. Navigate to **Monitor > Switch > Devices** 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 > Devices** 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. Separate multiple port numbers with "," and use "-" for port range, for example, 1,5,7-10.
   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 > Devices** 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 port cycle. Separate multiple port numbers with "," and use "-" for port range, for example, 1,5,7-10.
4. Click **Test**.

Performing a Locate Device Test

1. Navigate to **Monitor > Switch > Devices** 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 > Devices** 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

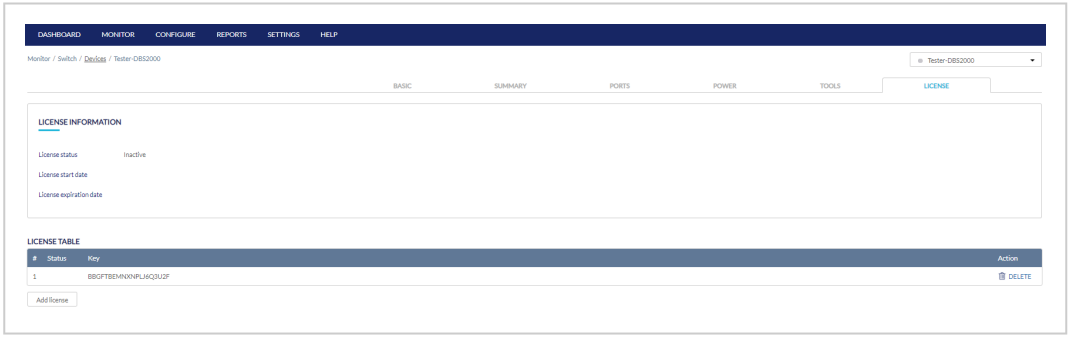
1. Navigate to **Monitor > Switch > Devices** and select a device from the list.
2. Select the **License** tab in the top-right of the screen.
3. In the License Table section, click **Add License**.
4. Enter a valid license key.
5. Click **Save**.



Deleting a License Key From a Device

1. Navigate to **Monitor > Switch > Devices** 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 reclassify it as unused in the license management inventory until it is reassigned to another device.

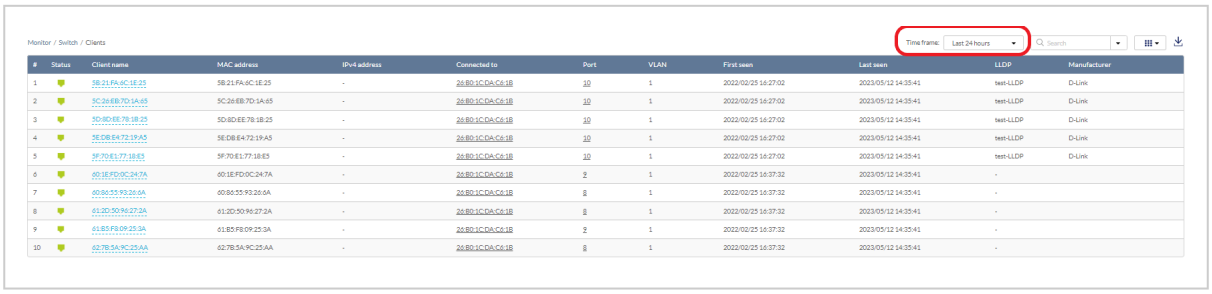


Clients

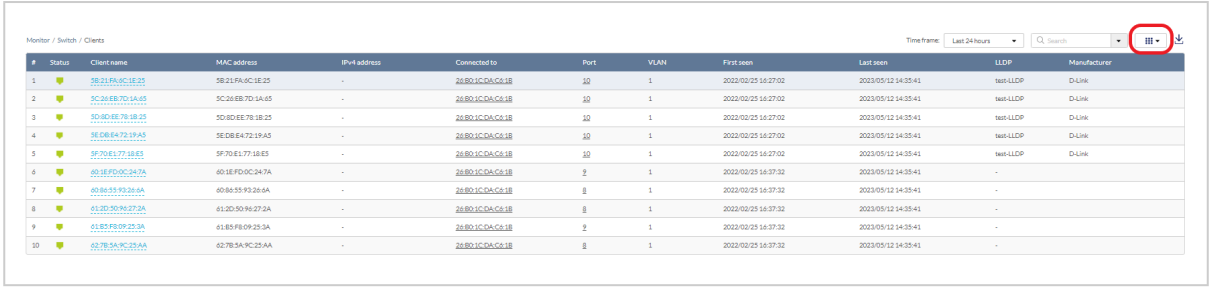
From the Clients window, you can consult a detailed overview of all currently connected devices with additional information including connected ports, VLAN, and other information such as MAC addresses and LLDP setting.

Customizing the Client Monitor Overview

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



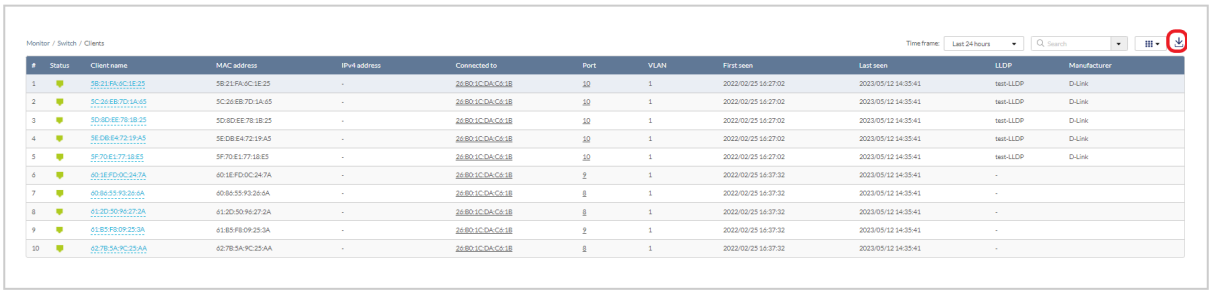
3. Click the parameter filter icon.



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 Log

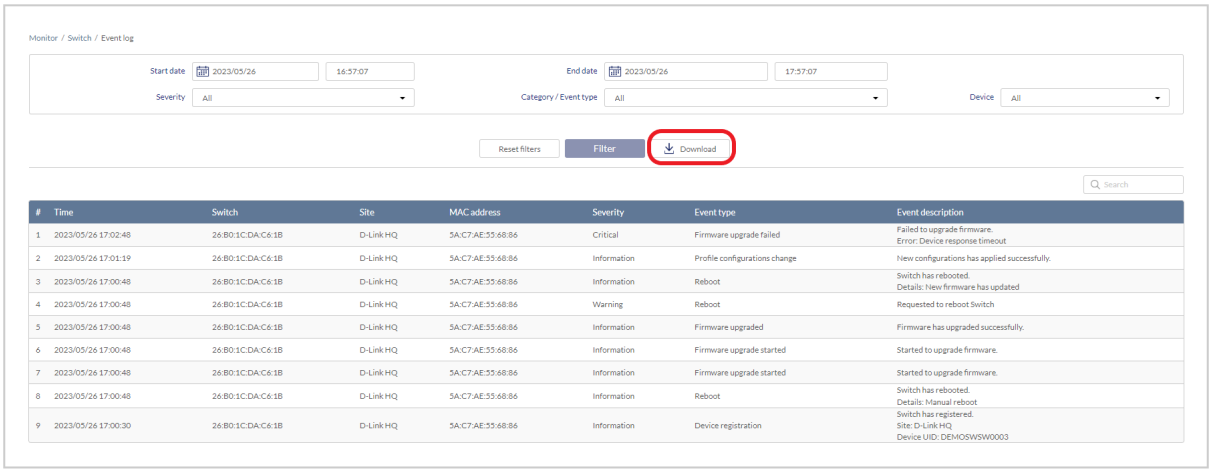
From the Event Logs window, you can consult a detailed log of events occurring on the network. You can define event filter parameters, including event type and time period.

Filtering Event Log Parameters

1. Navigate to **Monitor > Switch > Event Log**.
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. The severity is classified in 3 states: Critical- Indicates major configuration changes or offline/online status changes, Warning - Indicates system reboot events following scheduled firmware upgrade, Information- Indicates device clients association and disassociation events.
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 to filter the results.
   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

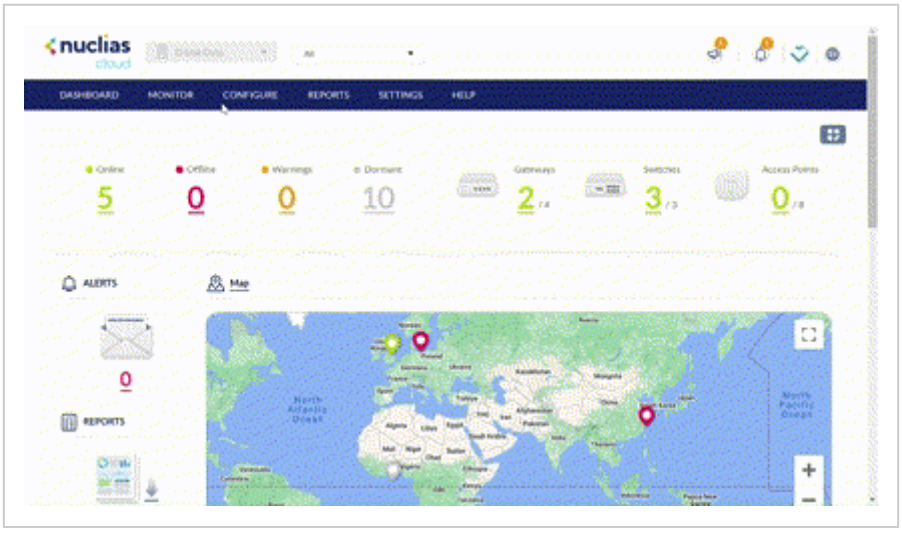
1. Navigate to **Monitor > Switch > Event Log**.
2. From the event log list, click **Download**.


Monitor / Switch / Event log
Start date 2023/05/26 16:57:07
End date 2023/05/26 17:57:07
Severity All
Category / Event type All
Device All
Reset filters
Filter
Download
Search
Time Switch Site MAC address Severity Event type Event description
1 2023/05/26 17:02:48 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Critical Firmware upgrade failed Failed to upgrade firmware. Error: Device response timeout
2 2023/05/26 17:01:19 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Information Profile configurations change New configurations has applied successfully.
3 2023/05/26 17:00:48 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Information Reboot Switch has rebooted. Details: New firmware has updated
4 2023/05/26 17:00:48 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Warning Reboot Requested to reboot Switch
5 2023/05/26 17:00:48 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Information Firmware upgraded Firmware has upgraded successfully.
6 2023/05/26 17:00:48 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Information Firmware upgrade started Started to upgrade firmware.
7 2023/05/26 17:00:48 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Information Firmware upgrade started Started to upgrade firmware.
8 2023/05/26 17:00:48 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Information Reboot Switch has rebooted. Details: Manual reboot
9 2023/05/26 17:00:30 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Information Device registration Switch has registered. Site: D-Link HQ Device UID: DEMOSWSW0003

Clients

Devices

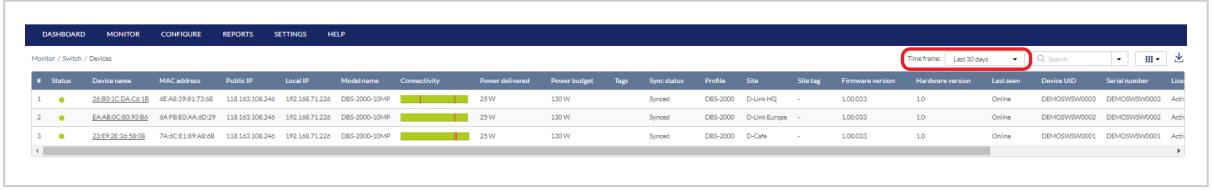
From the Devices window, you can consult a detailed log of events occurring on the network. You can also filter events using specific event filter parameters, including event type and time period.



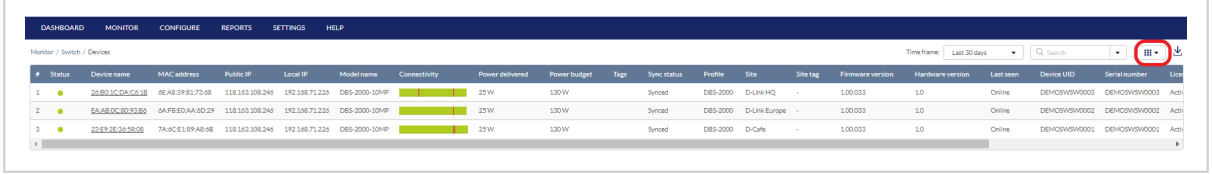
The Device Monitor

Customizing the Device Monitor Overview

1. Navigate to **Monitor > Switch > Devices**.
2. Select a time frame from the drop-down menu to set the duration for connectivity information.



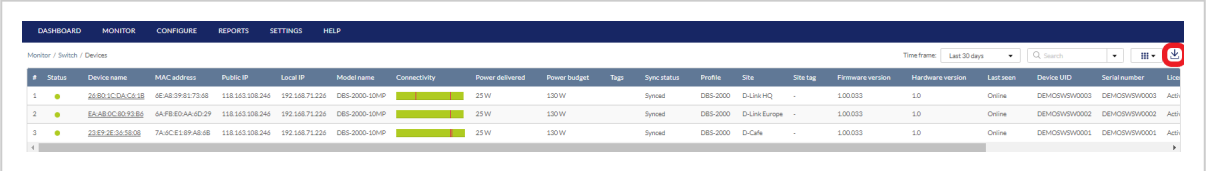
3. Click the filter parameter icon.



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 > Devices**.
2. From the device list, click the **Download** icon in the top-right.



Device Basic Settings

Changing the Device Site and Profile

1. Navigate to **Monitor > Switch > Devices** and select a device from the list.
2. Select the **Basic** tab at the top.
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 > Devices** and select a device from the list.
2. Select the **Basic** tab at the top.
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's 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 > Devices** and select a device from the list.
2. Select the **Basic** tab at the top.
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.
Management VLAN	Select a VLAN to be the management VLAN. This segments management traffic. Make sure that at least one member port

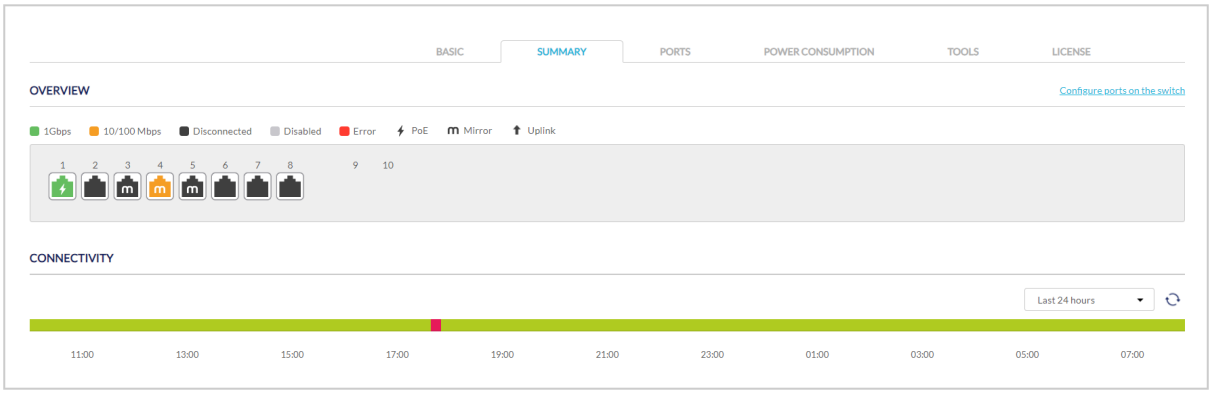
	belongs to the management VLAN to allow access to the management functions of the switch.
Subnet Mask	Enter the Subnet Mask.
Gateway	Enter the default gateway address.
DNS #1	Enter a primary DNS address.
DNS #2	[Optional] Enter a secondary DNS server address.
DNS #3	[Optional] Enter a tertiary DNS server address.
Proxy	[Optional] Enable or disable the use of DNS proxy. If enabled, enter the proxy host's IP address or domain name and port number (1-65535).

6. Click **Apply**.

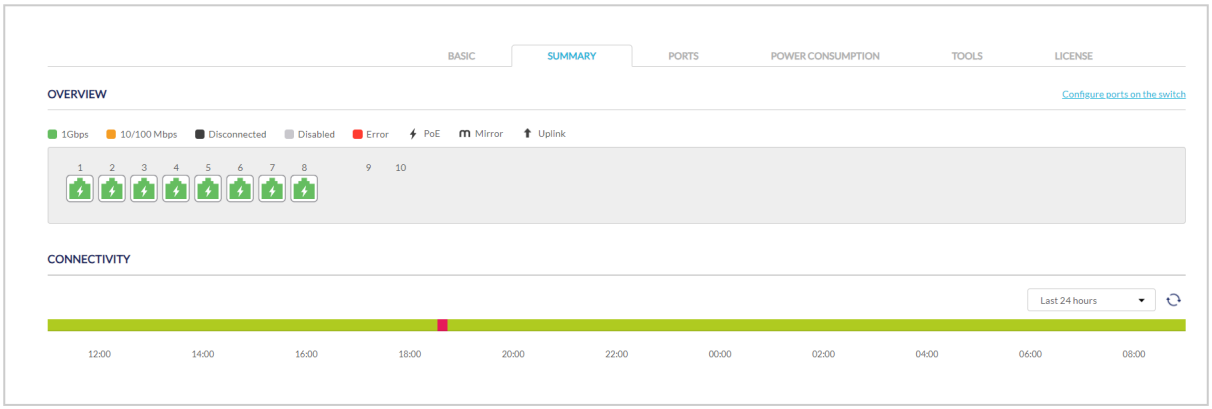
The Performance Summary

Viewing and Customizing the Switch Performance Summary

1. Navigate to **Monitor > Switch > Devices** and select a device from the list.
2. Select the **Summary** tab at the top.
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.



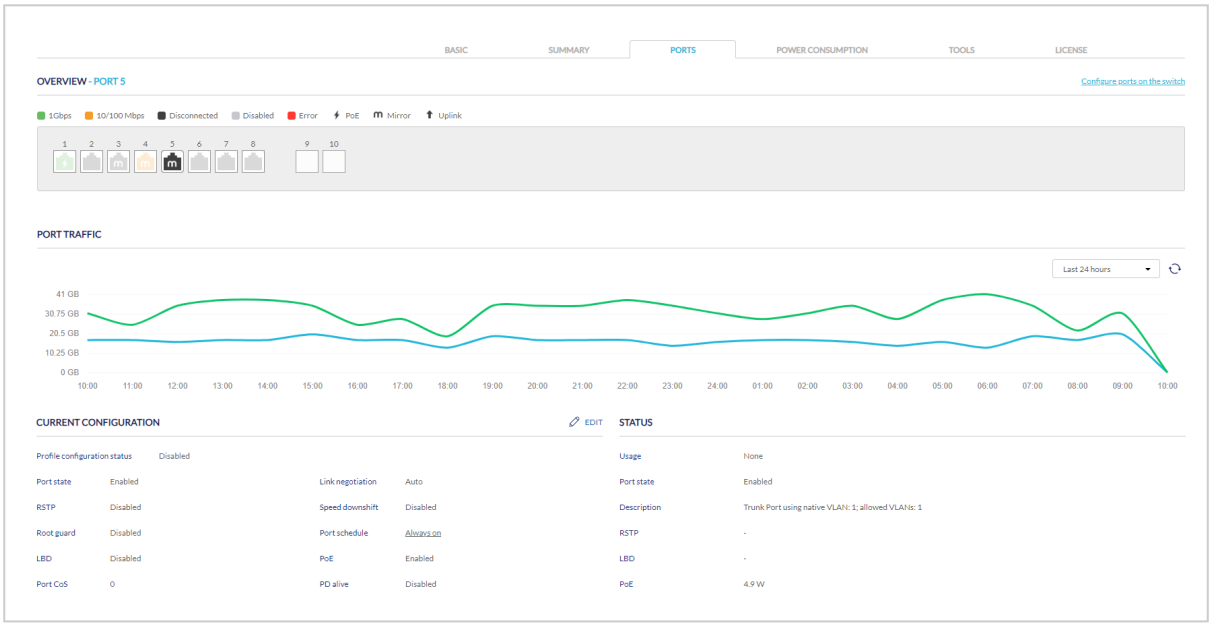
5. [Optional] Click **Configure ports on the switch** to go to the switch port configuration window. Refer to the Switch Ports section for more information.



Ports Status

Viewing and Customizing the Switch Port Status Overview

1. Navigate to **Monitor > Switch > Devices** and select a device from the list.
2. Select the **Ports** tab at the top.



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. **Note**: 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. Note: LBD cannot be used in conjunction with RSTP.
Port CoS	Select a value for Cos value (0-7).
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 if the Trunk type is selected.
Allowed VLANs	Enter the IDs of the VLANs that can route traffic through this port if the Trunk type is selected. Enter **All** to allow all traffic from all VLANs to pass through this port.
Access VLAN	Enter the ID of the VLAN the port belongs to if the Access type is selected.
Access Policy	Select the Access Policy for this port if the Access type is selected. The options include Disabled, MAC Whitelist, Port Security Delete-on-Time Mode, and Port Security Permanent Mode. MAC Whitelist: Allows only the specified MAC addresses in the Static Whitelisted MACs. Port Security Delete-on-Time Mode: All learned MAC addresses have a limited lifetime and will be erased when the lifetime is reached. Port Security Permanent Mode: Allows the MAC addresses learned through this port. The number of allowed addresses is set by Dynamic Whitelist Size Limit. When the number of Dynamic Whitelisted MACs reaches this limit, new devices will be denied access to this port.

Static Whitelisted MACs	Enter the MAC addresses that can access this port to restrict access to this port to devices with specific MAC addresses. If entering multiple MAC addresses, enter only one address per line.
Dynamic Whitelist Size Limit	Enter the maximum number of allowed MAC addresses that the device should learn dynamically for the Port Security Delete-on-time Mode or Port Security Permanent Mode.
Dynamic Whitelisted MACs	Display the learned MAC addresses for the Port Security Delete-on-time mode and Port Security Permanent Mode.
Tags	Enter a descriptive tag for the port. Multiple tags can be entered. If multiple ports are selected, 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.
Link (SFP)	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.
Speed Downshift	Enables/disables automatic speed downshift on the supported interface when the designated maximum speed cannot be established.
PoE	Choose to enable or disable Power over Ethernet (PoE) functionality on this port. **Note**: The PoE setting will only apply to ports that support Power over Ethernet.
PD Alive	Enable or disable the automatic detection of the Powered Devices status.
PD IP Address	Enter the IP address of the Powered Device.

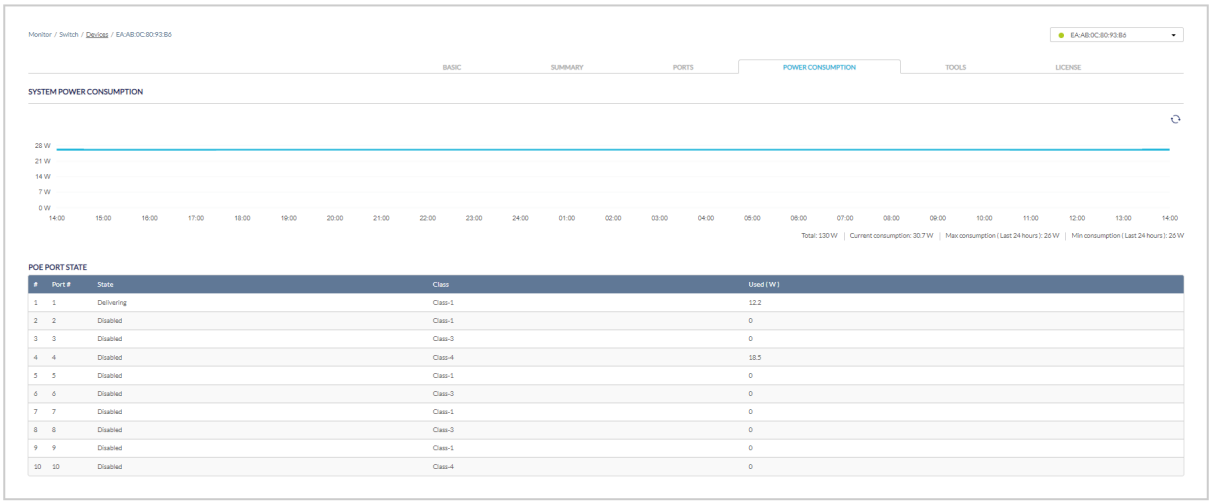
Port Schedule	Choose a pre-configured schedule policy. Go to **Configure > Schedule policies** to access the configured schedules.
Traffic Segmentation	Enable or disable traffic segmentation on this port to further restrict traffic flow in your network. If enabled, select the forward ports.
Forward Ports	Select the forward ports if traffic segmentation is enabled.
Flow Control	Enable or disable the flow control on the port to regulate the data transfer rate between two devices.

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 different packet types (e.g. broadcast , CRC error, or collision) for the selected time period.

Power Consumption

Viewing and Customizing the Switch Power Consumption Overview

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



Tools

Performing a Device Ping Test

1. Navigate to **Monitor > Switch > Devices** and select a device from the list.

2. Select the **Tools** tab in the top-right of the screen.
3. In the IP address/FQDN field in the Ping section, enter a valid IP address or FQDN.
4. Click **Ping**.

Performing a MAC Forwarding Table Test

1. Navigate to **Monitor > Switch > Devices** 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 > Devices** 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. Separate multiple port numbers with "," and use "-" for port range, for example, 1,5,7-10.
   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 > Devices** 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 port cycle. Separate multiple port numbers with "," and use "-" for port range, for example, 1,5,7-10.
4. Click **Test**.

Performing a Locate Device Test

1. Navigate to **Monitor > Switch > Devices** 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 > Devices** 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**.

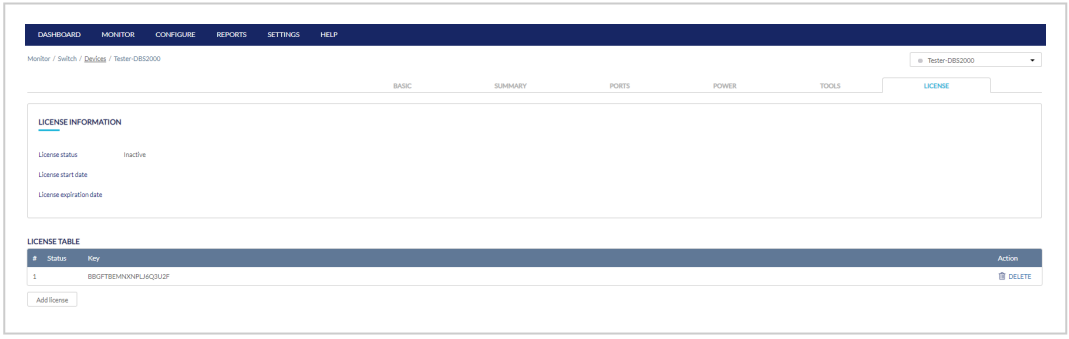
Adding a License Key to a Device

1. Navigate to **Monitor > Switch > Devices** 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 > Devices** 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 reclassify it as unused in the license management inventory until it is reassigned to another device.

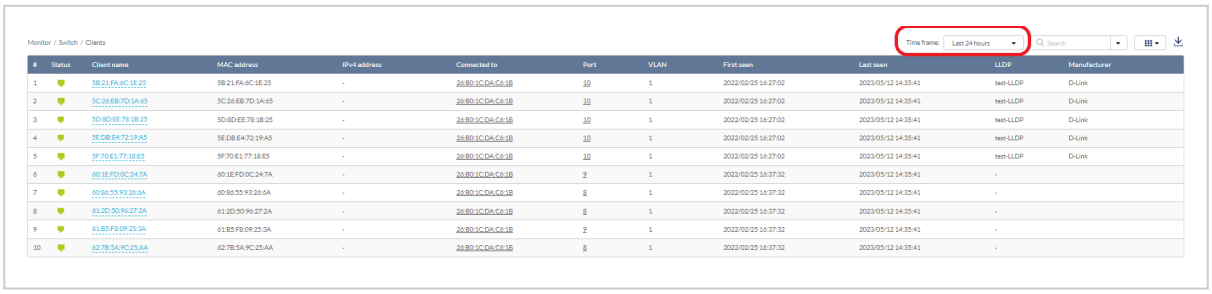


Clients

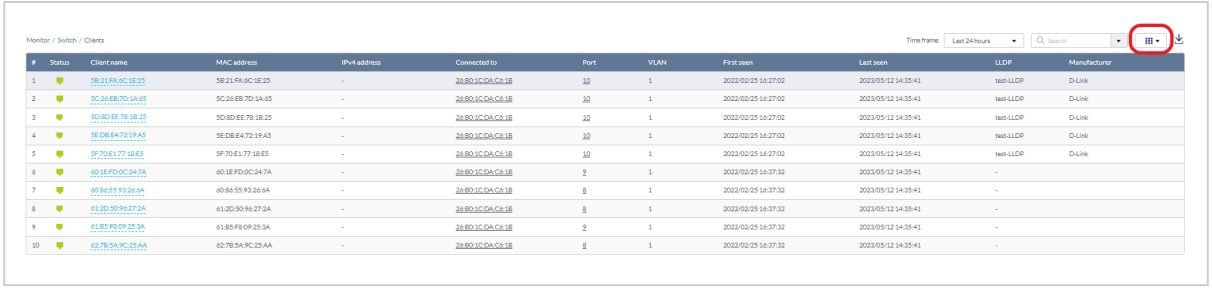
From the Clients window, you can consult a detailed overview of all currently connected devices with additional information including connected ports, VLAN, and other information such as MAC addresses and LLDP setting.

Customizing the Client Monitor Overview

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



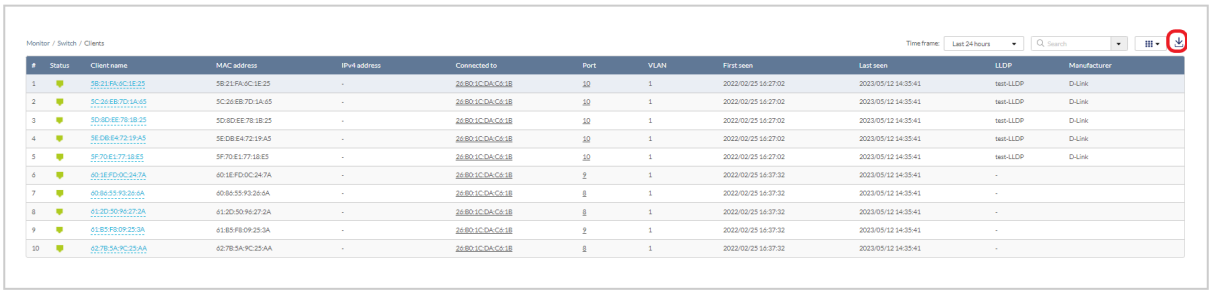
3. Click the parameter filter icon.



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 Log

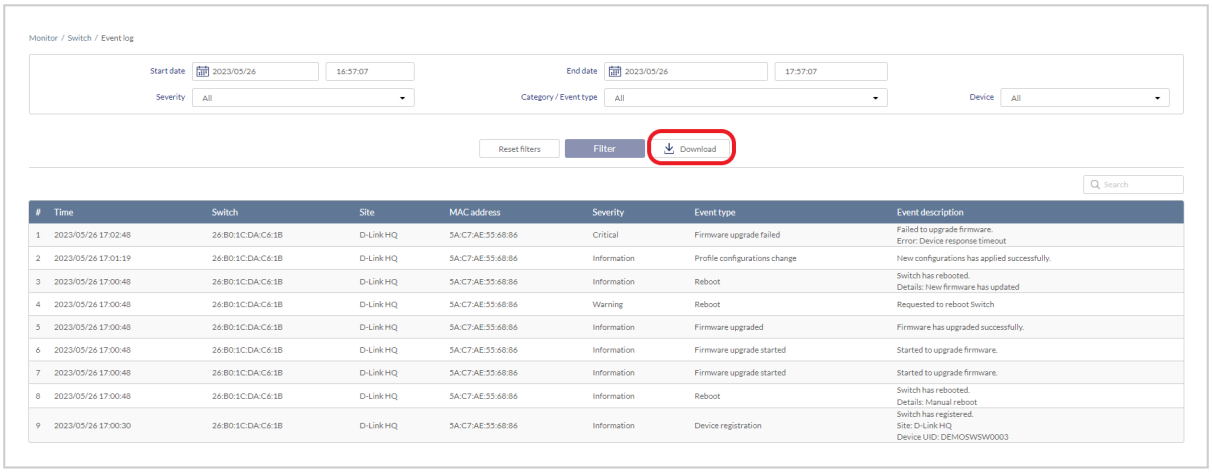
From the Event Logs window, you can consult a detailed log of events occurring on the network. You can define event filter parameters, including event type and time period.

Filtering Event Log Parameters

1. Navigate to **Monitor > Switch > Event Log**.
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. The severity is classified in 3 states: Critical- Indicates major configuration changes or offline/online status changes, Warning - Indicates system reboot events following scheduled firmware upgrade, Information- Indicates device clients association and disassociation events.
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 to filter the results.
   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

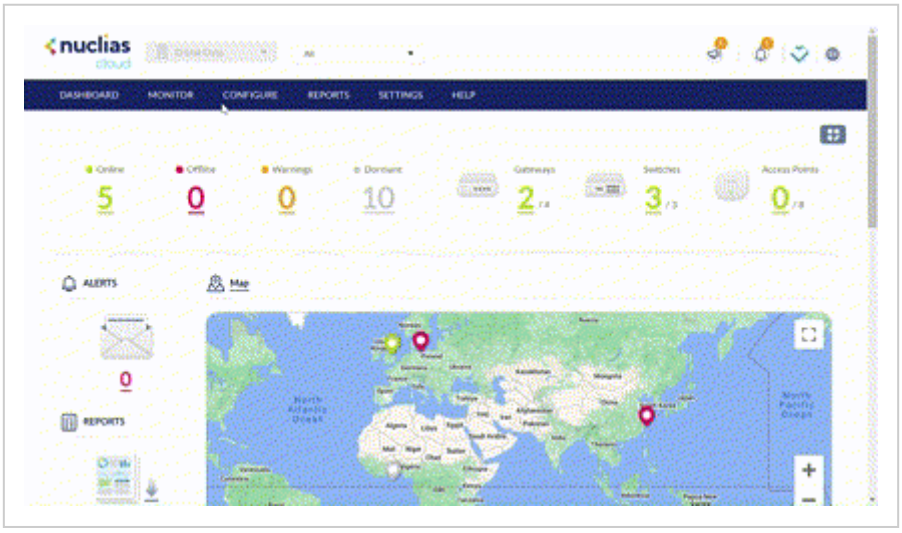
1. Navigate to **Monitor > Switch > Event Log**.
2. From the event log list, click **Download**.


Monitor / Switch / Event log
Start date
2023/05/26
16:57:07
End date
2023/05/26
17:57:07
Severity
All
Category / Event type
All
Device
All
Reset filters
Filter
Download
Search
Time Switch Site MAC address Severity Event type Event description
1 2023/05/26 17:02:48 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Critical Firmware upgrade failed Failed to upgrade firmware. Error: Device response timeout
2 2023/05/26 17:01:19 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Information Profile configurations change New configurations has applied successfully.
3 2023/05/26 17:00:48 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Information Reboot Switch has rebooted. Details: New firmware has updated
4 2023/05/26 17:00:48 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Warning Reboot Requested to reboot Switch
5 2023/05/26 17:00:48 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Information Firmware upgraded Firmware has upgraded successfully.
6 2023/05/26 17:00:48 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Information Firmware upgrade started Started to upgrade firmware.
7 2023/05/26 17:00:48 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Information Firmware upgrade started Started to upgrade firmware.
8 2023/05/26 17:00:48 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Information Reboot Switch has rebooted. Details: Manual reboot
9 2023/05/26 17:00:30 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Information Device registration Switch has registered. Site: D-Link HQ Device UID: DEMOSWSW0003

Event Log

Devices

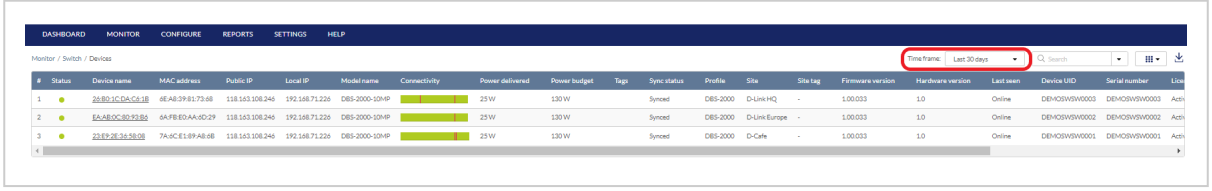
From the Devices window, you can consult a detailed log of events occurring on the network. You can also filter events using specific event filter parameters, including event type and time period.



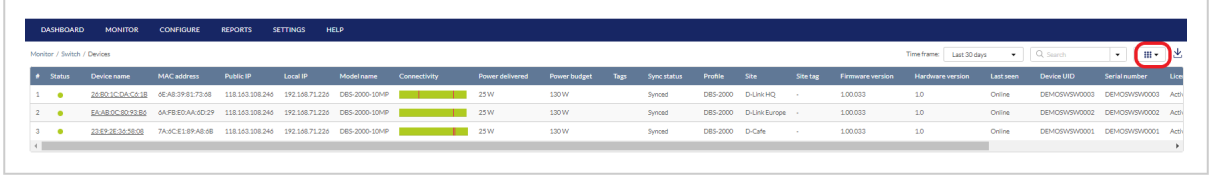
The Device Monitor

Customizing the Device Monitor Overview

1. Navigate to **Monitor > Switch > Devices**.
2. Select a time frame from the drop-down menu to set the duration for connectivity information.



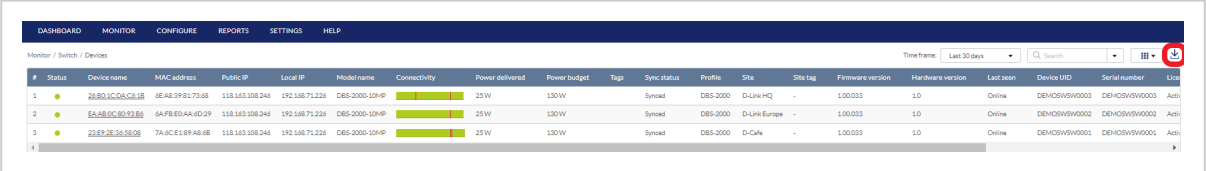
3. Click the filter parameter icon.



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 > Devices**.
2. From the device list, click the **Download** icon in the top-right.



Device Basic Settings

Changing the Device Site and Profile

1. Navigate to **Monitor > Switch > Devices** and select a device from the list.
2. Select the **Basic** tab at the top.
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 > Devices** and select a device from the list.
2. Select the **Basic** tab at the top.
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's 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 > Devices** and select a device from the list.
2. Select the **Basic** tab at the top.
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.
Management VLAN	Select a VLAN to be the management VLAN. This segments management traffic. Make sure that at least one member port

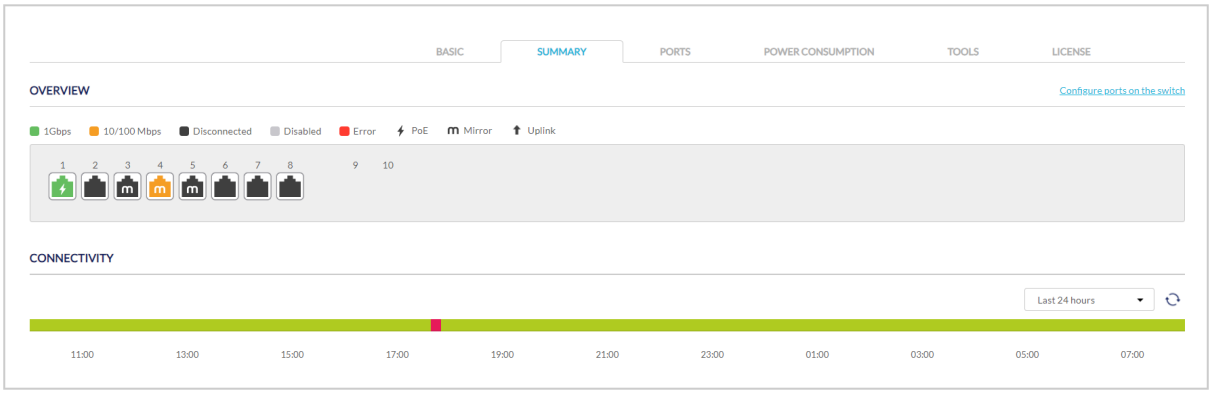
	belongs to the management VLAN to allow access to the management functions of the switch.
Subnet Mask	Enter the Subnet Mask.
Gateway	Enter the default gateway address.
DNS #1	Enter a primary DNS address.
DNS #2	[Optional] Enter a secondary DNS server address.
DNS #3	[Optional] Enter a tertiary DNS server address.
Proxy	[Optional] Enable or disable the use of DNS proxy. If enabled, enter the proxy host's IP address or domain name and port number (1-65535).

6. Click **Apply**.

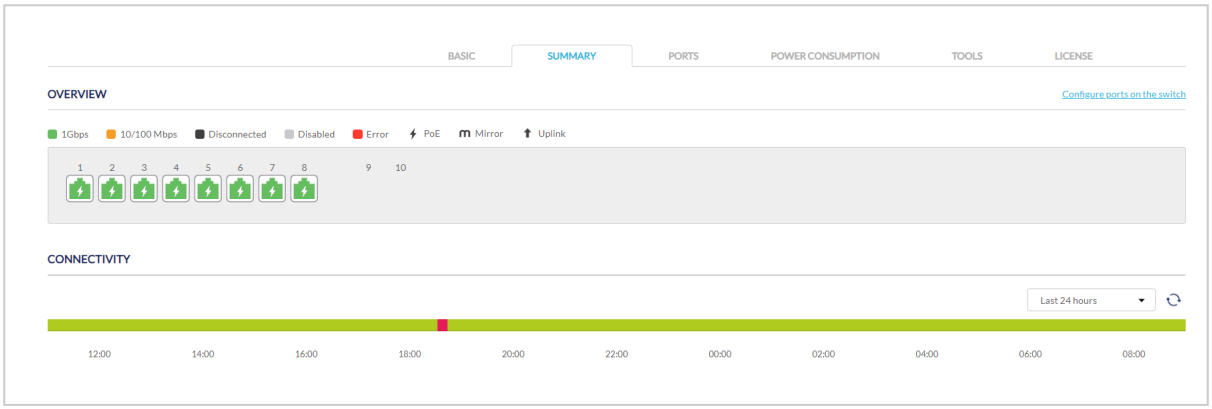
The Performance Summary

Viewing and Customizing the Switch Performance Summary

1. Navigate to **Monitor > Switch > Devices** and select a device from the list.
2. Select the **Summary** tab at the top.
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.



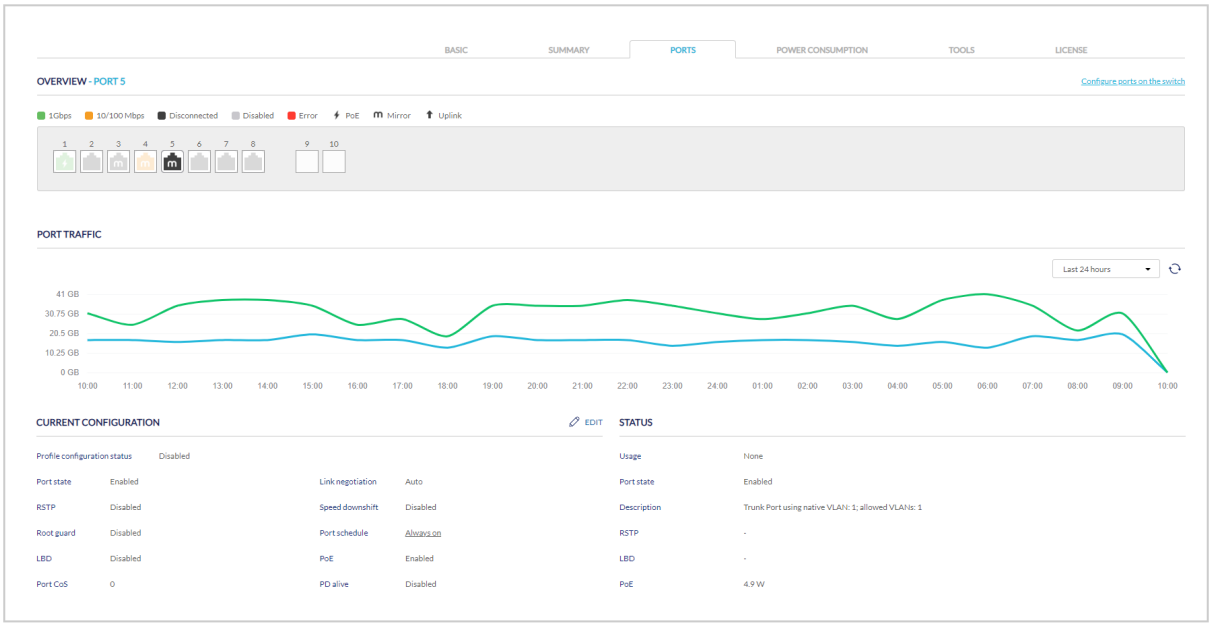
5. [Optional] Click **Configure ports on the switch** to go to the switch port configuration window. Refer to the Switch Ports section for more information.



Ports Status

Viewing and Customizing the Switch Port Status Overview

1. Navigate to **Monitor > Switch > Devices** and select a device from the list.
2. Select the **Ports** tab at the top.



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. **Note**: 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. Note: LBD cannot be used in conjunction with RSTP.
Port CoS	Select a value for Cos value (0-7).
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 if the Trunk type is selected.
Allowed VLANs	Enter the IDs of the VLANs that can route traffic through this port if the Trunk type is selected. Enter **All** to allow all traffic from all VLANs to pass through this port.
Access VLAN	Enter the ID of the VLAN the port belongs to if the Access type is selected.
Access Policy	Select the Access Policy for this port if the Access type is selected. The options include Disabled, MAC Whitelist, Port Security Delete-on-Time Mode, and Port Security Permanent Mode. MAC Whitelist: Allows only the specified MAC addresses in the Static Whitelisted MACs. Port Security Delete-on-Time Mode: All learned MAC addresses have a limited lifetime and will be erased when the lifetime is reached. Port Security Permanent Mode: Allows the MAC addresses learned through this port. The number of allowed addresses is set by Dynamic Whitelist Size Limit. When the number of Dynamic Whitelisted MACs reaches this limit, new devices will be denied access to this port.

Static Whitelisted MACs	Enter the MAC addresses that can access this port to restrict access to this port to devices with specific MAC addresses. If entering multiple MAC addresses, enter only one address per line.
Dynamic Whitelist Size Limit	Enter the maximum number of allowed MAC addresses that the device should learn dynamically for the Port Security Delete-on-time Mode or Port Security Permanent Mode.
Dynamic Whitelisted MACs	Display the learned MAC addresses for the Port Security Delete-on-time mode and Port Security Permanent Mode.
Tags	Enter a descriptive tag for the port. Multiple tags can be entered. If multiple ports are selected, 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.
Link (SFP)	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.
Speed Downshift	Enables/disables automatic speed downshift on the supported interface when the designated maximum speed cannot be established.
PoE	Choose to enable or disable Power over Ethernet (PoE) functionality on this port. **Note**: The PoE setting will only apply to ports that support Power over Ethernet.
PD Alive	Enable or disable the automatic detection of the Powered Devices status.
PD IP Address	Enter the IP address of the Powered Device.

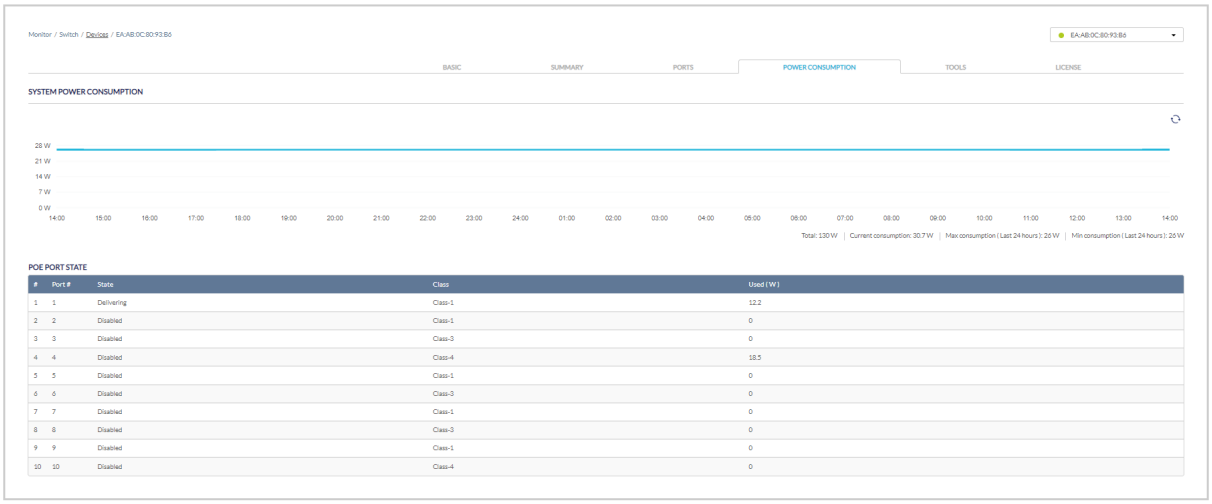
Port Schedule	Choose a pre-configured schedule policy. Go to **Configure > Schedule policies** to access the configured schedules.
Traffic Segmentation	Enable or disable traffic segmentation on this port to further restrict traffic flow in your network. If enabled, select the forward ports.
Forward Ports	Select the forward ports if traffic segmentation is enabled.
Flow Control	Enable or disable the flow control on the port to regulate the data transfer rate between two devices.

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 different packet types (e.g. broadcast , CRC error, or collision) for the selected time period.

Power Consumption

Viewing and Customizing the Switch Power Consumption Overview

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



Tools

Performing a Device Ping Test

1. Navigate to **Monitor > Switch > Devices** and select a device from the list.

2. Select the **Tools** tab in the top-right of the screen.
3. In the IP address/FQDN field in the Ping section, enter a valid IP address or FQDN.
4. Click **Ping**.

Performing a MAC Forwarding Table Test

1. Navigate to **Monitor > Switch > Devices** 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 > Devices** 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. Separate multiple port numbers with "," and use "-" for port range, for example, 1,5,7-10.
   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 > Devices** 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 port cycle. Separate multiple port numbers with "," and use "-" for port range, for example, 1,5,7-10.
4. Click **Test**.

Performing a Locate Device Test

1. Navigate to **Monitor > Switch > Devices** 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 > Devices** 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**.

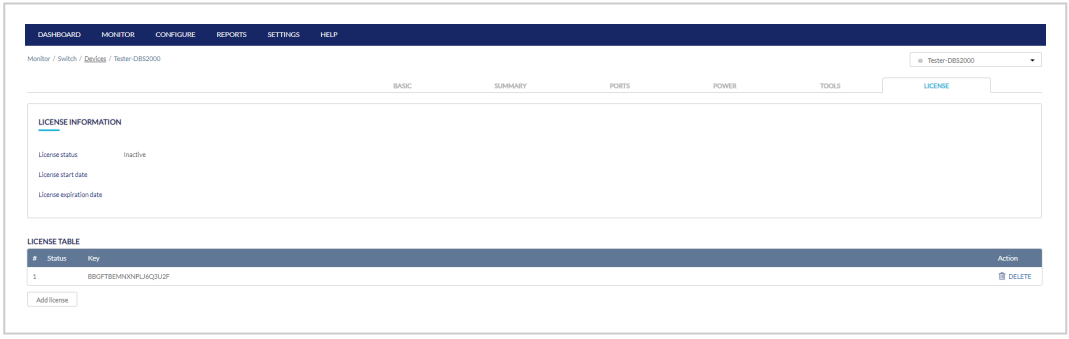
Adding a License Key to a Device

1. Navigate to **Monitor > Switch > Devices** 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 > Devices** 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 reclassify it as unused in the license management inventory until it is reassigned to another device.

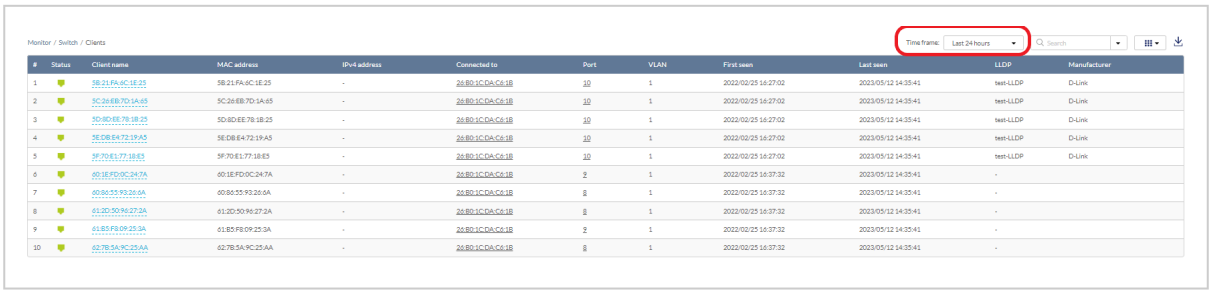


Clients

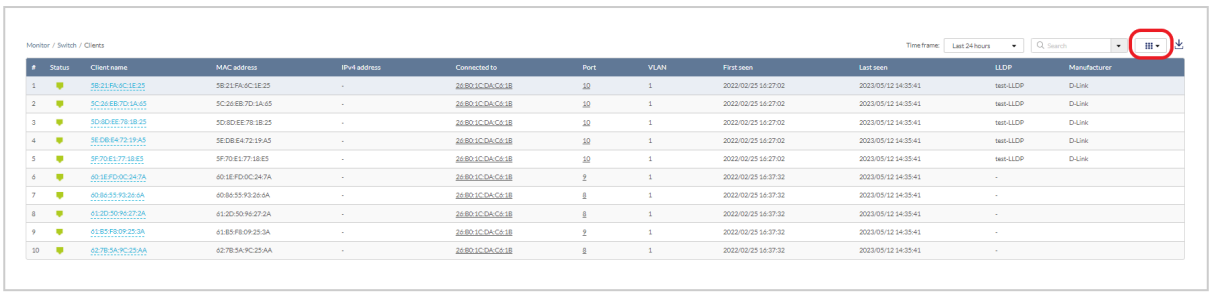
From the Clients window, you can consult a detailed overview of all currently connected devices with additional information including connected ports, VLAN, and other information such as MAC addresses and LLDP setting.

Customizing the Client Monitor Overview

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



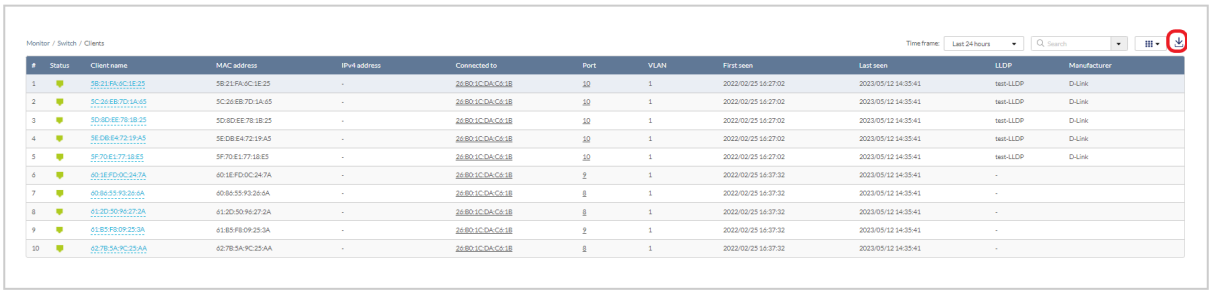
3. Click the parameter filter icon.



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 Log

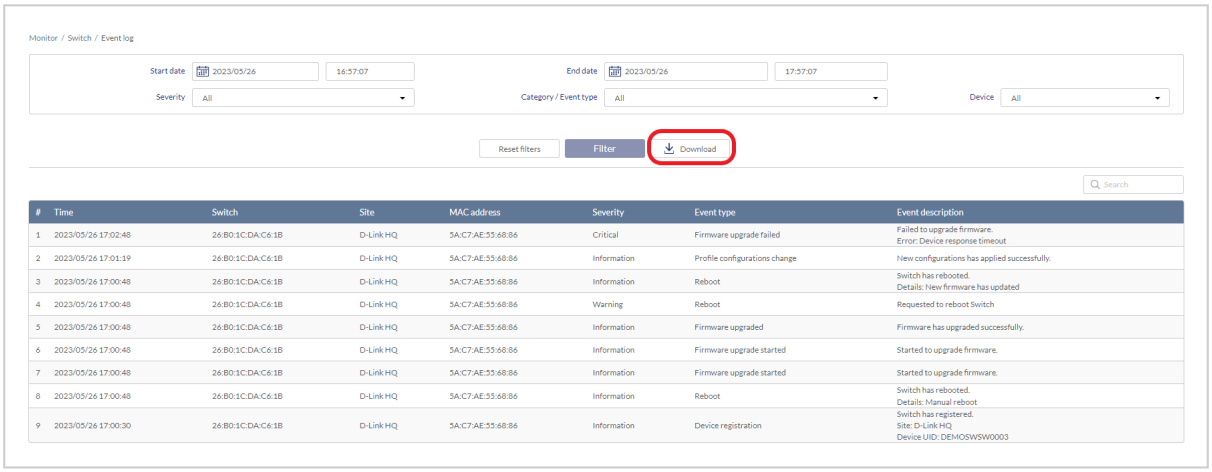
From the Event Logs window, you can consult a detailed log of events occurring on the network. You can define event filter parameters, including event type and time period.

Filtering Event Log Parameters

1. Navigate to **Monitor > Switch > Event Log**.
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. The severity is classified in 3 states: Critical- Indicates major configuration changes or offline/online status changes, Warning - Indicates system reboot events following scheduled firmware upgrade, Information- Indicates device clients association and disassociation events.
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 to filter the results.
   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

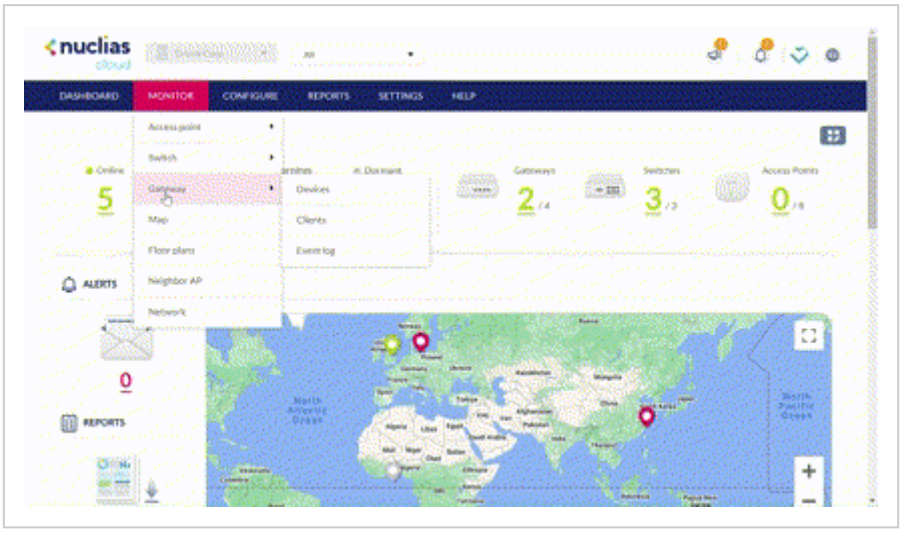
1. Navigate to **Monitor > Switch > Event Log**.
2. From the event log list, click **Download**.


Monitor / Switch / Event log
Start date 2023/05/26 16:57:07
End date 2023/05/26 17:57:07
Severity All
Category / Event type All
Device All
Reset filters
Filter
Download
Search
Time Switch Site MAC address Severity Event type Event description
1 2023/05/26 17:02:48 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Critical Firmware upgrade failed Failed to upgrade firmware. Error: Device response timeout
2 2023/05/26 17:01:19 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Information Profile configurations change New configurations has applied successfully.
3 2023/05/26 17:00:48 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Information Reboot Switch has rebooted. Details: New firmware has updated
4 2023/05/26 17:00:48 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Warning Reboot Requested to reboot Switch
5 2023/05/26 17:00:48 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Information Firmware upgraded Firmware has upgraded successfully.
6 2023/05/26 17:00:48 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Information Firmware upgrade started Started to upgrade firmware.
7 2023/05/26 17:00:48 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Information Firmware upgrade started Started to upgrade firmware.
8 2023/05/26 17:00:48 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Information Reboot Switch has rebooted. Details: Manual reboot
9 2023/05/26 17:00:30 26:B0:1C:DA:C6:1B D-Link HQ 5A:C7:AE:55:68:86 Information Device registration Switch has registered. Site: D-Link HQ Device UID: DEMOSWSW0003

Monitor - Gateway

Devices

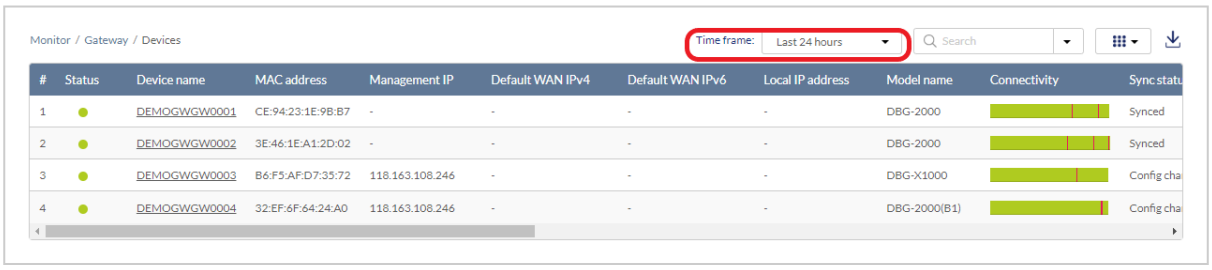
From the Devices window, you can consult a detailed log of events occurring on the network. You can also filter events using specific event filter parameters, including event type and time period.



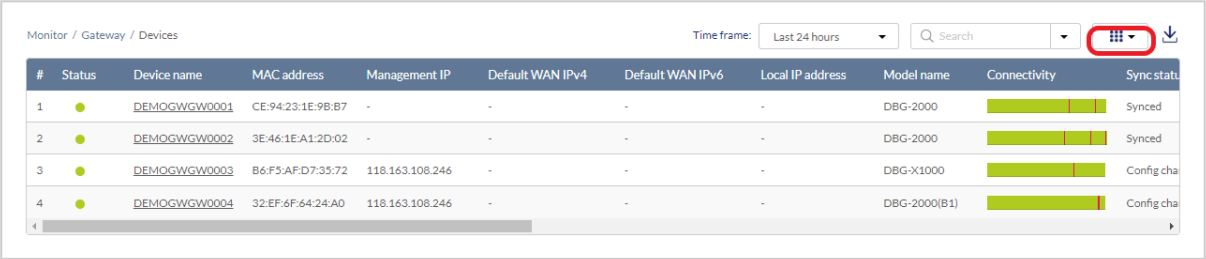
The Device Monitor

Customizing the Device Monitor Overview

1. Navigate to **Monitor > Gateway > Devices**.
2. Select a time frame from the drop-down menu to set the duration for connectivity information.



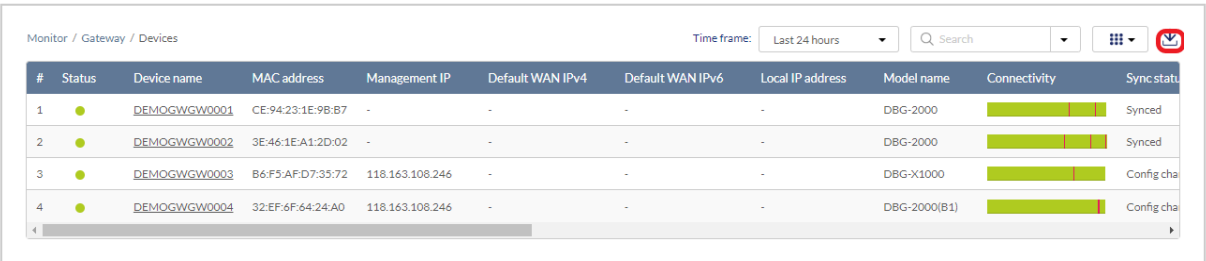
3. Click the filter parameter icon.



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

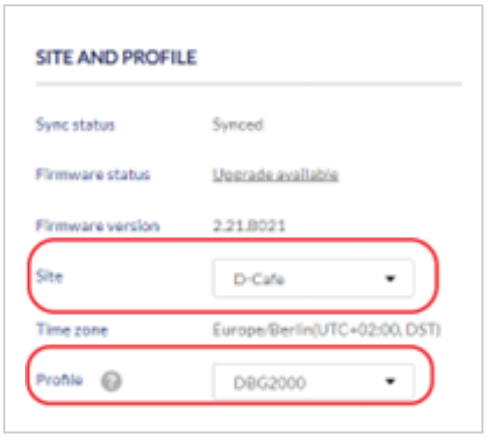
1. Navigate to **Monitor > Gateway > Devices**.
2. From the device list, click the **Download** icon in the top-right to export the table listing as a CSV file.



Device Basic Settings

Changing the Device Site and Profile

1. Navigate to **Monitor >Gateway > Devices** and select a device from the list.
2. Select the **Basic** tab at the top.
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 **Save**.

The Performance Summary

Viewing and Customizing the Gateway Performance Summary

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Summary** tab. Click the tabs at the top to obtain additional information described below:

Status	Provides connection information for the device along with basic port configuration and traffic statistics for each port. You can also obtain Internet usage for both download and upload data in a specified time frame.
Statistics	Provides reports of the number of connected clients in the selected time frame. You can also obtain reports of WAN port usage and the whole Internet usage as well as VPN usage.
DHCP	Provides the utilization rate of each configured DHCP subnet. It also lists the DHCP leases history.
VPN Status	Provides VPN connection statistics. The page lists the active VPN association or connections, the traffic details, and the tunnel state. You can view the status (connect or disconnect) of the gateway's VPN connections as a whole (by selecting Overview for the Display VPN type) or view each VPN separately.

Network Settings

Verifying and Changing the Default WAN Configuration

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Network** tab at the top.
3. Under **WAN Mode Configuration**, verify the WAN mode and the primary WAN port (or Default WAN Configuration) settings. Note that the settings or configurations here depend on the device model and firmware.

To change the Default WAN or WAN Mode Configuration:

1. Disable the option **Use Profile configuration** first at the top of the configuration page to allow changes.
2. Select IPv4 and IPv6 default WAN configuration. Or select a WAN mode from the available options. For **Primary WAN**, designate a WAN port as the primary WAN. For **Auto-rollover using WAN**, select both Primary and Secondary WAN ports as well as the **Health Check** method. For DNS servers and Ping IP address methods, enter the respective server IP address as the destination to check the connectivity. Also enter the **Retry interval** (seconds) and **Failover after** (number of failed retries). For Load balancing, select the method (either Round robin or Spillover mode).
3. For **Round robin**, configure the Health check method (or none) and enter the **Retry interval** (seconds) and **Failover after** (number of failed retries). Hence, if a WAN interface disconnects, only the alternate WAN ports will transfer traffic flows in a round robin manner. For **Spillover**, enter the **Load tolerance** (%) and **Max bandwidth** (Mbps) as the threshold value. Once the threshold is exceeded, new traffic flows will be allocated to the alternate WAN interfaces. The precedence for selection is based on the configuration of Primary, Secondary, and Tertiary WAN interface.
4. Click **Apply**.

Note: The WAN mode can be configured using Profiles. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Using Dynamic DNS

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Network** tab at the top.
3. Under **Dynamic DNS**, enable or disable the service.
4. > Click **Apply**.

To add a DDNS service:

1. Disable the option Use Profile configuration first at the top of the configuration page.
2. Click **Add**. Enter the following information:

WAN Interface	Select the WAN interface for configuration
Service Provider	Select the DDNS service provider.
Username/Password	Enter the DDNS account name and password.
Hostname	Enter the registered hostname with the DDNS service.
Wildcard	Enable or disable the wildcard option which will resolve *.hostname to the same designated IP address.
Use Public IP	Enable or disable the use of a public IP address.
Force Update Interval	Enter the DDNS update interval (days).

3. Click **Save** to close the screen. Then click **Apply**.

Using IP Alias for the WAN

Note: The IP Alias function is only available on supported models.

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Network** tab at the top.
3. Under **IP Aliasing** , click **Add** to bind one or multiple IP addresses to a WAN interface.

   Enter the following information:

WAN Interface	Select the WAN interface for configuration
IP Address/Subnet Mask	Enter the IP address and subnet mask to bind to the WAN interface.

4. Click **Save** to close the screen. Then click **Apply**.

Viewing and Customizing the Gateway Port Status Overview

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Summary** tab at the top. The ports of the gateway device are displayed along with their detailed information shown in the table below:

Port Number	Numbering of the ports on the connector panel.

Interface Name	The name that identifies the port.
Port Status	Displays the link state of the port.
MAC Address	The MAC address of the port.
IP Address/ Subnet Mask	The IP address and subnet mask assigned to the port
Gateway	The gateway IP address if it has been assigned.
DHCP Mode	Displays if DHCP service has been enabled on the device.
Sent Bytes	The amount of data sent out of the port (bytes).
Received Bytes	The amount of data received through the port (bytes).
Total Bytes	The total amount of sent and received data volume (bytes).

To configure a port's basic settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Network** tab at the top.
3. Disable **Use Profile Configuration** to allow modification.
4. Under **Port Configuration** , select a port and click **EDIT** under Actions. Specify the following information for the selected LAN port:

Interface Type	Select the connection type: LAN, WAN, or DMZ.

Interface Name	Enter a name to identify this interface.
Bridge Network	Enable or disable bridging with another network. Configure the interface with more settings below if bridging is not enabled.
IP Address/ Subnet Mask	Enter an IP address with subnet mask.
DHCP Mode	Enable or disable DHCP service for IP address assignment.
DHCP Server	Enter the following information if DHCP server is selected. Domain name: Assign a domain name for DHCP service. Starting IP address/Ending IP address: Enter the range of IP addresses that can be assigned dynamically. Default gateway: Assign a default gateway for DHCP service. DNS server: Configure DNS by specifying a static DNS server, DNS setting from the ISP, or using DNS proxy. For static DNS, enter the DNS servers or WIN server IP address. Lease Time: Enter a time value of 1 to 10080 minutes.
Allow Ping from LAN	Enable or disable ping command executed from this port.
DHCP Relay	Enter the remote DHCP server address if DHCP relay is selected.
DNS Proxy	Enable or disable DNS proxy.

For a WAN port (if the device supports this feature), configure the following:

Interface Type	Select the connection type: LAN, WAN, or DMZ.

Connection Type	Select the connection method: DHCP, Static IP, PPPoE, PPTP, or L2TP. For Static IP, enter the IP address/Subnet mask, Gateway IP address and Primary/Secondary DNS servers, and specify whether to keep the original MAC address as well as the MTU size. For PPPoE, select the Address mode: Dynamic IP or Static IP. For static IP, enter the IP address/Subnet mask and PPPoE connection Username and Password. Then specify the Authentication type from one of the following: None, MS-CHAPv2, MS-CHAP, CHAP, PAP, or Auto-negotiate. For Dynamic IP, you don't need to enter the IP address/subnet information but configure all other settings as specified above. For both addressing modes, enter the Service name (optional) and select the Reconnect mode: Always on, or On demand (enter the Maximum idle time to wait before terminating the connection in minutes for this option). Then configure the DNS servers and specify whether to keep the original MAC address as well as the MTU size. For PPTP, if Static IP is selected, enter the following IP address information: IP address/Subnet mask, Gateway IP address, and Static DNS IP address. For both Address modes, enter the PPTP server name and connection Username and Password. For both modes, configure whether MPPE (Microsoft Point-to-Point Encryption (MPPE) will be used and the Reconnect mode: Always on or On demand (enter the Maximum idle time to wait before terminating the connection in minutes for this option). Then configure the DNS servers and specify whether to keep the original MAC address as well as the MTU size. For L2TP, if Static IP is selected, enter the following IP address information: IP address/Subnet mask, Gateway IP address, and Static DNS IP address. For both Address modes, enter the L2TP server name and connection Username and Password. For both modes, enter the Secret (optional) and configure the Reconnect mode: Always on or On demand (enter the Maximum idle time to wait before terminating the connection in minutes for this option). Then configure the DNS servers and specify whether to keep the original MAC address as well as the MTU size.
Advanced Settings	Enable or disable the following passthroughs: **Internet Protocol Security (IPsec)** which is used for securing packets exchange at the IP layer.

	Point-to-Point Tunneling Protocol (PPTP) which is used for tunneling the Point-to-Point Protocol (PPP) communication in an IP network. **Layer 2 Tunneling Protocol (L2TP)** which is used for implementing Point-to-Point sessions utilizing multipoint tunneling technique.

5. Click **Save**. Then click **Apply** to apply the settings to the affected device immediately.

Viewing and Configuring VLANs

VLANs allow you to divide the network to different segments. To obtain the current VLAN settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Addressing.** The VLANs are displayed under the VLAN section with the following information:

Name	A name that helps identify this VLAN.
VLAN ID	The assigned VLAN ID.
Untagged/Tagged Ports	The member ports for the untagged VLAN and tagged VLAN .
IP address/Subnet Mask	The IP address/Subnet mask configured for the VLAN.
Captive Portal	The associated Captive Portal page.

To configure a VLAN:

1. Disable the **Use Profile configuration** option.
2. Under **VLAN**, click **Add** to add a new VLAN.

3. Click Apply at the top left to apply the changes to the affected device immediately.

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring IP Management List

The IP Management list displays the IP assignment of the DHCP clients:

Host Name	The host name of the client device.
Interface	The associated interface with the IP assignment.
IP Address	The assigned IP address of the host.
MAC Address	The MAC address of the host.
IPv6 Suffix	The assigned IPv6 suffix, which is the the last 64 bits of an IPv6 address.
IP-MAC Binding	Indicates whether the IP assignment is enforced on the client device with the specified MAC address to prevent the use of other static IP address on this client.
DHCP IP Reservation	Indicates whether this IP assignment is reserved for this client so that it can get the same IP assignment every time it sends a DHCP IP request.

To configure IP management for DHCP clients:

1. Disable the **Use Profile configuration** option.
2. Under **IP Management List**, click **Add** to add a new IP assignment.

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring Routing

Routing determines the path for packet delivery in a network. The routing capabilities vary depending on the device model.

To view the configured routing policies:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Routing**. The configured routing protocols are displayed:

IPv4/IPv6 Static Route

Name	A name that helps identify this route.
Destination	The destination subnetwork IP address.
Subnet Mask	The subnet mask of the destination address. This is only available for IPv4 configuration.
Gateway	The IP address of the gateway or next hop.
Interface	The associated interface for this route.
Metric	The number of hub count.
Active	Enable or disable this route configuration.

IPv4/IPv6 Policy Route

Name	The name that helps identify the route.
Local Gateway	The port of the device that the route would use.
Protocol	The protocols associated with this route.
Source Network	A single IP address or a range of IP addresses that this route will be applied to. “Any” means all source IP addresses.

Destination Network	A single IP address or a range of IP addresses that this route will be applied to. “Any” means all destination IP addresses.
Source Port	The port number used for this type of traffic. ”Any” means all source ports will be used for this service.
Destination Port	The port number used for this type of traffic. ”Any” means all destination ports will be used for this service.
Active	Enable or disable this route configuration.

RIP Configuration

Interface	The interface by which Routing Information Protocol (RIP) information exchange will be performed.
Direction	Indicates inbound, outbound, or traffic for both directions.
Version	The version of the RIP
Authentication	Indicates whether the authentication is enabled.
Active	Enable or disable this route configuration

OSPFV2 Configuration

Interface	The interface assigned to the area defined below.
NSSA	Enable or disable the not-so-stubby area (NSSA) which can import external route information.

Area	The assigned area ID.
Priority	The OSPF priority which is used for determining the OSPF designated router.
Hello Interval	The time interval (seconds) between each hello packet.
Dead Interval	The time (seconds) the device must wait before it declares a neighbor OSPF router down when a hello packet has not been received.
Cost	The cost of the OSPF path.
Authentication	Indicates the authentication method used
LAN Route Exchange	Enable or disable the exchange of LAN routing table.
Active	Enable or disable this OSPF route configuration.

To configure routing policy:

1. Disable the **Use Profile configuration**option.
2. Under each routing protocol supported by the device model, click Add to add a new routing policy.

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring Services

Supported services can be configured individually depending on the features of the gateway.

To view and configure the supported services and network functions:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.

2. Select the **Network > Services**.

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Managing Traffic

The Traffic Management provides control over certain types of traffic by setting limits on bandwidth and sessions. Note that the availability of this function depends on the capability of the gateway.
To view Traffic Shaping rules configured:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Traffic Management**.

Under Traffic Shaping, the following is displayed:

Name	The policy name.
Policy Type	Whether the traffic policy is applied to inbound or outbound traffic.
WAN Interface	The WAN port that this policy should be applied to.
Management Type	The metric to define the policy: Rate or Priority. Configure the following if Priority is selected: Low, Medium, or High. Higher priority means the traffic will be allocated with more bandwidth. If Rate is selected, enter the maximum bandwidth and minimum bandwidth (kbps).
Priority/Bandwidth Rate	The priority or the bandwidth configured for the respective management type.
Service	The type of traffic according to the protocol or application service configured.
Traffic Selector Match Type	The criteria for the traffic to which the policy should be applied: IP address, MAC address, or Interface.

Schedule Policy	The schedule policy that makes the policy effective during the designated time frame. Go to **Configure > Schedule policies** for scheduling information and configuration.

Viewing and Managing Session Limiting

To view Session Limiting rules configured:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Traffic Management**.

   Under Session Limiting, the following is displayed:

Name	The policy name.
Source Type	The source address can be configured as a single IP address, an IP address range, or an interface.
Maximum Sessions	The maximum number of sessions allowed (1-999).
Schedule Policy	The schedule policy that makes the policy effective during the designated time frame. Go to **Configure > Schedule policies** for scheduling information and configuration.

Viewing and Managing Custom Warning Pages

To view Custom Warning Page configured:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Traffic Management**.

   Under Custom Warning Page, the following is displayed:

Name	The policy name.
Source Type	The configured warning page to be displayed to users when the maximum limit of sessions has been reached . Go to

	Configure > Splash pages to view all the configured splash pages.
Active	Whether this rule is active or inactive.

To configure Traffic Management:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Traffic Management**.
3. Disable the option **Use Profile configuration.**

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring Captive Portal

The captive portal displays a splash page to wireless users who are required to agree to terms and conditions to use Internet services.
To view Captive Portal configured:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Captive Portal.**

The following information is displayed:

Name	The profile name.
Captive Portal	The authentication method for the users.
Splash Page	The pre-configured splash page which a wireless user must visit prior to using Internet services. The design of the page depends on the use case.
Basic Login	For basic login page, the associated authentication method: a local authentication database or an authentication server system.
3rd party Credentials	The configured third-party credential to be used for login.

SSID/VLANs	A pre-configured SSID/VLAN assigned to this captive portal setting.

To configure Captive Portal:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Captive Portal.**
3. Disable the option **Use Profile configuration.**

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring High Availability

Virtual Router Redundancy Protocol (VRRP) can be utilized to implement fault tolerance and load balancing on a network by designating primary and backup roles among the virtual routers. The primary router is responsible for processing packets sent to a virtual IP address and the backup router takes up the primary role when the primary becomes unavailable. This availability of this feature depends on device model.

To view VRRP settings configured:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > High Availability.** The following is displayed:

VRRP ID	The unique identifier for the VRRP group.
Interface	The interface to which the VRRP configuration would be applied.
IP Address	The virtual IP address.
Node Type	The designated role of the virtual router: Master or Backup.
Priority	The Priority determines the order of selection for a primary virtual router among the backup virtual routers (1-255). Higher number means high priority.

To configure VRRP settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > High Availability.**
3. Disable the option **Use Profile configuration.**

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring Wireless

You can create multiple SSIDs for your wireless network and configure each SSID with unique settings to accommodate different wireless usage scenarios. You can also configure radio settings such as operating mode and channels for different frequencies supported for the device model. Note that this feature is only available for supported models.

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Security Settings

Security features consist of firewall, intrusion prevention, and web content filtering as well as application control.

Note: Changing the Routing mode from Network Address Translation (NAT) to Router (go to Network > Addressing), the Security Firewall's option of Use Profile configuration will be disabled. Moreover, the rules configured for Port forwarding, Port triggering, and 1:1 NAT will be erased.

Firewall

To view a gateway's firewall settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Firewall.**

The following information is displayed:

IPV4/IPv6 FIREWALL RULES

IPv4/Ipv6 Firewall Rules allow or block certain types of traffic that need to be forwarded through the device.

Priority	The assigned priority number (1-998). Lower number means higher priority.
Name	The name of the rule.
Policy	Indicates whether it is a allow or deny rule.

Protocol	The associated protocol for the rule: Any, TCP, UDP, TCP/UDP, or ICMP.
Source Interface	The interface that the traffic is sent from.
Source	A single IP address or a range of IP addresses as the source host. Any means traffic from all IP addresses.
Source Port	The source port number used for this type of traffic. Any means all ports.
Destination	A single IP address or a range of IP addresses as the destination host. Any means traffic destined to all IP addresses.
Destination Port	The destination port number used for this type of traffic. Any means all ports.
Schedule	The associated Schedule Policy.
Active	Indicates whether this rule is enabled or disabled.

Note: The availability of IPv6 Firewall Settings depends on the features of the device model.

Port Forwarding

Port Forwarding redirects traffic entering the WAN to another port on the LAN. This is useful when a certain service is hosted on an interval server on the LAN.

To view Port Forwarding rules:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Firewall.**

The following information is displayed:

Name	The name for the rule.
Mode	Indicates whether the rule is for traffic forwarding or port translation.

Interface	The WAN interface to which this rule should be applied.
Protocol	The associated protocol of this rule: TCP, UDP, or TCP/UDP.
Public Port	The external port associated with this type of traffic or service (1-65535). It can be a single port or a range of ports.
Local IP	The IP address of the local server.
Local Port	The local port used for this service if translation mode is selected.
Allowed Remote IPs	The IP addresses of the remote hosts that this rule will be applied to. Any means all remote hosts.
Active	Indicates whether this rule is enabled or disabled.

Port Triggering

Port Triggering dynamically opens public ports for inbound traffic after certain ports are triggered by a service request.

To view Port Triggering rules:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Firewall.**

The following information is displayed:

Name	The rule's name.
Protocol	The protocol to which the rule is applied: TCP, UDP, or TCP/UDP.
Outgoing Trigger Port	The outgoing port used for this service.
Incoming Trigger Port	The incoming port used for this service.

Active	Indicates whether this rule is enabled or disabled.

1:1 NAT

One-to-one NAT allows a static mapping between an internal IP address and an external IP address.

To configure 1:1 NAT rules:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Firewall.**

   The following information is displayed:

Name	The rule name.
Interface	The WAN interface that this rule should be applied to.
WAN IP	The WAN IP address as the external IP address for translation.
Local IP	The local IP address as the interval IP address for translation.
Protocol	Indicates the associated protocol of this rule: TCP, UDP, or TCP/UDP.
Port	The port used for this traffic type.
Allowed remote IPs	The IP addresses of the remote hosts that this rule will be applied to. Any means to allow all remote hosts.

To configure Firewall rules:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Firewall.**
3. Disable the option **Use Profile configuration.**

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring IPS Settings

To view Intrusion detection and prevention settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security >IPS.**
3. Disable the option **Use Profile configuration.**

If the device is equipped of intrusion detection functions, you can enable or disable the following services:

Intrusion Detection	Enable intrusion detection. And select the WAN and LAN interfaces that the IPS and IDS should be implemented.
Intrusion Prevention	Enable intrusion prevention. And select the WAN and LAN interfaces that the IPS and IDS should be implemented.
Stealth Mode	This mode protects your device from Internet intrusion by not responding to unauthorized requests.
Block TCP Flood	Enable to block TCP flooding to WAN.
Bock UDP Flood	Enable to block UDP flooding to LAN.
Filter Check Mode	Enable the TCP filtering check mode.
Allow ICMP Traffic	Enable to allow packets of Internet Control Message Protocol to pass through.
DoS Attacks	Denial-of-Service (DoS) attacks encompass SYN Flood, ICMP Flood, and Echo storm. Configure the flood rate of each attack in packets/second for detection.

4. Click **Apply** at the top left to apply the settings to the affected devices immediately.

Viewing and Configuring Web Content Filter

The Web Content Filter is used to prevent access to unwanted websites. It allows you to create profiles that can take effective during the designated time frame and block websites belonging to a certain category.

Web Content Filter List

To view the Web Content Filter List:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security >Web Content Filter.**

Under Web Content Filter List, the following is displayed:

Name	The name for the filtering rule.
Policy	State whether this is a allow or block policy.
Schedule	The pre-configured scheduling.
Scope	The specified hosts or the whole network that this rule will be applied to.
Filtering Type	The type consists of a variety of categories, URLs, and custom groups to restrict the access to defined websites.
Active	State whether the rule is active.

Under Custom Warning Page, you can obtain the configured warning page that will display related messages when a restricted webpage is being visited. The following is displayed:

Name	Enter a name for this configuration.
Source Type	The pre-defined warning page to be displayed.
Actions	State whether the rule is active.

Under **Custom Group List**, you can obtain the Custom group which will be used to define the content filtering type above:

Group Name	The name for the custom group.
URLs	If URL filtering is used, it shows the name and keyword for the website. This blocks access to websites based on a website's domain name (e.g. google.com) and keywords with matching

	URLs. For example, keyword "ABC" will block "www.ABC.com" and "xxx.ABC.com" and other URLs containing ABC.
Category Filtering	If Category filtering is used, it shows the pre-defined categories to block access to.
In Use	State whether this rule has been activated.

To configure Firewall rules:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Web Content Filter.**
3. Disable the option **Use Profile configuration.**

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring Application Control

The Application Control is used to restrict certain communication of applications. It allows you to create profiles that can take effective during the designated time frame and prevent traffic of certain applications from being transferred.

Auto Upgrade

Enable automatic upgrade of application signature database and select the update schedule by entering the upgrade frequency in minutes or setting a specified time of a designated weekday for weekly updates.

To add an application control rule:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Application Control.**
3. Under Application Control List, the following information is displayed:

Name	The policy name.
Policy	State whether this is a allow or block policy.
Schedule	The pre-configured schedule. For configured scheduling methods, go to **Configure > Schedule policies**.

Scope	The specified hosts or the whole network that this rule will be applied to.
Application	State whether the filtering rule is based on a single application, or a single application from a pre-defined category, or a custom group of selected applications.
Active	State whether the application control policy is active or inactive.

Under **Custom Group List,** you can obtain Custom Group defined which will be used to define the application type above:

Group Name	The name of the custom group.
Application List	The selected applications for the custom group.
In Use	State whether this rule has been activated.

To configure Application Control:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Application Control.**
3. Disable the option **Use Profile configuration.**

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

VPN Settings

A Virtual Private Network (VPN) builds an encrypted connection between endpoints over a public network utilizing tunneling techniques. VPN can be configured only if your device supports this feature.

Site to Site VPN

The site-to-site VPN is a technique that allows connectivity between the offices located at multiple locations by setting up an IPsec tunnel over the Internet to access the intranet. In short, a site-to-site VPN builds a secure path over an insecure path. The Nuclias cloud gateway allows users to establish a VPN tunnel without manually entering the tunnel endpoint details and the local/remote

networks. Instead, the Nuclias cloud gateway maintains these details and lets users select the networks.

Configuring Quick VPN

Quick VPN is a Nuclias auto-provisioning site-to-site VPN technology that allows you to quickly and easily build VPN tunnels between Nuclias gateway devices without tedious manual VPN configuration. If it is disabled, set up VPN manually at Manual VPN Settings to establish VPN connection with other partners.

To view or configure Quick VPN settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **VPN > Site-to-site VPN**.s
3. Select the topology: Hub-and-Spoke or Full Mesh. If Full Mesh is selected, the VPN establishes the Gateway-to-Gateway IPsec tunnel with other devices registered in the same or different sites of the same organization. To establish a tunnel with a particular remote device, enable the Join member field in the Remote VPN participants table. Once the tunnel configuration is pushed to the remote peers, traffic gets initiated by the user, and a tunnel is established between the remote peers.
4. If Hub-and-Spoke is selected, specify the role to be either a hub or spoke. If Spoke is selected, you can choose hubs to build VPN tunnels in the Exist hubs table. In addition, it lists the Exist hub devices available with the option of Primary Hub. If you enable the Primary Hub field, the selected hub will be the primary hub for the spoke and can communicate to all the spoke devices linked to this hub. At a time, you can enable only one primary hub. If Hub is selected, then VPN tunnels will be built among hubs and dependent spokes.
5. If Hub mode is selected, enable or disable VPN connection with a remote peer. You may also choose to designate a remote peer as a backup hub.
6. If Spoke mode is selected, you can choose to designate a remote peer as the primary hub.
7. Click **Apply**.

Quick VPN Settings

In the Local networks section, if you have multiple subnets, you can specify which one subnet participates in the VPN, i.e., traffic from the enabled subnet will be encrypted by the IPsec VPN. All local subnets must be unique within the VPN topology

Note: A list of Quick VPN connections will be displayed in the **Summary > VPN Status** page. Select Quick VPN (Full Mesh and Hub-and-Spoke) as the Display VPN type.

Configuring Manual VPN

To view or configure Manual VPN settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **VPN > Site-to-site VPN**. Enter the following:

Connection Name	Enter a name for this VPN connection (1-64 characters).
IKE Profile	Select the IKE profile which contains security settings that will be used for the VPN connection.
Local Network	The scope of the local network to which the VPN connection will apply.
Local Network	Enter a local IP address or subnetwork of the local network to participate in the VPN. If Single IP is selected, enter the IP address. If Subnet is selected, enter the IP address and subnet mask (or prefix for IPv6). Select Any for the entire local network.
Remote Network	Enter a remote IP address or subnetwork of the remote network to participate in the VPN. If Single IP is selected, enter the IP address. If Subnet is selected, enter the IP address and subnet mask (or prefix for IPv6). Select Any for the entire remote network.
Outgoing Interface	Select an interface to which the VPN connection will use.
Remote Gateway	Select FQDN or Static IP for configuring the remote gateway address. Then enter the IP address or FQDN address.
Keep-alive	Enable or disable keep-alive for VPN reconnection. If enabled, enter the source and destination IP address as well as the detection period in seconds (10-199) and retry after the number of failures (3-99).
Idle Timeout	Enter the maximum length of time that the VPN connection can stay active when three is no traffic.
Dead Peer Detection	Enable detection for dead peers. If enabled, enter the detection interval (10-999 seconds) and Retry after failure (3-99 times).
NetBIOS Broadcast	Enable or disable NetBIOS broadcast from one end to be forwarded to the other end of the VPN connection.

Outgoing Backup Interface	Select an interface to which the VPN connection will use as a backup if Dead Peer Detection is enabled.
Remote Backup Gateway	Select FQDN or Static IP for configuring the remote gateway address if Dead Peer Detection is enabled.
IKE Backup Profile	Select the IKE profile which contains security settings that will be used for the backup VPN connection if Dead Peer Detection is enabled.

To add an IKE profile,enter the following:

Profile Name	Enter a name for this IKE profile.
IKE Version	Select the IKE version: v1 or v2.
IKE phase-1 Settings	
Exchange Mode	Select the exchange mode: Aggressive or Main.
Local Identifier Type	Select the identification method: Local WAN IP, FQDN, or User-FQDN. And enter the identifier according to the selected method.
Remote Identifier Type	Select the identification method: Remote WAN IP, FQDN, or User-FQDN. And enter the identifier according to the selected method.
DH Group	Select a Diffie-Hellman (DH) Group for key exchange. These groups vary in prime key lengths.
Encryption Algorithm	Select encryption algorithm(s) for ESP packets encryption.
Authentication Algorithm	Select authentication algorithm(s). And enter the SA lifetime in seconds (300-604800).

Authentication Method	Select the authentication method. Then enter the preshared key or select a certificate depending on the method selected. Go to **Settings > Certificate Management** for Certificate list.
Extended Authentication	Enable this and select extended authentication method: Authentication server, IPsec host, or Local authentication. Depending on the method, select the corresponding RADIUS/ LDAP/POP3/Active Directory/NT Domain server or Local Authentication profile or enter the username and password for IPsec host. Refer to **Configure > Authentication > Local Authentication list** and **Authentication servers** for Authentication profiles and servers.
IKE phase-2 Settings	
Protocol Selection	Select either ESP or AH. If Encapsulating Security Payload (ESP) is selected, select the Encryption algorithm to encrypt or decrypt ESP packets.
Authentication Algorithm	Select the authentication algorithm for header packets validation.
SA Lifetime (sec.)	Enter the SA lifetime (300-604800 seconds) for the active duration of a VPN tunnel.
Perfect Forward Secrecy	Enable or disable the Perfect Forward Secrecy. If enabled, the VPN communication is better protected with renewed negotiation of key values in the exchange.
DH Group	If the above PFS is enabled, select the DH group for key establishment.

3. Click **Apply** at the top.

Note: A list of Quick VPN connections will be displayed in the **Summary > VPN Status** page. Select Quick VPN (Manual) as the Display VPN type.

Client to Site VPN

An IPsec policy can be defined between this router and another gateway to create network-to-network IPsec tunnels. To configure IPsec VPN Server settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **VPN > Client-to-site VPN**. Enter the following:

Connection Name	Enter a name for this configuration
IKE	Select a pre-configured IKE profile for this VPN configuration.
Local Network	Enter the IP address and subnet mask of the local network. Select Any to not restrict to a single subnet.
Tunnel Mode	Select either full or split tunnel for the mode. Select Full tunnel or Split tunnel. The Split mode will split DNS requests among DNS servers. It allows you to create two zones for the same domain, one to be used by the internal network, the other used by the external network .For Split tunnel, enter the Split Domain names.
DHCP Relay	Enable or disable DHCP relay. If enabled, enter the IP address of the relay gateway. If disabled, enter the following IP address information.
Starting IP Address/ Ending IP Address	Enter the range of the IP addresses for VPN connections.
Primary/Secondary DNS	Enter the primary and optional secondary DNS servers.
Primary WINS Server/ Secondary WINS Server	Enter the primary and optional secondary Windows Internet Naming Service (WINS) servers.
Outgoing Interface	Select the WAN interface to which the IPsec VPN should apply.
Split DNS	Enable or disable Split DNS if Split tunnel is selected. And enter the domain names if enabled (3-253 characters).
NetBIOS Broadcast	Enable or disable NetBIOS information to be forwarded to the other endpoint of the VPN tunnel. The information is used for name resolution in Windows networking.

To add an IKE profile, enter the following:

Profile Name	Enter a name for this IKE profile.
IKE Version	Select the IKE version: v1 or v2.
IKE phase-1 Settings	
Exchange Mode	Select the exchange mode: Aggressive or Main.
Local Identifier Type	Select the identification method: Local WAN IP, FQDN, or User-FQDN. And enter the identifier according to the selected method.
Remote Identifier Type	Select the identification method: Remote WAN IP, FQDN, or User-FQDN. And enter the identifier according to the selected method.
DH Group	Select a Diffie-Hellman (DH) Group for key exchange. These groups vary in prime key lengths.
Encryption Algorithm	Select encryption algorithm(s) for ESP packets encryption.
Authentication Algorithm	Select authentication algorithm(s). And enter the SA lifetime in seconds (300-604800).
Authentication Method	Select the authentication method. Then enter the preshared key or select a certificate depending on the method selected. Go to **Settings > Certificate Management** for Certificate list (refer to Certificate Management) .
Extended Authentication	Enable this and select extended authentication method: Authentication server, IPsec host, or Local authentication. Depending on the method, select the corresponding RADIUS/ LDAP/POP3/Active Directory/NT Domain server or Local Authentication profile or enter the username and password for IPsec host. Refer to **Configure > Authentication > Local Authentication list** and **Authentication servers** for Authentication profiles and servers.

IKE phase-2 Settings	
Protocol Selection	Select either ESP or AH. If Encapsulating Security Payload (ESP) is selected, select the Encryption algorithm to encrypt or decrypt ESP packets.
Authentication Algorithm	Select the authentication algorithm for header packets validation.
SA Lifetime (sec.)	Enter the SA lifetime (300-604800 seconds) for the active duration of a VPN tunnel.
Perfect Forward Secrecy	Enable or disable the Perfect Forward Secrecy. If enabled, the VPN communication is better protected with renewed negotiation of key values in the exchange.
DH Group	If the above PFS is enabled, select the DH group for key establishment.

3. Click **Apply** at the top.

PPTP/L2TP

A PPTP server is available on the router for LAN and WAN PPTP client users to access.

To configure PPTP/L2TP Server settings

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **VPN > PPTP/L2TP**. Enter the following:

Name	Enter a name for the configuration profile of the server (1-64 characters).
Server Type	Select either PPTP or L2TP.
Routing Mode	Select either NAT or Router.
Starting IP Address/ Ending IP Address	Enter the LAN IP address range to be assigned to the VPN clients.

Authentication Server	Select the authentication server. Depending on the method, select the corresponding RADIUS/LDAP/POP3/Active Directory/NT Domain server or Local Authentication profile. Go to **Configure > Authentication > Local Authentication list** and **Authentication Servers** for Local authentication profiles and authentication servers list.
Authentication Protocol	Select the authentication protocol(s): All, PAP, CHAP, MS-CHAP, and MS-CHAPv2.
Encryption	[PPTP only] Select the encryption method(s) for PPTP: For PPTP, select All, MPPE 40 bit, MPPE 128 bit, or Stateful MPPE. The Microsoft Point-to-Point (MPPE) encrypts data for PPTP VPN.
Idle Timeout	The length of time (seconds) to wait before terminating a VPN session (300-1800).
NetBIOS	[PPTP only] Enable or disable NetBIOS, which is used for name resolution in Windows networking, if there is a WINS server set up in your LAN. If enabled, enter the Windows Internet Naming Service (WINS) server IP address. This option is only available for PPTP.
Enable Secret Key	[L2TP only] Enable or disable the secret key (or preshared key) with 8-63 characters which will be required for client VPN settings.
L2TP over IPsec	[L2TP only] Enable or disable L2TP over Internet Protocol Security (IPsec), on which L2TP relies for secure packets exchange.
IKE Version: Configure Internet Key Exchange (IKE) if L2TP Over IPsec is enabled.	
IKE version	Select the IKE version for configuration.
IKE phase-1 settings	
Exchange Mode	Select the exchange mode: Aggressive or Main.
Local Identifier Type	Select the identification method: Local WAN IP or FQDN. And enter the identifier according to the selected method.

Remote Identifier Type	Select the identification method: Remote WAN IP or FQDN. And enter the identifier according to the selected method.
DH Group	Select a Diffie-Hellman (DH) Group for key exchange. These groups vary in prime key lengths.
Encryption Algorithm	Select encryption algorithm(s) for ESP packets encryption.
Authentication Algorithm	Select authentication algorithm(s). And enter the SA lifetime in seconds (300-604800).
Authentication Method	Select the authentication method. Then enter the preshared key or select a certificate depending on the method selected. Go to **Settings > Certificate Management** for Certificate list.
Extended Authentication	Enable this and select extended authentication method: Authentication server, IPsec host, or Local authentication. Depending on the method, select the corresponding RADIUS/ LDAP/POP3/Active Directory/NT Domain server or Local Authentication profile or enter the username and password for IPsec host. Refer to **Configure > Authentication > Local Authentication list** and **Authentication servers** for Local authentication profiles and authentication servers.
IKE phase-2 settings	
Protocol Selection	Select either ESP or AH. If Encapsulating Security Payload (ESP) is selected, select the Encryption algorithm to encrypt or decrypt ESP packets.
Authentication Algorithm	Select the authentication algorithm for header packets validation.
SA Lifetime (sec.)	Enter the SA lifetime (300-604800 seconds) for the active duration of a VPN tunnel.
Perfect Forward Secrecy	Enable or disable the Perfect Forward Secrecy. If enabled, the VPN communication is better protected with renewed negotiation of key values in the exchange.

DH Group	If the above PFS is enabled, select the DH group for key establishment.

PPTP VPN Client can be configured on this router to access a remote network.

To configure a VPN client,enter the following:

Name	Enter a name for the PPTP/L2TP configuration profile of the client (1-64 characters).
Client Type	Select either PPTP or L2TP.
VPN Server	Enter the IP address or FQDN of the VPN server
Tunnel Type	Select Full tunnel or Split tunnel. Split tunnel mode only sends traffic to the private LAN with pre-specified client routes and give the client access to specific private networks, thereby allowing access control over specific LAN services.
Remote Network/ Netmask	Enter the remote network and netmask if split tunnel is selected.
Username/Password	Enter the username and password required for connection.
Encryption	For L2TP server, enter the Secret key (8-63 characters) if encryption is enabled. This value must match the preshared key value entered on the VPN server.
MPPE	Enable the Microsoft Point-to-Point Encryption (MPPE), which encrypts data for VPN communication.
Idle Timeout	For PPTP, enter the length of time (seconds) to wait before terminating a session.
Reconnect Mode	For L2TP, select On demand or Always on. Enter the Maximum idle time in seconds (300-1800) to wait before dropping an idle connection.

L2TP over IPsec	Enable or disable L2TP over Internet Protocol Security (IPsec), on which L2TP relies for secure packets exchange.
IKE Version: Configure Internet Key Exchange (IKE) if L2TP Over IPsec is enabled.	
IKE version	Select the IKE version for configuration.
IKE phase-1 settings	
Exchange Mode	Select the exchange mode: Aggressive or Main.
Local Identifier Type	Select the identification method: Local WAN IP or FQDN. And enter the identifier according to the selected method.
Remote Identifier Type	Select the identification method: Remote WAN IP or FQDN. And enter the identifier according to the selected method.
DH Group	Select a Diffie-Hellman (DH) Group for key exchange. These groups vary in prime key lengths.
Encryption Algorithm	Select encryption algorithm(s) for ESP packets encryption.
Authentication Algorithm	Select authentication algorithm(s). And enter the SA lifetime in seconds (300-604800).
Authentication Method	Select the authentication method. Then enter the preshared key or select a certificate depending on the method selected. Go to **Settings > Certificate Management** for Certificate list.
Extended Authentication	Enable this and select extended authentication method. Enter the Username and Password if IPsec host is selected.
IKE phase-2 settings	
Protocol Selection	Select either ESP or AH. If Encapsulating Security Payload (ESP) is selected, select the Encryption algorithm to encrypt or decrypt ESP packets.

Authentication Algorithm	Select the authentication algorithm for header packets validation.
SA Lifetime (sec.)	Enter the SA lifetime (300-604800 seconds) for the active duration of a VPN tunnel.
Perfect Forward Secrecy	Enable or disable the Perfect Forward Secrecy. If enabled, the VPN communication is better protected with renewed negotiation of key values in the exchange.
DH Group	If the above PFS is enabled, select the DH group for key establishment.

3. Click **Save**.

Note: A list of PPTP/L2TP connections will be displayed in the **Summary > VPN Status** page.

OpenVPN

OpenVPN allows peers to authenticate each other using certificates, or username/password. When used in a multiclient-server configuration, it allows the server to release an authentication certificate for every client, using signature and Certificate authority. An OpenVPN can be established through this router.

To configure OpenVPN settings

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **VPN > OpenVPN**. Enter the following:

Mode	Select the mode for the OpenVPN: Server, Client, or Access server client.
Upload Access Server Client	[Access Server Client mode only] Upload a configuration file which contains server and client IP address information if Access server client mode is selected. In access server client mode, the user has to download the auto login profile from the OpenVPN Access Server and upload the same to connect.
CRL Certificate	[Access Server Client mode only] Openvpn provides CRL authentication using CRL certificate. You can upload the required certificates by enabling it it first.

VPN Network/Netmask	[Server mode only] Enter the network IP address/netmask of the VPN. This is only available for the Server mode.
Server IP/Failover Server IP	The IP address or FQDN of the VPN server and failover server. This is only available for the Client mode.
Duplicate CN	[Server mode only] Enable or disable the duplicate CN to allow or disallow the same certification for multiple clients. This is only available for the Server mode.
Port	Enter the port number for VPN communication. The default is 1194.
Tunnel Protocol	Select the protocol for tunneling: TCP or UDP.
Encryption Algorithm	Select the encryption method: AES-128, BF-CBC, AES-192, or AES-256.
Hash Algorithm	Select the hash algorithm: SHA1, SHA256, or SHA512.
Tunnel Type	[Server mode only] Select the tunnel type: Full or Split. If Split is selected, enable or disable the client-to-client communication. Full Tunnel mode sends all traffic from the client across the VPN tunnel to the router. Split Tunnel mode only sends traffic to the private LAN with specified client routes. This is only available for Server mode configuration.
User-based Authentication	Enable or disable user-based authentication. If this is enabled, select the user profiles for Local authentication if server mode is used (refer to Local Authentication). If client mode is used, enter the username and password for VPN connection. Also select a certificate for TLS key if TLS authentication is used (refer to Certificate Management).
Certificate Verification	Enable or disable the use of certificate for verification.
Certificate	Select an available certificate from the list. The content of the certificate will be loaded in the field below.

TLS Authentication Key	Enable or disable the TLS authentication. If enabled, select an TLS authentication key from the certificate list. To obtain the certificate list, go to **Settings > Certificate Management**.
DH Key	Select a DH key from the certificate list. This is only available for Server mode configuration. To obtain certificate list, go to **Settings > Certificate Management**
Server Policies	Enable or disable the server policy. Enter the server policy and add a new server policy to permit or block networks for VPN connections. These policies can be applied to a specific IP address or IP networks on the LAN and can be enforced on the specified scope according to the supported features of the router. The List of Available Policies can be filtered based on whether it applies to a user, group, or all users (global). To add a new server policy, enter the following: Policy name: Give a name for this policy. Policy: Select whether it is a Deny or Permit policy. Scope: Select whether it is a global policy or to be applied for certain users using Local authentication. Select the user profile if Local authentication is selected. Apply policy to: Select whether to apply this policy to a single IP address or a subnet work and enter the required IP address and/or the Subnet mask and the port number. ICMP: enable or disable Internet Control Message Protocol (ICMP) traffic in VPN connections.
Remote Networks	If this is enabled, click Add to add a remote network configuration: enter a name for the configuration and the remote network IP address and subnet mask.
Port	Enter the port number (1-65535). This can be a single port or a range of ports, e.g. 3000-3200.
ICMP	Enable or disable the use of ICMP in the VPN communication.

OpenVPN provides authentication using certificates. This system will allow you to configure client list using **Local Authentication list (refer to Local Authentication)** and centrally manage the client certificates (refer to Certificate Management).To configure Client list for Server mode configuration:

1. Under Client list, click **Import**. The **Import users from local authentication list** page displays.
2. Select a pre-configured local user profile or click **Add local authentication** and configure a local user profile by specifying the following: the Local Authentication profile name, the Access level, Managed Sites, and the username and password for each new user. You can use the Bulk import function to upload a CSV file containing the user information to add multiple users at once. Refer to **Configure > Authentication > Local Authentication list** for more information.
3. Click **Save.** Once a Local authentication profile is imported successfully, you can manage the clients' certificates in the Certificate Management page (go to **Settings > Certificate management**) .

To configure OmniSSL Portal Layout for Server mode configuration:

OmniSSL facilitates the client installation from the device via the instructions on the portal page and is an enhancement to the existing OpenVPN. The enhancements allow the VPN tool to be used via mobile devices and eliminate browser and Java dependencies.

1. Under OmniSSL Portal Layout, click **Add**. The **Add portal layout configuration** page displays.
2. Enter a name for the profile and select a pre-defined login page for OmniSSL. Refer to **Configure > Splash pages** for more information. The Splash pages allow you to create a custom page that is presented upon authentication to the remote OmniSSL users.
3. Click **Save.**

Note: A list of OpenVPN connections will be displayed in the **Summary > VPN Status** page.

GRE Tunnel

GRE tunnels allow for broadcast traffic on the LAN of the router to be passed over the internet and received by remote LAN hosts.

To view or configure GRE Tunnel settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **VPN > GRE Tunnel**. Enter the following:

Name	The name for the GRE Tunnel configuration.

Interface	Select the WAN interface to create this tunnel with from the drop-down menu.
GRE Tunnel IP/ Subnet Mask	Enter the IP address/subnet mask of this endpoint. It will be referenced in the other router's static route as the Gateway IP address.
Remote IP	Enter the WAN IP address of the endpoint router.
Static Route Configuration	IP address/Subnet mask: Enter the destination IP address/subnet mask of the static route from the remote LAN subnet. Gateway IP address: Enter the GRE tunnel IP of the terminating router that manages the remote LAN.

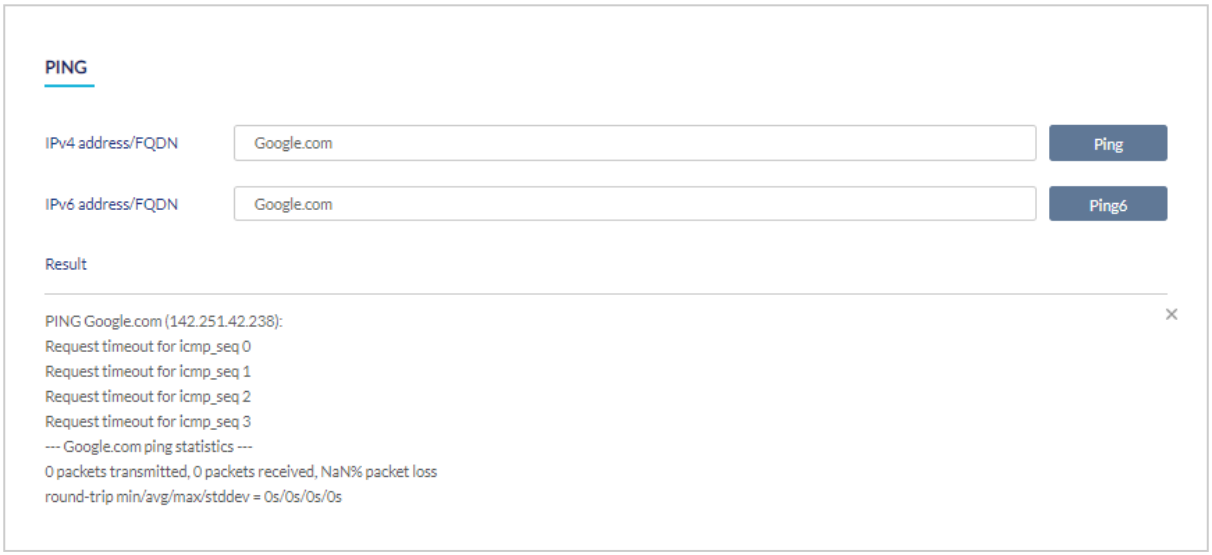
3. Click **Save.**
4. Click **Apply** at the top left to apply the settings to the affected device immediately.

Note: The GRE connection status will be displayed in the **Summary > VPN Status** page.

Tools

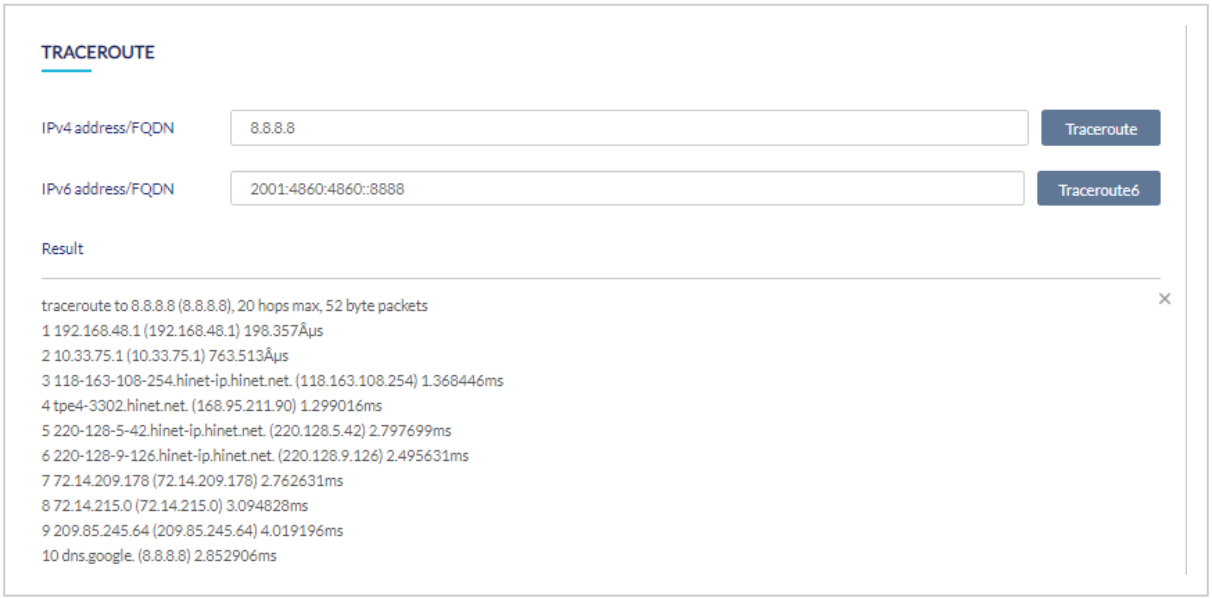
Performing a Device Ping Test

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Tools** tab in the top-right of the screen.
3. In the IPv4 or IPv6 address/FQDN field in the Ping section, enter a valid IP address or FQDN.
4. Click **Ping** for IPv4 addresses or **Ping6** for IPv6 addresses of the remote hosts. The results will be displayed as shown below:



Performing a Traceroute Test

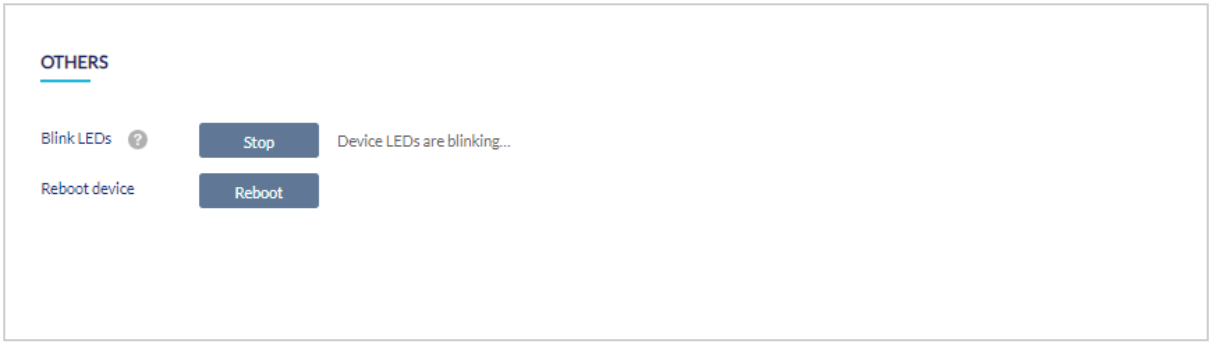
1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Tools** tab in the top-right of the screen.
3. Under Traceroute, enter a valid IP address or FQDN in the IP address/FQDN field.
4. Click **Traceroute** for IPv4 addresses or **Traceroute6** for IPv6 addresses of the remote hosts. The results will be displayed as shown below:



Performing LED Blinking and Device Reboot

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Tools** tab in the top-right of the screen.

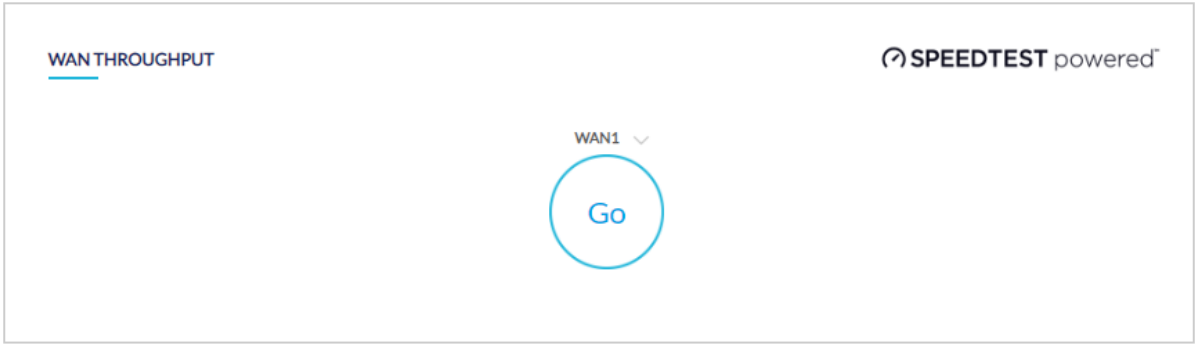
3. In the Others section, click **Reboot** to reboot the device. Or click **Start** to start blink LEDs on the device. Click **Stop** to top blinking LEDs.



Note: Please refer to the respective device's manual for the status of LED indicators.

Performing WAN Throughput Test

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Tools** tab at the top right of the screen.
3. In the WAN Throughput section, click **Go**. The upload and download speed will be displayed.



Exporting or Importing Device Settings

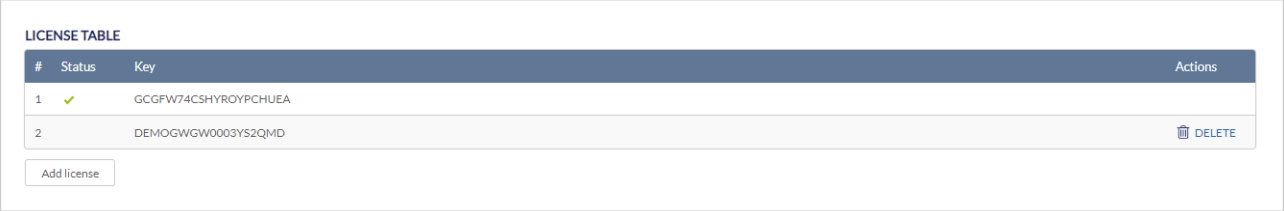
The device setting metadata can be exported as a single CSV file and it can be later imported for configuration restoration. To export device settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Tools** tab at the top right of the screen.
3. In the Export and Import Device Settings section, click **Download**. The exported file will be downloaded to your browser's default download folder.

License

Adding a License Key to a Device

1. Navigate to **Monitor > Gateway > Devices** 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 > Gateway > Devices** 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 reclassify it as Unused in the license management inventory.

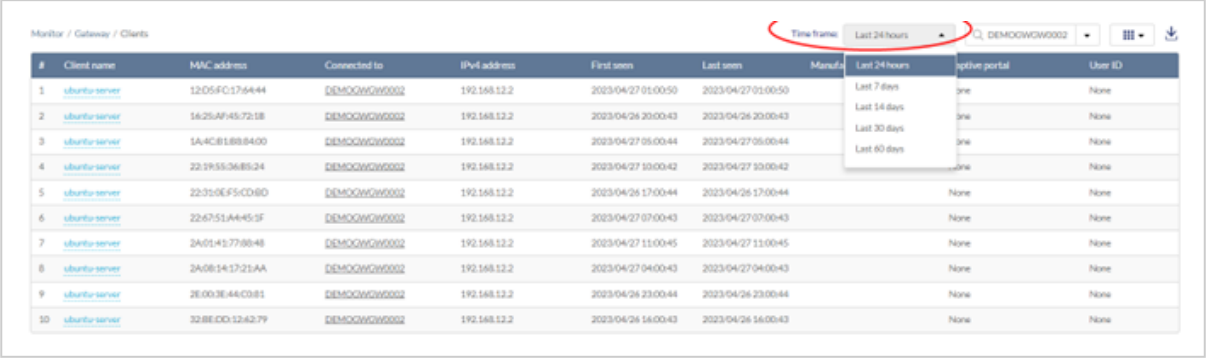


Clients

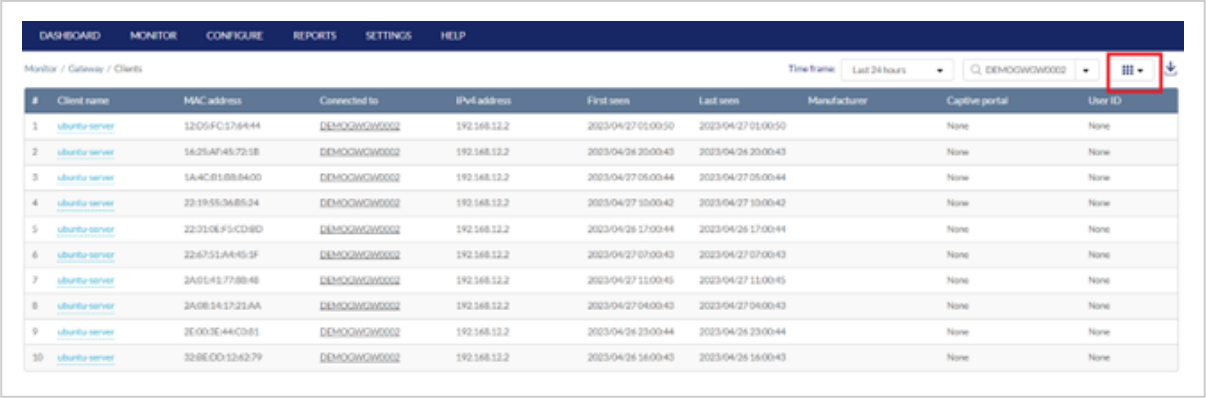
From the Clients window, you can consult a detailed overview of all currently connected devices with additional information including status, VLAN, and general settings.

Customizing the Client Monitor Overview

1. Navigate to **Monitor > Gateway > Clients**. The client list for all gateways will appear.
2. Select a time frame from the drop-down menu to define the time frame that the device was detected online.



3. Click the parameter filter icon.

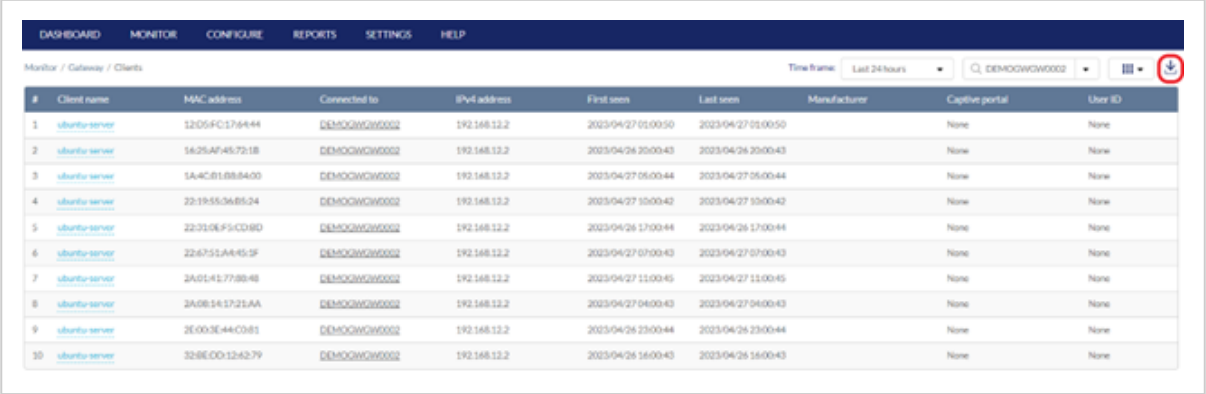


4. Click the checkbox next to the parameters to display them in the table listing.
   Note: All checked parameters will automatically appear.

Downloading Client Monitoring Logs

1. Navigate to **Monitor > Gateway > Clients**.

2. From the client monitoring logs, click the download icon in the top-right.



Event Log

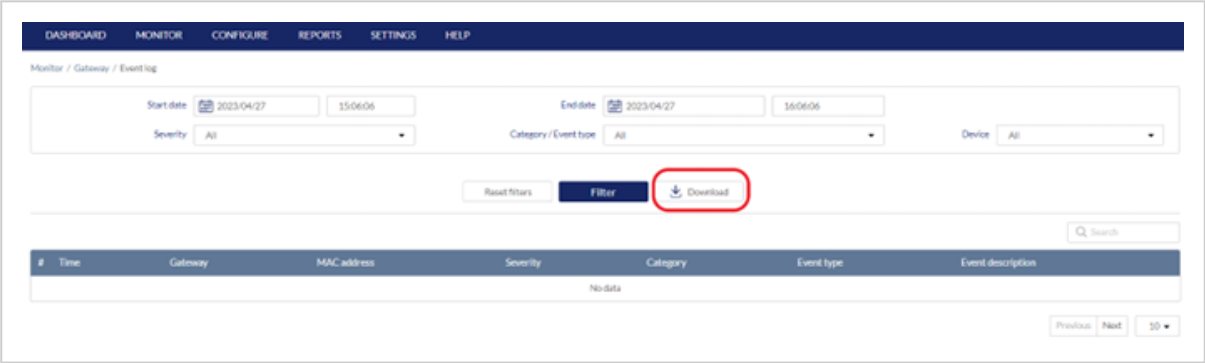
From the Event Logs window, you can consult a detailed log of events occurring on the network. You can also define event filter parameters, including event type and time period.

Filtering Event Log Parameters

1. Navigate to **Monitor > Gateway > Event Log**.
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 Category/Event type drop-down menu and select the event types to display. Select All to show all event types.
6. Click the Device drop-down menu and select a device to filter the results. Select All to show all event logs for all devices.
7. Click **Filter** to display all events matching the defined parameters. Click **Reset filters** to reset all currently set parameters.

Downloading Event Logs

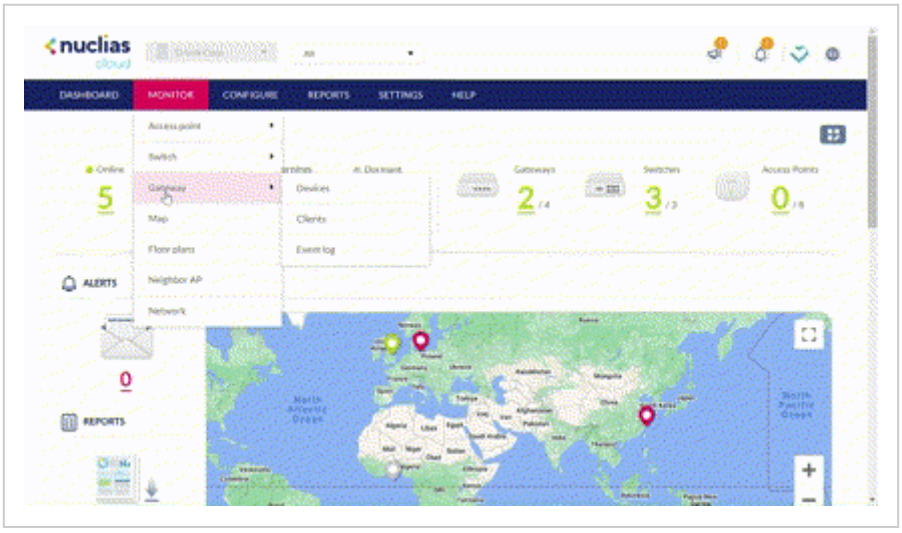
1. Navigate to **Monitor > Gateway > Event Log**.
2. From the event log list, click **Download**.


DASHBOARD
MONITOR
CONFIGURE
REPORTS
SETTINGS
HELP
Monitor / Gateway / Event log
Start date
2023/04/27
15:06:06
End date
2023/04/27
16:06:06
Severity
All
Category / Event type
All
Device
All
Reset filters
Filter
Download
Search
Time
Gateway
MAC address
Severity
Category
Event type
Event description
No data
Previous
Next
10

Devices

Devices

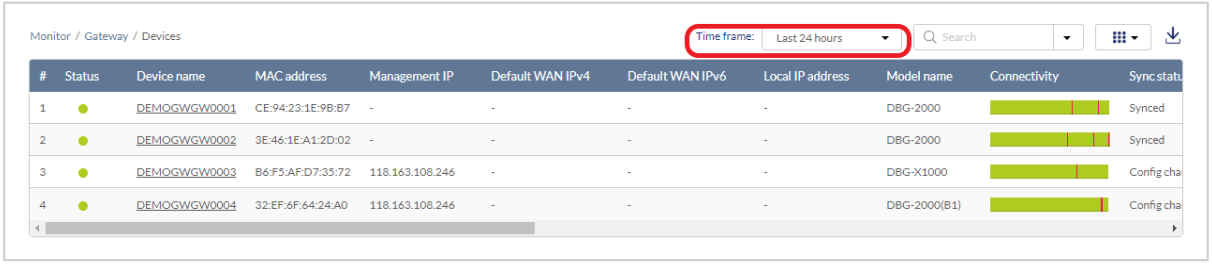
From the Devices window, you can consult a detailed log of events occurring on the network. You can also filter events using specific event filter parameters, including event type and time period.



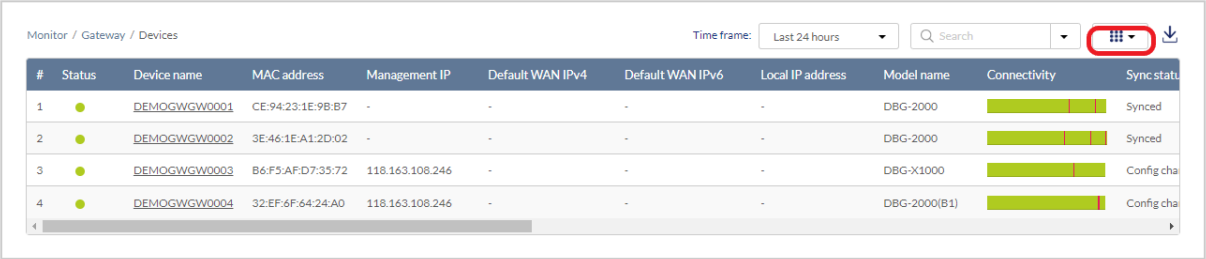
The Device Monitor

Customizing the Device Monitor Overview

1. Navigate to **Monitor > Gateway > Devices**.
2. Select a time frame from the drop-down menu to set the duration for connectivity information.



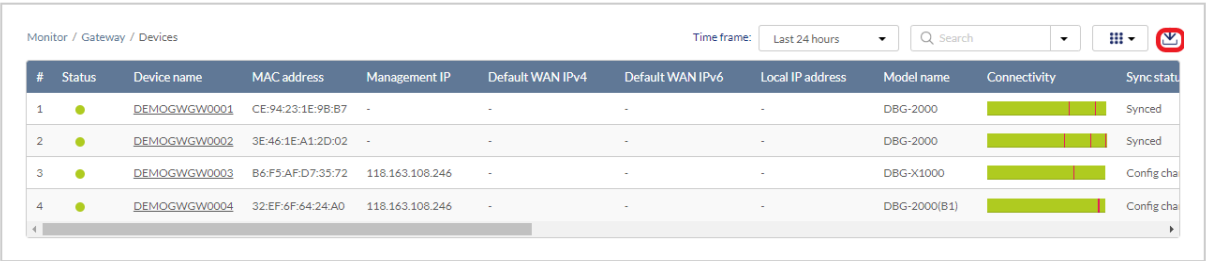
3. Click the filter parameter icon.



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

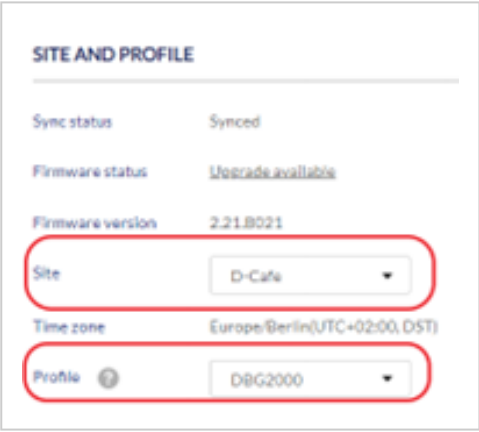
1. Navigate to **Monitor > Gateway > Devices**.
2. From the device list, click the **Download** icon in the top-right to export the table listing as a CSV file.



Device Basic Settings

Changing the Device Site and Profile

1. Navigate to **Monitor >Gateway > Devices** and select a device from the list.
2. Select the **Basic** tab at the top.
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 **Save**.

The Performance Summary

Viewing and Customizing the Gateway Performance Summary

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Summary** tab. Click the tabs at the top to obtain additional information described below:

Status	Provides connection information for the device along with basic port configuration and traffic statistics for each port. You can also obtain Internet usage for both download and upload data in a specified time frame.
Statistics	Provides reports of the number of connected clients in the selected time frame. You can also obtain reports of WAN port usage and the whole Internet usage as well as VPN usage.
DHCP	Provides the utilization rate of each configured DHCP subnet. It also lists the DHCP leases history.
VPN Status	Provides VPN connection statistics. The page lists the active VPN association or connections, the traffic details, and the tunnel state. You can view the status (connect or disconnect) of the gateway's VPN connections as a whole (by selecting Overview for the Display VPN type) or view each VPN separately.

Network Settings

Verifying and Changing the Default WAN Configuration

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Network** tab at the top.
3. Under **WAN Mode Configuration**, verify the WAN mode and the primary WAN port (or Default WAN Configuration) settings. Note that the settings or configurations here depend on the device model and firmware.

To change the Default WAN or WAN Mode Configuration:

1. Disable the option **Use Profile configuration** first at the top of the configuration page to allow changes.
2. Select IPv4 and IPv6 default WAN configuration. Or select a WAN mode from the available options. For **Primary WAN**, designate a WAN port as the primary WAN. For **Auto-rollover using WAN**, select both Primary and Secondary WAN ports as well as the **Health Check** method. For DNS servers and Ping IP address methods, enter the

respective server IP address as the destination to check the connectivity. Also enter the **Retry interval** (seconds) and **Failover after** (number of failed retries). For Load balancing, select the method (either Round robin or Spillover mode).

3. For **Round robin**, configure the Health check method (or none) and enter the **Retry interval** (seconds) and **Failover after** (number of failed retries). Hence, if a WAN interface disconnects, only the alternate WAN ports will transfer traffic flows in a round robin manner. For **Spillover**, enter the **Load tolerance** (%) and **Max bandwidth** (Mbps) as the threshold value. Once the threshold is exceeded, new traffic flows will be allocated to the alternate WAN interfaces. The precedence for selection is based on the configuration of Primary, Secondary, and Tertiary WAN interface.
4. Click **Apply**.

Note: The WAN mode can be configured using Profiles. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Using Dynamic DNS

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Network** tab at the top.
3. Under **Dynamic DNS**, enable or disable the service.
4. > Click **Apply**.

To add a DDNS service:

1. Disable the option Use Profile configuration first at the top of the configuration page.
2. Click **Add**. Enter the following information:

WAN Interface	Select the WAN interface for configuration
Service Provider	Select the DDNS service provider.
Username/Password	Enter the DDNS account name and password.
Hostname	Enter the registered hostname with the DDNS service.
Wildcard	Enable or disable the wildcard option which will resolve *.hostname to the same designated IP address.
Use Public IP	Enable or disable the use of a public IP address.
Force Update Interval	Enter the DDNS update interval (days).

3. Click **Save** to close the screen. Then click **Apply**.

Using IP Alias for the WAN

Note: The IP Alias function is only available on supported models.

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Network** tab at the top.

3. Under **IP Aliasing** , click **Add** to bind one or multiple IP addresses to a WAN interface.

   Enter the following information:

WAN Interface	Select the WAN interface for configuration
IP Address/Subnet Mask	Enter the IP address and subnet mask to bind to the WAN interface.

4. Click **Save** to close the screen. Then click **Apply**.

Viewing and Customizing the Gateway Port Status Overview

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Summary** tab at the top. The ports of the gateway device are displayed along with their detailed information shown in the table below:

Port Number	Numbering of the ports on the connector panel.
Interface Name	The name that identifies the port.
Port Status	Displays the link state of the port.
MAC Address	The MAC address of the port.
IP Address/ Subnet Mask	The IP address and subnet mask assigned to the port
Gateway	The gateway IP address if it has been assigned.
DHCP Mode	Displays if DHCP service has been enabled on the device.
Sent Bytes	The amount of data sent out of the port (bytes).
Received Bytes	The amount of data received through the port (bytes).

Total Bytes	The total amount of sent and received data volume (bytes).

To configure a port's basic settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Network** tab at the top.
3. Disable **Use Profile Configuration** to allow modification.
4. Under **Port Configuration** , select a port and click **EDIT** under Actions. Specify the following information for the selected LAN port:

Interface Type	Select the connection type: LAN, WAN, or DMZ.
Interface Name	Enter a name to identify this interface.
Bridge Network	Enable or disable bridging with another network. Configure the interface with more settings below if bridging is not enabled.
IP Address/ Subnet Mask	Enter an IP address with subnet mask.
DHCP Mode	Enable or disable DHCP service for IP address assignment.
DHCP Server	Enter the following information if DHCP server is selected. Domain name: Assign a domain name for DHCP service. Starting IP address/Ending IP address: Enter the range of IP addresses that can be assigned dynamically. Default gateway: Assign a default gateway for DHCP service. DNS server: Configure DNS by specifying a static DNS server, DNS setting from the ISP, or using DNS proxy. For static DNS, enter the DNS servers or WIN server IP address. Lease Time: Enter a time value of 1 to 10080 minutes.

Allow Ping from LAN	Enable or disable ping command executed from this port.
DHCP Relay	Enter the remote DHCP server address if DHCP relay is selected.
DNS Proxy	Enable or disable DNS proxy.

For a WAN port (if the device supports this feature), configure the following:

Interface Type	Select the connection type: LAN, WAN, or DMZ.
Connection Type	Select the connection method: DHCP, Static IP, PPPoE, PPTP, or L2TP. For Static IP, enter the IP address/Subnet mask, Gateway IP address and Primary/Secondary DNS servers, and specify whether to keep the original MAC address as well as the MTU size. For PPPoE, select the Address mode: Dynamic IP or Static IP. For static IP, enter the IP address/Subnet mask and PPPoE connection Username and Password. Then specify the Authentication type from one of the following: None, MS-CHAPv2, MS-CHAP, CHAP, PAP, or Auto-negotiate. For Dynamic IP, you don't need to enter the IP address/subnet information but configure all other settings as specified above. For both addressing modes, enter the Service name (optional) and select the Reconnect mode: Always on, or On demand (enter the Maximum idle time to wait before terminating the connection in minutes for this option). Then configure the DNS servers and specify whether to keep the original MAC address as well as the MTU size. For PPTP, if Static IP is selected, enter the following IP address information: IP address/Subnet mask, Gateway IP address, and Static DNS IP address. For both Address modes, enter the PPTP server name and connection Username and Password. For both modes, configure whether MPPE (Microsoft Point-to-Point Encryption (MPPE) will be used and the Reconnect mode: Always on or On demand (enter the Maximum idle time to wait before terminating the connection in minutes for this option). Then configure the DNS servers and specify whether to keep the original MAC address as well as the MTU size. For L2TP, if Static IP is selected, enter the following IP

	address information: IP address/Subnet mask, Gateway IP address, and Static DNS IP address. For both Address modes, enter the L2TP server name and connection Username and Password. For both modes, enter the Secret (optional) and configure the Reconnect mode: Always on or On demand (enter the Maximum idle time to wait before terminating the connection in minutes for this option). Then configure the DNS servers and specify whether to keep the original MAC address as well as the MTU size.
Advanced Settings	Enable or disable the following passthroughs: **Internet Protocol Security (IPsec)** which is used for securing packets exchange at the IP layer. **Point-to-Point Tunneling Protocol (PPTP)** which is used for tunneling the Point-to-Point Protocol (PPP) communication in an IP network. **Layer 2 Tunneling Protocol (L2TP)** which is used for implementing Point-to-Point sessions utilizing multipoint tunneling technique.

5. Click **Save**. Then click **Apply** to apply the settings to the affected device immediately.

Viewing and Configuring VLANs

VLANs allow you to divide the network to different segments. To obtain the current VLAN settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Addressing.** The VLANs are displayed under the VLAN section with the following information:

Name	A name that helps identify this VLAN.
VLAN ID	The assigned VLAN ID.
Untagged/Tagged Ports	The member ports for the untagged VLAN and tagged VLAN .

IP address/Subnet Mask	The IP address/Subnet mask configured for the VLAN.
Captive Portal	The associated Captive Portal page.

To configure a VLAN:

1. Disable the **Use Profile configuration** option.
2. Under **VLAN**, click **Add** to add a new VLAN.
3. Click Apply at the top left to apply the changes to the affected device immediately.

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring IP Management List

The IP Management list displays the IP assignment of the DHCP clients:

Host Name	The host name of the client device.
Interface	The associated interface with the IP assignment.
IP Address	The assigned IP address of the host.
MAC Address	The MAC address of the host.
IPv6 Suffix	The assigned IPv6 suffix, which is the the last 64 bits of an IPv6 address.
IP-MAC Binding	Indicates whether the IP assignment is enforced on the client device with the specified MAC address to prevent the use of other static IP address on this client.
DHCP IP Reservation	Indicates whether this IP assignment is reserved for this client so that it can get the same IP assignment every time it sends a DHCP IP request.

To configure IP management for DHCP clients:

1. Disable the **Use Profile configuration** option.
2. Under **IP Management List**, click **Add** to add a new IP assignment.

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring Routing

Routing determines the path for packet delivery in a network. The routing capabilities vary depending on the device model.

To view the configured routing policies:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Routing**. The configured routing protocols are displayed:

IPv4/IPv6 Static Route

Name	A name that helps identify this route.
Destination	The destination subnetwork IP address.
Subnet Mask	The subnet mask of the destination address. This is only available for IPv4 configuration.
Gateway	The IP address of the gateway or next hop.
Interface	The associated interface for this route.
Metric	The number of hub count.
Active	Enable or disable this route configuration.

IPv4/IPv6 Policy Route

Name	The name that helps identify the route.

Local Gateway	The port of the device that the route would use.
Protocol	The protocols associated with this route.
Source Network	A single IP address or a range of IP addresses that this route will be applied to. “Any” means all source IP addresses.
Destination Network	A single IP address or a range of IP addresses that this route will be applied to. “Any” means all destination IP addresses.
Source Port	The port number used for this type of traffic. ”Any” means all source ports will be used for this service.
Destination Port	The port number used for this type of traffic. ”Any” means all destination ports will be used for this service.
Active	Enable or disable this route configuration.

RIP Configuration

Interface	The interface by which Routing Information Protocol (RIP) information exchange will be performed.
Direction	Indicates inbound, outbound, or traffic for both directions.
Version	The version of the RIP
Authentication	Indicates whether the authentication is enabled.
Active	Enable or disable this route configuration

OSPFV2 Configuration

Interface	The interface assigned to the area defined below.
NSSA	Enable or disable the not-so-stubby area (NSSA) which can import external route information.
Area	The assigned area ID.
Priority	The OSPF priority which is used for determining the OSPF designated router.
Hello Interval	The time interval (seconds) between each hello packet.
Dead Interval	The time (seconds) the device must wait before it declares a neighbor OSPF router down when a hello packet has not been received.
Cost	The cost of the OSPF path.
Authentication	Indicates the authentication method used
LAN Route Exchange	Enable or disable the exchange of LAN routing table.
Active	Enable or disable this OSPF route configuration.

To configure routing policy:

1. Disable the **Use Profile configuration**option.
2. Under each routing protocol supported by the device model, click Add to add a new routing policy.

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring Services

Supported services can be configured individually depending on the features of the gateway.

To view and configure the supported services and network functions:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Network > Services**.

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Managing Traffic

The Traffic Management provides control over certain types of traffic by setting limits on bandwidth and sessions. Note that the availability of this function depends on the capability of the gateway.
To view Traffic Shaping rules configured:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Traffic Management**.

   Under Traffic Shaping, the following is displayed:

Name	The policy name.
Policy Type	Whether the traffic policy is applied to inbound or outbound traffic.
WAN Interface	The WAN port that this policy should be applied to.
Management Type	The metric to define the policy: Rate or Priority. Configure the following if Priority is selected: Low, Medium, or High. Higher priority means the traffic will be allocated with more bandwidth. If Rate is selected, enter the maximum bandwidth and minimum bandwidth (kbps).
Priority/Bandwidth Rate	The priority or the bandwidth configured for the respective management type.

Service	The type of traffic according to the protocol or application service configured.
Traffic Selector Match Type	The criteria for the traffic to which the policy should be applied: IP address, MAC address, or Interface.
Schedule Policy	The schedule policy that makes the policy effective during the designated time frame. Go to **Configure > Schedule policies** for scheduling information and configuration.

Viewing and Managing Session Limiting

To view Session Limiting rules configured:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Traffic Management**.

   Under Session Limiting, the following is displayed:

Name	The policy name.
Source Type	The source address can be configured as a single IP address, an IP address range, or an interface.
Maximum Sessions	The maximum number of sessions allowed (1-999).
Schedule Policy	The schedule policy that makes the policy effective during the designated time frame. Go to **Configure > Schedule policies** for scheduling information and configuration.

Viewing and Managing Custom Warning Pages

To view Custom Warning Page configured:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Traffic Management**.

   Under Custom Warning Page, the following is displayed:

Name	The policy name.
Source Type	The configured warning page to be displayed to users when the maximum limit of sessions has been reached . Go to **Configure > Splash pages** to view all the configured splash pages.
Active	Whether this rule is active or inactive.

To configure Traffic Management:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Traffic Management**.
3. Disable the option **Use Profile configuration.**

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring Captive Portal

The captive portal displays a splash page to wireless users who are required to agree to terms and conditions to use Internet services.
To view Captive Portal configured:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Captive Portal.**

The following information is displayed:

Name	The profile name.
Captive Portal	The authentication method for the users.
Splash Page	The pre-configured splash page which a wireless user must visit prior to using Internet services. The design of the page depends on the use case.
Basic Login	For basic login page, the associated authentication method: a local authentication database or an authentication server system.

3rd party Credentials	The configured third-party credential to be used for login.
SSID/VLANs	A pre-configured SSID/VLAN assigned to this captive portal setting.

To configure Captive Portal:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Captive Portal.**
3. Disable the option **Use Profile configuration.**

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring High Availability

Virtual Router Redundancy Protocol (VRRP) can be utilized to implement fault tolerance and load balancing on a network by designating primary and backup roles among the virtual routers. The primary router is responsible for processing packets sent to a virtual IP address and the backup router takes up the primary role when the primary becomes unavailable. This availability of this feature depends on device model.

To view VRRP settings configured:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > High Availability.** The following is displayed:

VRRP ID	The unique identifier for the VRRP group.
Interface	The interface to which the VRRP configuration would be applied.
IP Address	The virtual IP address.
Node Type	The designated role of the virtual router: Master or Backup.
Priority	The Priority determines the order of selection for a primary virtual router among the backup virtual routers (1-255). Higher number means high priority.

To configure VRRP settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > High Availability.**

3. Disable the option **Use Profile configuration.**

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring Wireless

You can create multiple SSIDs for your wireless network and configure each SSID with unique settings to accommodate different wireless usage scenarios. You can also configure radio settings such as operating mode and channels for different frequencies supported for the device model. Note that this feature is only available for supported models.

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Security Settings

Security features consist of firewall, intrusion prevention, and web content filtering as well as application control.

Note: Changing the Routing mode from Network Address Translation (NAT) to Router (go to Network > Addressing), the Security Firewall's option of Use Profile configuration will be disabled. Moreover, the rules configured for Port forwarding, Port triggering, and 1:1 NAT will be erased.

Firewall

To view a gateway's firewall settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Firewall.**

The following information is displayed:

IPV4/IPv6 FIREWALL RULES

IPv4/Ipv6 Firewall Rules allow or block certain types of traffic that need to be forwarded through the device.

Priority	The assigned priority number (1-998). Lower number means higher priority.
Name	The name of the rule.
Policy	Indicates whether it is a allow or deny rule.

Protocol	The associated protocol for the rule: Any, TCP, UDP, TCP/UDP, or ICMP.
Source Interface	The interface that the traffic is sent from.
Source	A single IP address or a range of IP addresses as the source host. Any means traffic from all IP addresses.
Source Port	The source port number used for this type of traffic. Any means all ports.
Destination	A single IP address or a range of IP addresses as the destination host. Any means traffic destined to all IP addresses.
Destination Port	The destination port number used for this type of traffic. Any means all ports.
Schedule	The associated Schedule Policy.
Active	Indicates whether this rule is enabled or disabled.

Note: The availability of IPv6 Firewall Settings depends on the features of the device model.

Port Forwarding

Port Forwarding redirects traffic entering the WAN to another port on the LAN. This is useful when a certain service is hosted on an interval server on the LAN.

To view Port Forwarding rules:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Firewall.**

The following information is displayed:

Name	The name for the rule.
Mode	Indicates whether the rule is for traffic forwarding or port translation.

Interface	The WAN interface to which this rule should be applied.
Protocol	The associated protocol of this rule: TCP, UDP, or TCP/UDP.
Public Port	The external port associated with this type of traffic or service (1-65535). It can be a single port or a range of ports.
Local IP	The IP address of the local server.
Local Port	The local port used for this service if translation mode is selected.
Allowed Remote IPs	The IP addresses of the remote hosts that this rule will be applied to. Any means all remote hosts.
Active	Indicates whether this rule is enabled or disabled.

Port Triggering

Port Triggering dynamically opens public ports for inbound traffic after certain ports are triggered by a service request.

To view Port Triggering rules:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Firewall.**

The following information is displayed:

Name	The rule's name.
Protocol	The protocol to which the rule is applied: TCP, UDP, or TCP/UDP.
Outgoing Trigger Port	The outgoing port used for this service.
Incoming Trigger Port	The incoming port used for this service.
Active	Indicates whether this rule is enabled or disabled.

1:1 NAT

One-to-one NAT allows a static mapping between an internal IP address and an external IP address.

To configure 1:1 NAT rules:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Firewall.**

   The following information is displayed:

Name	The rule name.
Interface	The WAN interface that this rule should be applied to.
WAN IP	The WAN IP address as the external IP address for translation.
Local IP	The local IP address as the interval IP address for translation.
Protocol	Indicates the associated protocol of this rule: TCP, UDP, or TCP/UDP.
Port	The port used for this traffic type.
Allowed remote IPs	The IP addresses of the remote hosts that this rule will be applied to. Any means to allow all remote hosts.

To configure Firewall rules:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Firewall.**
3. Disable the option **Use Profile configuration.**

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring IPS Settings

To view Intrusion detection and prevention settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security >IPS.**
3. Disable the option **Use Profile configuration.**

If the device is equipped of intrusion detection functions, you can enable or disable the following services:

Intrusion Detection	Enable intrusion detection. And select the WAN and LAN interfaces that the IPS and IDS should be implemented.
Intrusion Prevention	Enable intrusion prevention. And select the WAN and LAN interfaces that the IPS and IDS should be implemented.
Stealth Mode	This mode protects your device from Internet intrusion by not responding to unauthorized requests.
Block TCP Flood	Enable to block TCP flooding to WAN.
Bock UDP Flood	Enable to block UDP flooding to LAN.
Filter Check Mode	Enable the TCP filtering check mode.
Allow ICMP Traffic	Enable to allow packets of Internet Control Message Protocol to pass through.
DoS Attacks	Denial-of-Service (DoS) attacks encompass SYN Flood, ICMP Flood, and Echo storm. Configure the flood rate of each attack in packets/second for detection.

4. Click **Apply** at the top left to apply the settings to the affected devices immediately.

Viewing and Configuring Web Content Filter

The Web Content Filter is used to prevent access to unwanted websites. It allows you to create profiles that can take effective during the designated time frame and block websites belonging to a certain category.

Web Content Filter List

To view the Web Content Filter List:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security >Web Content Filter.**

Under Web Content Filter List, the following is displayed:

Name	The name for the filtering rule.

Policy	State whether this is a allow or block policy.
Schedule	The pre-configured scheduling.
Scope	The specified hosts or the whole network that this rule will be applied to.
Filtering Type	The type consists of a variety of categories, URLs, and custom groups to restrict the access to defined websites.
Active	State whether the rule is active.

Under Custom Warning Page, you can obtain the configured warning page that will display related messages when a restricted webpage is being visited. The following is displayed:

Name	Enter a name for this configuration.
Source Type	The pre-defined warning page to be displayed.
Actions	State whether the rule is active.

Under **Custom Group List,** you can obtain the Custom group which will be used to define the content filtering type above:

Group Name	The name for the custom group.
URLs	If URL filtering is used, it shows the name and keyword for the website. This blocks access to websites based on a website's domain name (e.g. google.com) and keywords with matching URLs. For example, keyword "ABC" will block "www.ABC.com" and "xxx.ABC.com" and other URLs containing ABC.
Category Filtering	If Category filtering is used, it shows the pre-defined categories to block access to.
In Use	State whether this rule has been activated.

To configure Firewall rules:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Web Content Filter.**
3. Disable the option **Use Profile configuration.**

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring Application Control

The Application Control is used to restrict certain communication of applications. It allows you to create profiles that can take effective during the designated time frame and prevent traffic of certain applications from being transferred.

Auto Upgrade

Enable automatic upgrade of application signature database and select the update schedule by entering the upgrade frequency in minutes or setting a specified time of a designated weekday for weekly updates.

To add an application control rule:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Application Control.**
3. Under Application Control List, the following information is displayed:

Name	The policy name.
Policy	State whether this is a allow or block policy.
Schedule	The pre-configured schedule. For configured scheduling methods, go to **Configure > Schedule policies**.
Scope	The specified hosts or the whole network that this rule will be applied to.
Application	State whether the filtering rule is based on a single application, or a single application from a pre-defined category, or a custom group of selected applications.
Active	State whether the application control policy is active or inactive.

Under **Custom Group List,** you can obtain Custom Group defined which will be used to define the application type above:

Group Name	The name of the custom group.
Application List	The selected applications for the custom group.
In Use	State whether this rule has been activated.

To configure Application Control:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Application Control.**
3. Disable the option **Use Profile configuration.**

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

VPN Settings

A Virtual Private Network (VPN) builds an encrypted connection between endpoints over a public network utilizing tunneling techniques. VPN can be configured only if your device supports this feature.

Site to Site VPN

The site-to-site VPN is a technique that allows connectivity between the offices located at multiple locations by setting up an IPsec tunnel over the Internet to access the intranet. In short, a site-to-site VPN builds a secure path over an insecure path. The Nuclias cloud gateway allows users to establish a VPN tunnel without manually entering the tunnel endpoint details and the local/remote networks. Instead, the Nuclias cloud gateway maintains these details and lets users select the networks.

Configuring Quick VPN

Quick VPN is a Nuclias auto-provisioning site-to-site VPN technology that allows you to quickly and easily build VPN tunnels between Nuclias gateway devices without tedious manual VPN configuration. If it is disabled, set up VPN manually at Manual VPN Settings to establish VPN connection with other partners.

To view or configure Quick VPN settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **VPN > Site-to-site VPN**.s
3. Select the topology: Hub-and-Spoke or Full Mesh. If Full Mesh is selected, the VPN establishes the Gateway-to-Gateway IPsec tunnel with other devices registered in the same or different sites of the same organization. To establish a tunnel with a particular remote device, enable the Join member field in the Remote VPN participants table. Once

the tunnel configuration is pushed to the remote peers, traffic gets initiated by the user, and a tunnel is established between the remote peers.

4. If Hub-and-Spoke is selected, specify the role to be either a hub or spoke. If Spoke is selected, you can choose hubs to build VPN tunnels in the Exist hubs table. In addition, it lists the Exist hub devices available with the option of Primary Hub. If you enable the Primary Hub field, the selected hub will be the primary hub for the spoke and can communicate to all the spoke devices linked to this hub. At a time, you can enable only one primary hub. If Hub is selected, then VPN tunnels will be built among hubs and dependent spokes.
5. If Hub mode is selected, enable or disable VPN connection with a remote peer. You may also choose to designate a remote peer as a backup hub.
6. If Spoke mode is selected, you can choose to designate a remote peer as the primary hub.
7. Click **Apply**.

Quick VPN Settings

In the Local networks section, if you have multiple subnets, you can specify which one subnet participates in the VPN, i.e., traffic from the enabled subnet will be encrypted by the IPsec VPN. All local subnets must be unique within the VPN topology

Note: A list of Quick VPN connections will be displayed in the **Summary > VPN Status** page. Select Quick VPN (Full Mesh and Hub-and-Spoke) as the Display VPN type.

Configuring Manual VPN

To view or configure Manual VPN settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **VPN > Site-to-site VPN**. Enter the following:

Connection Name	Enter a name for this VPN connection (1-64 characters).
IKE Profile	Select the IKE profile which contains security settings that will be used for the VPN connection.
Local Network	The scope of the local network to which the VPN connection will apply.
Local Network	Enter a local IP address or subnetwork of the local network to participate in the VPN. If Single IP is selected, enter the IP address. If Subnet is selected, enter the IP address and subnet mask (or prefix for IPv6). Select Any for the entire local network.

Remote Network	Enter a remote IP address or subnetwork of the remote network to participate in the VPN. If Single IP is selected, enter the IP address. If Subnet is selected, enter the IP address and subnet mask (or prefix for IPv6). Select Any for the entire remote network.
Outgoing Interface	Select an interface to which the VPN connection will use.
Remote Gateway	Select FQDN or Static IP for configuring the remote gateway address. Then enter the IP address or FQDN address.
Keep-alive	Enable or disable keep-alive for VPN reconnection. If enabled, enter the source and destination IP address as well as the detection period in seconds (10-199) and retry after the number of failures (3-99).
Idle Timeout	Enter the maximum length of time that the VPN connection can stay active when three is no traffic.
Dead Peer Detection	Enable detection for dead peers. If enabled, enter the detection interval (10-999 seconds) and Retry after failure (3-99 times).
NetBIOS Broadcast	Enable or disable NetBIOS broadcast from one end to be forwarded to the other end of the VPN connection.
Outgoing Backup Interface	Select an interface to which the VPN connection will use as a backup if Dead Peer Detection is enabled.
Remote Backup Gateway	Select FQDN or Static IP for configuring the remote gateway address if Dead Peer Detection is enabled.
IKE Backup Profile	Select the IKE profile which contains security settings that will be used for the backup VPN connection if Dead Peer Detection is enabled.

To add an IKE profile,enter the following:

Profile Name	Enter a name for this IKE profile.

IKE Version	Select the IKE version: v1 or v2.
IKE phase-1 Settings	
Exchange Mode	Select the exchange mode: Aggressive or Main.
Local Identifier Type	Select the identification method: Local WAN IP, FQDN, or User-FQDN. And enter the identifier according to the selected method.
Remote Identifier Type	Select the identification method: Remote WAN IP, FQDN, or User-FQDN. And enter the identifier according to the selected method.
DH Group	Select a Diffie-Hellman (DH) Group for key exchange. These groups vary in prime key lengths.
Encryption Algorithm	Select encryption algorithm(s) for ESP packets encryption.
Authentication Algorithm	Select authentication algorithm(s). And enter the SA lifetime in seconds (300-604800).
Authentication Method	Select the authentication method. Then enter the preshared key or select a certificate depending on the method selected. Go to **Settings > Certificate Management** for Certificate list.
Extended Authentication	Enable this and select extended authentication method: Authentication server, IPsec host, or Local authentication. Depending on the method, select the corresponding RADIUS/ LDAP/POP3/Active Directory/NT Domain server or Local Authentication profile or enter the username and password for IPsec host. Refer to **Configure > Authentication > Local Authentication list** and **Authentication servers** for Authentication profiles and servers.
IKE phase-2 Settings	

Protocol Selection	Select either ESP or AH. If Encapsulating Security Payload (ESP) is selected, select the Encryption algorithm to encrypt or decrypt ESP packets.
Authentication Algorithm	Select the authentication algorithm for header packets validation.
SA Lifetime (sec.)	Enter the SA lifetime (300-604800 seconds) for the active duration of a VPN tunnel.
Perfect Forward Secrecy	Enable or disable the Perfect Forward Secrecy. If enabled, the VPN communication is better protected with renewed negotiation of key values in the exchange.
DH Group	If the above PFS is enabled, select the DH group for key establishment.

3. Click **Apply** at the top.

Note: A list of Quick VPN connections will be displayed in the **Summary > VPN Status** page. Select Quick VPN (Manual) as the Display VPN type.

Client to Site VPN

An IPsec policy can be defined between this router and another gateway to create network-to-network IPsec tunnels. To configure IPsec VPN Server settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **VPN > Client-to-site VPN**. Enter the following:

Connection Name	Enter a name for this configuration
IKE	Select a pre-configured IKE profile for this VPN configuration.
Local Network	Enter the IP address and subnet mask of the local network. Select Any to not restrict to a single subnet.
Tunnel Mode	Select either full or split tunnel for the mode. Select Full tunnel or Split tunnel. The Split mode will split DNS requests among DNS servers. It allows you to create two zones for the same domain, one to be used by the internal network, the other used

	by the external network .For Split tunnel, enter the Split Domain names.
DHCP Relay	Enable or disable DHCP relay. If enabled, enter the IP address of the relay gateway. If disabled, enter the following IP address information.
Starting IP Address/ Ending IP Address	Enter the range of the IP addresses for VPN connections.
Primary/Secondary DNS	Enter the primary and optional secondary DNS servers.
Primary WINS Server/ Secondary WINS Server	Enter the primary and optional secondary Windows Internet Naming Service (WINS) servers.
Outgoing Interface	Select the WAN interface to which the IPsec VPN should apply.
Split DNS	Enable or disable Split DNS if Split tunnel is selected. And enter the domain names if enabled (3-253 characters).
NetBIOS Broadcast	Enable or disable NetBIOS information to be forwarded to the other endpoint of the VPN tunnel. The information is used for name resolution in Windows networking.

To add an IKE profile, enter the following:

Profile Name	Enter a name for this IKE profile.
IKE Version	Select the IKE version: v1 or v2.
IKE phase-1 Settings	
Exchange Mode	Select the exchange mode: Aggressive or Main.

Local Identifier Type	Select the identification method: Local WAN IP, FQDN, or User-FQDN. And enter the identifier according to the selected method.
Remote Identifier Type	Select the identification method: Remote WAN IP, FQDN, or User-FQDN. And enter the identifier according to the selected method.
DH Group	Select a Diffie-Hellman (DH) Group for key exchange. These groups vary in prime key lengths.
Encryption Algorithm	Select encryption algorithm(s) for ESP packets encryption.
Authentication Algorithm	Select authentication algorithm(s). And enter the SA lifetime in seconds (300-604800).
Authentication Method	Select the authentication method. Then enter the preshared key or select a certificate depending on the method selected. Go to **Settings > Certificate Management** for Certificate list (refer to Certificate Management) .
Extended Authentication	Enable this and select extended authentication method: Authentication server, IPsec host, or Local authentication. Depending on the method, select the corresponding RADIUS/ LDAP/POP3/Active Directory/NT Domain server or Local Authentication profile or enter the username and password for IPsec host. Refer to **Configure > Authentication > Local Authentication list** and **Authentication servers** for Authentication profiles and servers.
IKE phase-2 Settings	
Protocol Selection	Select either ESP or AH. If Encapsulating Security Payload (ESP) is selected, select the Encryption algorithm to encrypt or decrypt ESP packets.
Authentication Algorithm	Select the authentication algorithm for header packets validation.

SA Lifetime (sec.)	Enter the SA lifetime (300-604800 seconds) for the active duration of a VPN tunnel.
Perfect Forward Secrecy	Enable or disable the Perfect Forward Secrecy. If enabled, the VPN communication is better protected with renewed negotiation of key values in the exchange.
DH Group	If the above PFS is enabled, select the DH group for key establishment.

3. Click **Apply** at the top.

PPTP/L2TP

A PPTP server is available on the router for LAN and WAN PPTP client users to access.

To configure PPTP/L2TP Server settings

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **VPN > PPTP/L2TP**. Enter the following:

Name	Enter a name for the configuration profile of the server (1-64 characters).
Server Type	Select either PPTP or L2TP.
Routing Mode	Select either NAT or Router.
Starting IP Address/ Ending IP Address	Enter the LAN IP address range to be assigned to the VPN clients.
Authentication Server	Select the authentication server. Depending on the method, select the corresponding RADIUS/LDAP/POP3/Active Directory/NT Domain server or Local Authentication profile. Go to **Configure > Authentication > Local Authentication list** and **Authentication Servers** for Local authentication profiles and authentication servers list.
Authentication Protocol	Select the authentication protocol(s): All, PAP, CHAP, MS-CHAP, and MS-CHAPv2.

Encryption	[PPTP only] Select the encryption method(s) for PPTP: For PPTP, select All, MPPE 40 bit, MPPE 128 bit, or Stateful MPPE. The Microsoft Point-to-Point (MPPE) encrypts data for PPTP VPN.
Idle Timeout	The length of time (seconds) to wait before terminating a VPN session (300-1800).
NetBIOS	[PPTP only] Enable or disable NetBIOS, which is used for name resolution in Windows networking, if there is a WINS server set up in your LAN. If enabled, enter the Windows Internet Naming Service (WINS) server IP address. This option is only available for PPTP.
Enable Secret Key	[L2TP only] Enable or disable the secret key (or preshared key) with 8-63 characters which will be required for client VPN settings.
L2TP over IPsec	[L2TP only] Enable or disable L2TP over Internet Protocol Security (IPsec), on which L2TP relies for secure packets exchange.
IKE Version: Configure Internet Key Exchange (IKE) if L2TP Over IPsec is enabled.	
IKE version	Select the IKE version for configuration.
IKE phase-1 settings	
Exchange Mode	Select the exchange mode: Aggressive or Main.
Local Identifier Type	Select the identification method: Local WAN IP or FQDN. And enter the identifier according to the selected method.
Remote Identifier Type	Select the identification method: Remote WAN IP or FQDN. And enter the identifier according to the selected method.
DH Group	Select a Diffie-Hellman (DH) Group for key exchange. These groups vary in prime key lengths.
Encryption Algorithm	Select encryption algorithm(s) for ESP packets encryption.

Authentication Algorithm	Select authentication algorithm(s). And enter the SA lifetime in seconds (300-604800).
Authentication Method	Select the authentication method. Then enter the preshared key or select a certificate depending on the method selected. Go to **Settings > Certificate Management** for Certificate list.
Extended Authentication	Enable this and select extended authentication method: Authentication server, IPsec host, or Local authentication. Depending on the method, select the corresponding RADIUS/ LDAP/POP3/Active Directory/NT Domain server or Local Authentication profile or enter the username and password for IPsec host. Refer to **Configure > Authentication > Local Authentication list** and **Authentication servers** for Local authentication profiles and authentication servers.
IKE phase-2 settings	
Protocol Selection	Select either ESP or AH. If Encapsulating Security Payload (ESP) is selected, select the Encryption algorithm to encrypt or decrypt ESP packets.
Authentication Algorithm	Select the authentication algorithm for header packets validation.
SA Lifetime (sec.)	Enter the SA lifetime (300-604800 seconds) for the active duration of a VPN tunnel.
Perfect Forward Secrecy	Enable or disable the Perfect Forward Secrecy. If enabled, the VPN communication is better protected with renewed negotiation of key values in the exchange.
DH Group	If the above PFS is enabled, select the DH group for key establishment.

PPTP VPN Client can be configured on this router to access a remote network.

To configure a VPN client,enter the following:

Name	Enter a name for the PPTP/L2TP configuration profile of the client (1-64 characters).
Client Type	Select either PPTP or L2TP.
VPN Server	Enter the IP address or FQDN of the VPN server
Tunnel Type	Select Full tunnel or Split tunnel. Split tunnel mode only sends traffic to the private LAN with pre-specified client routes and give the client access to specific private networks, thereby allowing access control over specific LAN services.
Remote Network/ Netmask	Enter the remote network and netmask if split tunnel is selected.
Username/Password	Enter the username and password required for connection.
Encryption	For L2TP server, enter the Secret key (8-63 characters) if encryption is enabled. This value must match the preshared key value entered on the VPN server.
MPPE	Enable the Microsoft Point-to-Point Encryption (MPPE), which encrypts data for VPN communication.
Idle Timeout	For PPTP, enter the length of time (seconds) to wait before terminating a session.
Reconnect Mode	For L2TP, select On demand or Always on. Enter the Maximum idle time in seconds (300-1800) to wait before dropping an idle connection.
L2TP over IPsec	Enable or disable L2TP over Internet Protocol Security (IPsec), on which L2TP relies for secure packets exchange.
IKE Version: Configure Internet Key Exchange (IKE) if L2TP Over IPsec is enabled.	
IKE version	Select the IKE version for configuration.
IKE phase-1 settings	

Exchange Mode	Select the exchange mode: Aggressive or Main.
Local Identifier Type	Select the identification method: Local WAN IP or FQDN. And enter the identifier according to the selected method.
Remote Identifier Type	Select the identification method: Remote WAN IP or FQDN. And enter the identifier according to the selected method.
DH Group	Select a Diffie-Hellman (DH) Group for key exchange. These groups vary in prime key lengths.
Encryption Algorithm	Select encryption algorithm(s) for ESP packets encryption.
Authentication Algorithm	Select authentication algorithm(s). And enter the SA lifetime in seconds (300-604800).
Authentication Method	Select the authentication method. Then enter the preshared key or select a certificate depending on the method selected. Go to **Settings > Certificate Management** for Certificate list.
Extended Authentication	Enable this and select extended authentication method. Enter the Username and Password if IPsec host is selected.
IKE phase-2 settings	
Protocol Selection	Select either ESP or AH. If Encapsulating Security Payload (ESP) is selected, select the Encryption algorithm to encrypt or decrypt ESP packets.
Authentication Algorithm	Select the authentication algorithm for header packets validation.
SA Lifetime (sec.)	Enter the SA lifetime (300-604800 seconds) for the active duration of a VPN tunnel.
Perfect Forward Secrecy	Enable or disable the Perfect Forward Secrecy. If enabled, the VPN communication is better protected with renewed negotiation of key values in the exchange.

DH Group	If the above PFS is enabled, select the DH group for key establishment.

3. Click **Save**.

Note: A list of PPTP/L2TP connections will be displayed in the **Summary > VPN Status** page.

OpenVPN

OpenVPN allows peers to authenticate each other using certificates, or username/password. When used in a multiclient-server configuration, it allows the server to release an authentication certificate for every client, using signature and Certificate authority. An OpenVPN can be established through this router.

To configure OpenVPN settings

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **VPN > OpenVPN**. Enter the following:

Mode	Select the mode for the OpenVPN: Server, Client, or Access server client.
Upload Access Server Client	[Access Server Client mode only] Upload a configuration file which contains server and client IP address information if Access server client mode is selected. In access server client mode, the user has to download the auto login profile from the OpenVPN Access Server and upload the same to connect.
CRL Certificate	[Access Server Client mode only] Openvpn provides CRL authentication using CRL certificate. You can upload the required certificates by enabling it it first.
VPN Network/Netmask	[Server mode only] Enter the network IP address/netmask of the VPN. This is only available for the Server mode.
Server IP/Failover Server IP	The IP address or FQDN of the VPN server and failover server. This is only available for the Client mode.
Duplicate CN	[Server mode only] Enable or disable the duplicate CN to allow or disallow the same certification for multiple clients. This is only available for the Server mode.

Port	Enter the port number for VPN communication. The default is 1194.
Tunnel Protocol	Select the protocol for tunneling: TCP or UDP.
Encryption Algorithm	Select the encryption method: AES-128, BF-CBC, AES-192, or AES-256.
Hash Algorithm	Select the hash algorithm: SHA1, SHA256, or SHA512.
Tunnel Type	[Server mode only] Select the tunnel type: Full or Split. If Split is selected, enable or disable the client-to-client communication. Full Tunnel mode sends all traffic from the client across the VPN tunnel to the router. Split Tunnel mode only sends traffic to the private LAN with specified client routes. This is only available for Server mode configuration.
User-based Authentication	Enable or disable user-based authentication. If this is enabled, select the user profiles for Local authentication if server mode is used (refer to Local Authentication). If client mode is used, enter the username and password for VPN connection. Also select a certificate for TLS key if TLS authentication is used (refer to Certificate Management).
Certificate Verification	Enable or disable the use of certificate for verification.
Certificate	Select an available certificate from the list. The content of the certificate will be loaded in the field below.
TLS Authentication Key	Enable or disable the TLS authentication. If enabled, select an TLS authentication key from the certificate list. To obtain the certificate list, go to **Settings > Certificate Management**.
DH Key	Select a DH key from the certificate list. This is only available for Server mode configuration. To obtain certificate list, go to **Settings > Certificate Management**
Server Policies	Enable or disable the server policy. Enter the server policy and add a new server policy to permit or block networks for VPN connections. These policies can be applied to a specific IP

	address or IP networks on the LAN and can be enforced on the specified scope according to the supported features of the router. The List of Available Policies can be filtered based on whether it applies to a user, group, or all users (global). To add a new server policy, enter the following: Policy name: Give a name for this policy. Policy: Select whether it is a Deny or Permit policy. Scope: Select whether it is a global policy or to be applied for certain users using Local authentication. Select the user profile if Local authentication is selected. Apply policy to: Select whether to apply this policy to a single IP address or a subnet work and enter the required IP address and/or the Subnet mask and the port number. ICMP: enable or disable Internet Control Message Protocol (ICMP) traffic in VPN connections.
Remote Networks	If this is enabled, click Add to add a remote network configuration: enter a name for the configuration and the remote network IP address and subnet mask.
Port	Enter the port number (1-65535). This can be a single port or a range of ports, e.g. 3000-3200.
ICMP	Enable or disable the use of ICMP in the VPN communication.

OpenVPN provides authentication using certificates. This system will allow you to configure client list using **Local Authentication list (refer to Local Authentication)** and centrally manage the client certificates (refer to Certificate Management).To configure Client list for Server mode configuration:

1. Under Client list, click **Import**. The **Import users from local authentication list** page displays.
2. Select a pre-configured local user profile or click **Add local authentication** and configure a local user profile by specifying the following: the Local Authentication profile name, the Access level, Managed Sites, and the username and password for each new user. You can use the Bulk import function to upload a CSV file containing the user information to add multiple users at once. Refer to **Configure > Authentication > Local Authentication list** for more information.

3. Click **Save.** Once a Local authentication profile is imported successfully, you can manage the clients' certificates in the Certificate Management page (go to **Settings > Certificate management**) .

To configure OmniSSL Portal Layout for Server mode configuration:

OmniSSL facilitates the client installation from the device via the instructions on the portal page and is an enhancement to the existing OpenVPN. The enhancements allow the VPN tool to be used via mobile devices and eliminate browser and Java dependencies.

1. Under OmniSSL Portal Layout, click **Add**. The **Add portal layout configuration** page displays.
2. Enter a name for the profile and select a pre-defined login page for OmniSSL. Refer to **Configure > Splash pages** for more information. The Splash pages allow you to create a custom page that is presented upon authentication to the remote OmniSSL users.
3. Click **Save.**

Note: A list of OpenVPN connections will be displayed in the **Summary > VPN Status** page.

GRE Tunnel

GRE tunnels allow for broadcast traffic on the LAN of the router to be passed over the internet and received by remote LAN hosts.

To view or configure GRE Tunnel settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **VPN > GRE Tunnel**. Enter the following:

Name	The name for the GRE Tunnel configuration.
Interface	Select the WAN interface to create this tunnel with from the drop-down menu.
GRE Tunnel IP/ Subnet Mask	Enter the IP address/subnet mask of this endpoint. It will be referenced in the other router's static route as the Gateway IP address.
Remote IP	Enter the WAN IP address of the endpoint router.
Static Route Configuration	IP address/Subnet mask: Enter the destination IP address/subnet mask of the static route from the remote LAN subnet. Gateway IP address: Enter the GRE tunnel IP of the terminating router that manages the remote LAN.

3. Click **Save.**

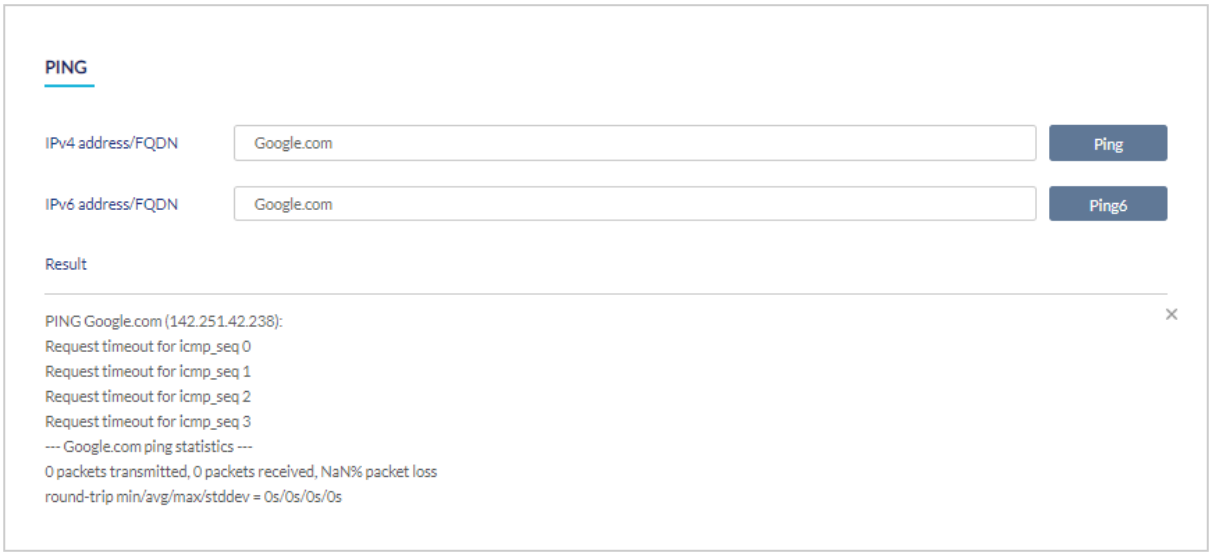
4. Click **Apply** at the top left to apply the settings to the affected device immediately.

Note: The GRE connection status will be displayed in the **Summary > VPN Status** page.

Tools

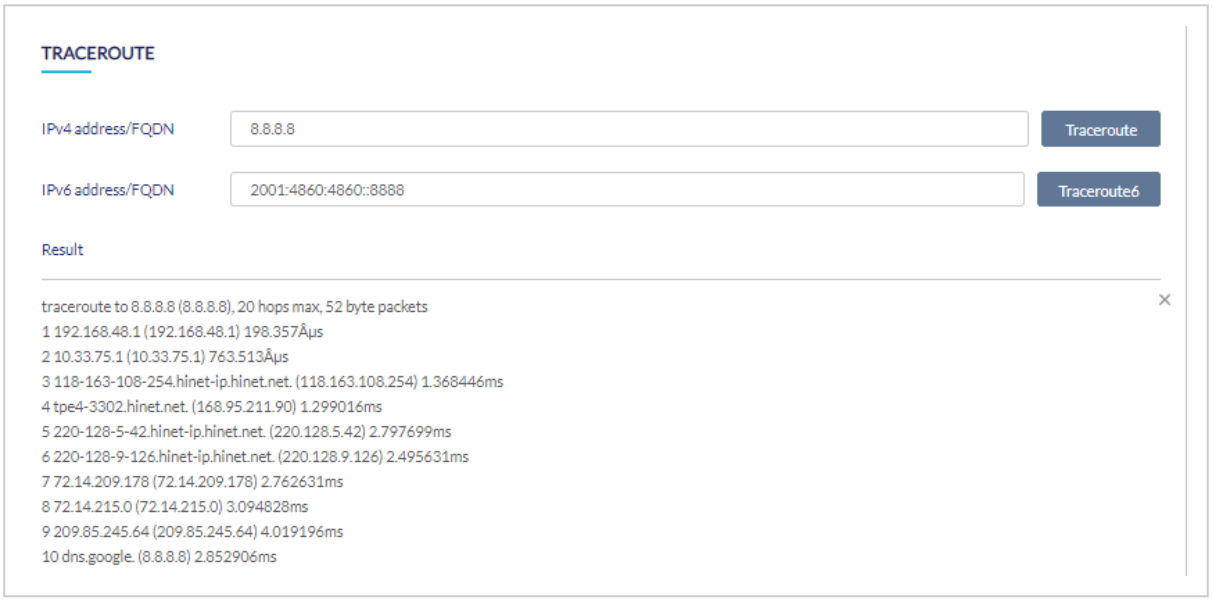
Performing a Device Ping Test

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Tools** tab in the top-right of the screen.
3. In the IPv4 or IPv6 address/FQDN field in the Ping section, enter a valid IP address or FQDN.
4. Click **Ping** for IPv4 addresses or **Ping6** for IPv6 addresses of the remote hosts. The results will be displayed as shown below:



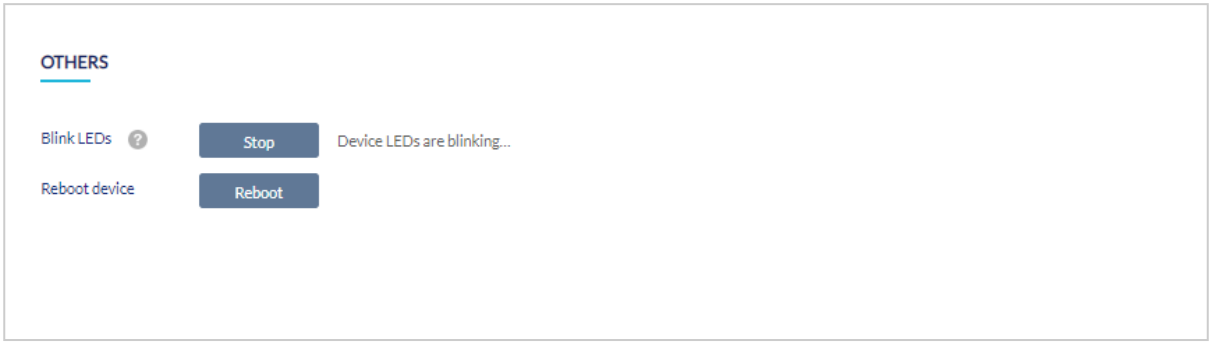
Performing a Traceroute Test

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Tools** tab in the top-right of the screen.
3. Under Traceroute, enter a valid IP address or FQDN in the IP address/FQDN field.
4. Click **Traceroute** for IPv4 addresses or **Traceroute6** for IPv6 addresses of the remote hosts. The results will be displayed as shown below:



Performing LED Blinking and Device Reboot

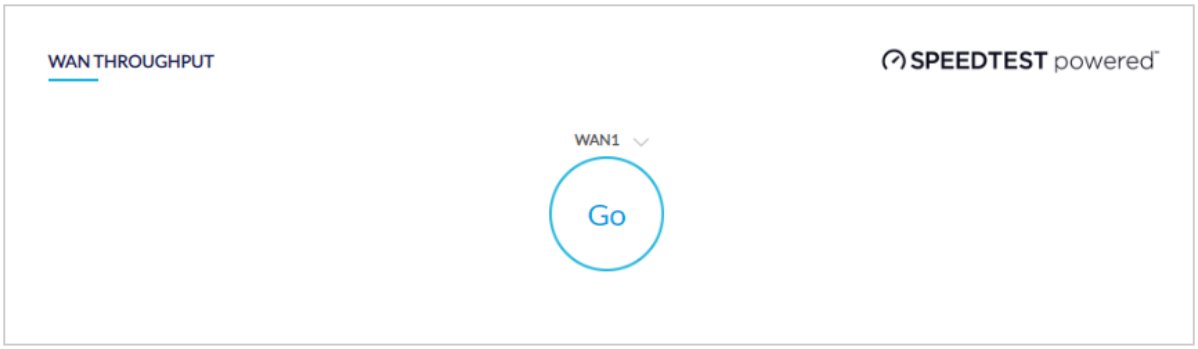
1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Tools** tab in the top-right of the screen.
3. In the Others section, click **Reboot** to reboot the device. Or click **Start** to start blink LEDs on the device. Click **Stop** to top blinking LEDs.



Note: Please refer to the respective device's manual for the status of LED indicators.

Performing WAN Throughput Test

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Tools** tab at the top right of the screen.
3. In the WAN Throughput section, click **Go**. The upload and download speed will be displayed.



Exporting or Importing Device Settings

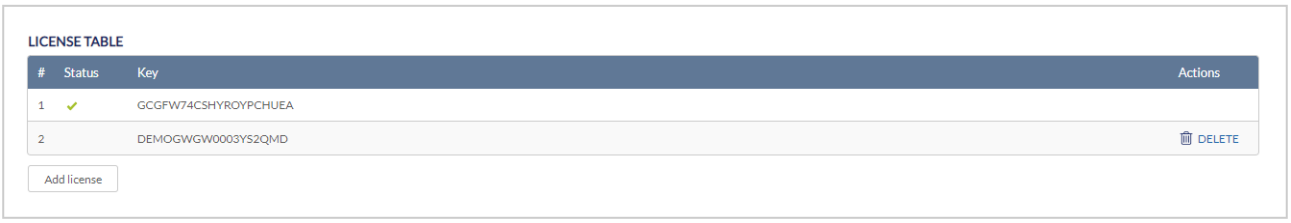
The device setting metadata can be exported as a single CSV file and it can be later imported for configuration restoration. To export device settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Tools** tab at the top right of the screen.
3. In the Export and Import Device Settings section, click **Download**. The exported file will be downloaded to your browser's default download folder.

License

Adding a License Key to a Device

1. Navigate to **Monitor > Gateway > Devices** 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 > Gateway > Devices** 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 reclassify it as Unused in the license

management inventory.

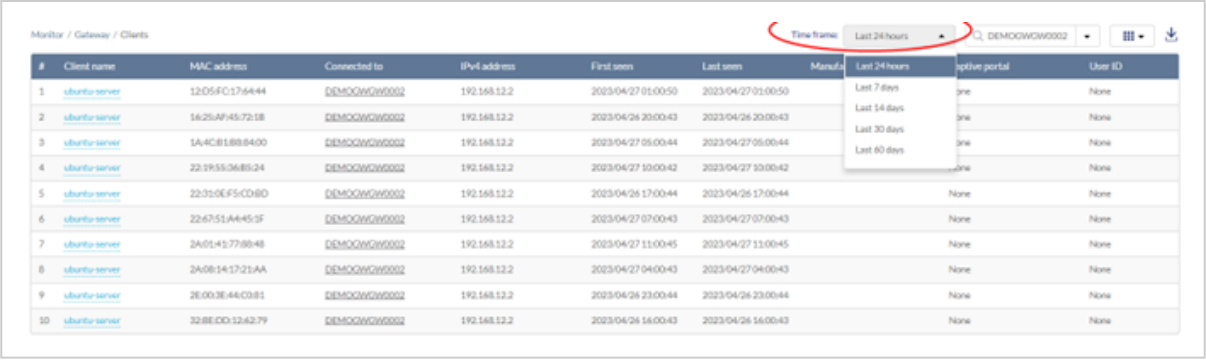


Clients

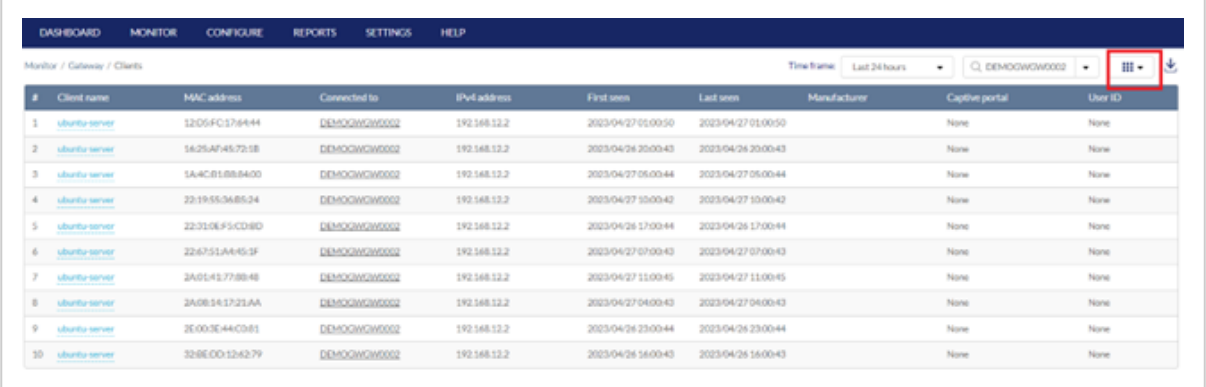
From the Clients window, you can consult a detailed overview of all currently connected devices with additional information including status, VLAN, and general settings.

Customizing the Client Monitor Overview

1. Navigate to **Monitor > Gateway > Clients**. The client list for all gateways will appear.
2. Select a time frame from the drop-down menu to define the time frame that the device was detected online.



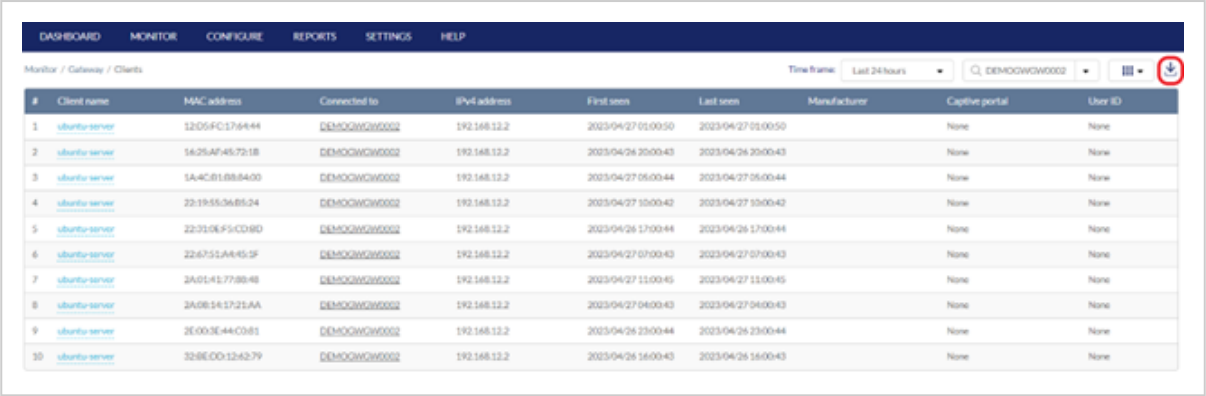
3. Click the parameter filter icon.



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

Downloading Client Monitoring Logs

1. Navigate to **Monitor > Gateway > Clients**.
2. From the client monitoring logs, click the download icon in the top-right.



Event Log

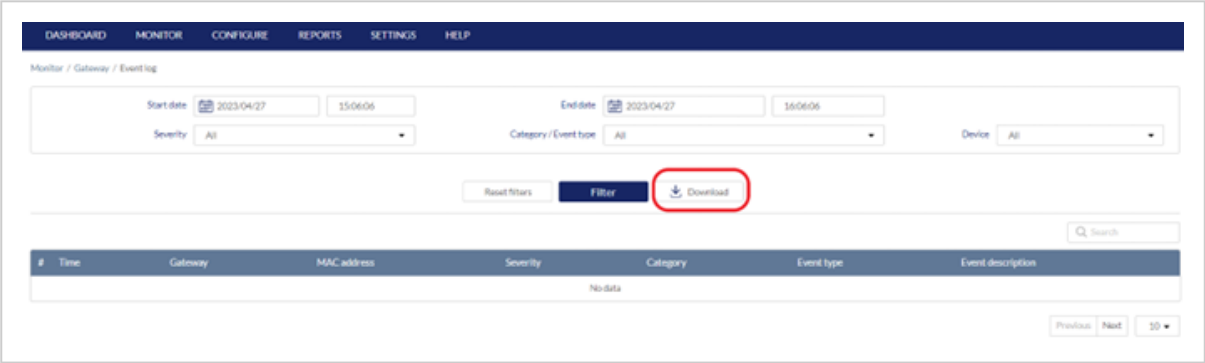
From the Event Logs window, you can consult a detailed log of events occurring on the network. You can also define event filter parameters, including event type and time period.

Filtering Event Log Parameters

1. Navigate to **Monitor > Gateway > Event Log**.
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 Category/Event type drop-down menu and select the event types to display. Select All to show all event types.
6. Click the Device drop-down menu and select a device to filter the results. Select All to show all event logs for all devices.
7. Click **Filter** to display all events matching the defined parameters. Click **Reset filters** to reset all currently set parameters.

Downloading Event Logs

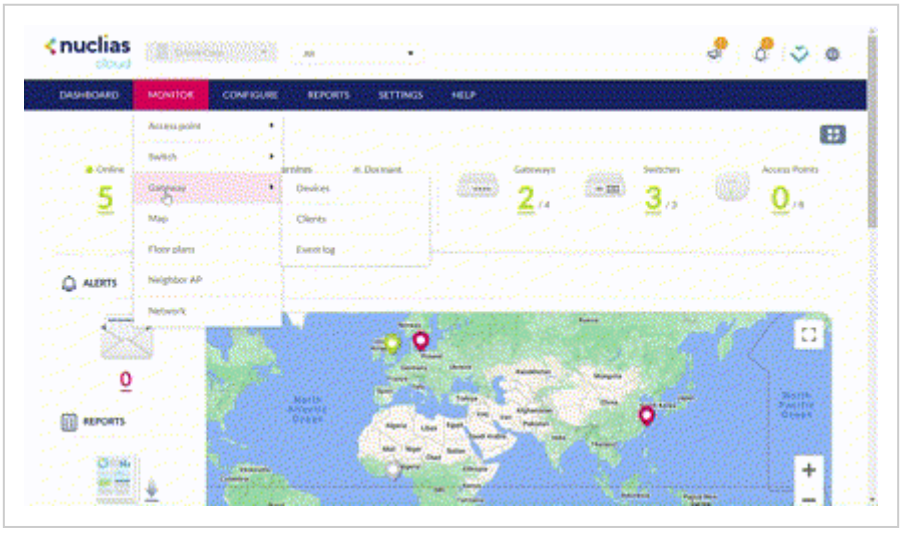
1. Navigate to **Monitor > Gateway > Event Log**.
2. From the event log list, click **Download**.


DASHBOARD
MONITOR
CONFIGURE
REPORTS
SETTINGS
HELP
Monitor / Gateway / Event log
Start date
2023/04/27
15:06:06
End date
2023/04/27
16:06:06
Severity
All
Category / Event type
All
Device
All
Reset filters
Filter
Download
Search
Time
Gateway
MAC address
Severity
Category
Event type
Event description
No data
Previous
Next
10

Clients

Devices

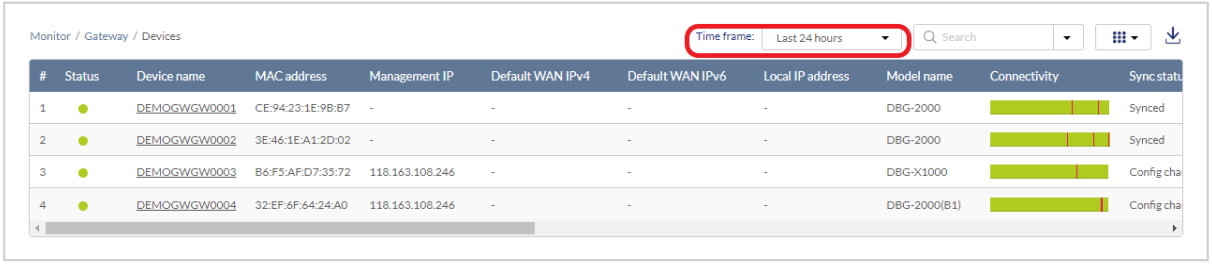
From the Devices window, you can consult a detailed log of events occurring on the network. You can also filter events using specific event filter parameters, including event type and time period.



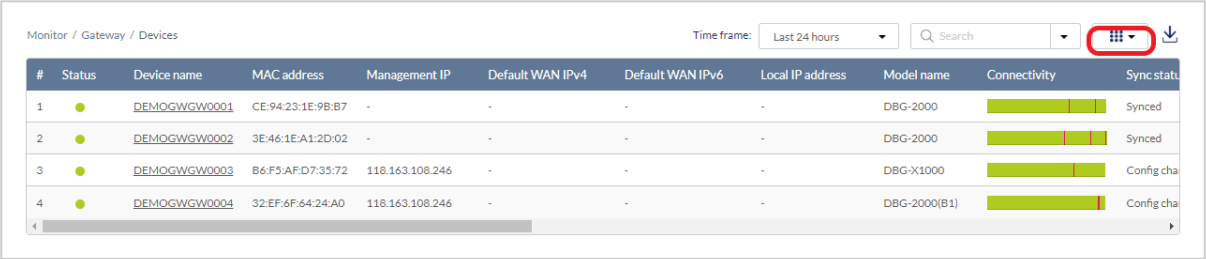
The Device Monitor

Customizing the Device Monitor Overview

1. Navigate to **Monitor > Gateway > Devices**.
2. Select a time frame from the drop-down menu to set the duration for connectivity information.



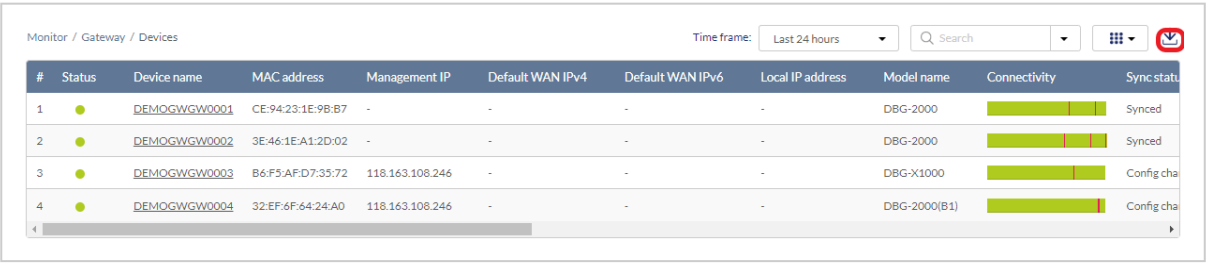
3. Click the filter parameter icon.



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

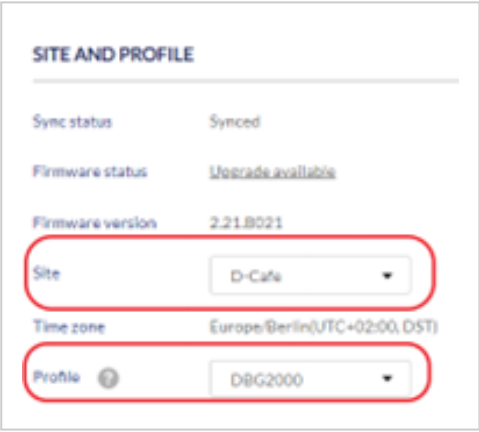
1. Navigate to **Monitor > Gateway > Devices**.
2. From the device list, click the **Download** icon in the top-right to export the table listing as a CSV file.



Device Basic Settings

Changing the Device Site and Profile

1. Navigate to **Monitor >Gateway > Devices** and select a device from the list.
2. Select the **Basic** tab at the top.
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 **Save**.

The Performance Summary

Viewing and Customizing the Gateway Performance Summary

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Summary** tab. Click the tabs at the top to obtain additional information described below:

Status	Provides connection information for the device along with basic port configuration and traffic statistics for each port. You can also obtain Internet usage for both download and upload data in a specified time frame.
Statistics	Provides reports of the number of connected clients in the selected time frame. You can also obtain reports of WAN port usage and the whole Internet usage as well as VPN usage.
DHCP	Provides the utilization rate of each configured DHCP subnet. It also lists the DHCP leases history.
VPN Status	Provides VPN connection statistics. The page lists the active VPN association or connections, the traffic details, and the tunnel state. You can view the status (connect or disconnect) of the gateway's VPN connections as a whole (by selecting Overview for the Display VPN type) or view each VPN separately.

Network Settings

Verifying and Changing the Default WAN Configuration

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Network** tab at the top.
3. Under **WAN Mode Configuration**, verify the WAN mode and the primary WAN port (or Default WAN Configuration) settings. Note that the settings or configurations here depend on the device model and firmware.

To change the Default WAN or WAN Mode Configuration:

1. Disable the option **Use Profile configuration** first at the top of the configuration page to allow changes.
2. Select IPv4 and IPv6 default WAN configuration. Or select a WAN mode from the available options. For **Primary WAN**, designate a WAN port as the primary WAN. For **Auto-rollover using WAN**, select both Primary and Secondary WAN ports as well as the **Health Check** method. For DNS servers and Ping IP address methods, enter the

respective server IP address as the destination to check the connectivity. Also enter the **Retry interval** (seconds) and **Failover after** (number of failed retries). For Load balancing, select the method (either Round robin or Spillover mode).

3. For **Round robin**, configure the Health check method (or none) and enter the **Retry interval** (seconds) and **Failover after** (number of failed retries). Hence, if a WAN interface disconnects, only the alternate WAN ports will transfer traffic flows in a round robin manner. For **Spillover**, enter the **Load tolerance** (%) and **Max bandwidth** (Mbps) as the threshold value. Once the threshold is exceeded, new traffic flows will be allocated to the alternate WAN interfaces. The precedence for selection is based on the configuration of Primary, Secondary, and Tertiary WAN interface.
4. Click **Apply**.

Note: The WAN mode can be configured using Profiles. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Using Dynamic DNS

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Network** tab at the top.
3. Under **Dynamic DNS**, enable or disable the service.
4. > Click **Apply**.

To add a DDNS service:

1. Disable the option Use Profile configuration first at the top of the configuration page.
2. Click **Add**. Enter the following information:

WAN Interface	Select the WAN interface for configuration
Service Provider	Select the DDNS service provider.
Username/Password	Enter the DDNS account name and password.
Hostname	Enter the registered hostname with the DDNS service.
Wildcard	Enable or disable the wildcard option which will resolve *.hostname to the same designated IP address.
Use Public IP	Enable or disable the use of a public IP address.
Force Update Interval	Enter the DDNS update interval (days).

3. Click **Save** to close the screen. Then click **Apply**.

Using IP Alias for the WAN

Note: The IP Alias function is only available on supported models.

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Network** tab at the top.

3. Under **IP Aliasing** , click **Add** to bind one or multiple IP addresses to a WAN interface.

   Enter the following information:

WAN Interface	Select the WAN interface for configuration
IP Address/Subnet Mask	Enter the IP address and subnet mask to bind to the WAN interface.

4. Click **Save** to close the screen. Then click **Apply**.

Viewing and Customizing the Gateway Port Status Overview

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Summary** tab at the top. The ports of the gateway device are displayed along with their detailed information shown in the table below:

Port Number	Numbering of the ports on the connector panel.
Interface Name	The name that identifies the port.
Port Status	Displays the link state of the port.
MAC Address	The MAC address of the port.
IP Address/ Subnet Mask	The IP address and subnet mask assigned to the port
Gateway	The gateway IP address if it has been assigned.
DHCP Mode	Displays if DHCP service has been enabled on the device.
Sent Bytes	The amount of data sent out of the port (bytes).
Received Bytes	The amount of data received through the port (bytes).

Total Bytes	The total amount of sent and received data volume (bytes).

To configure a port's basic settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Network** tab at the top.
3. Disable **Use Profile Configuration** to allow modification.
4. Under **Port Configuration** , select a port and click **EDIT** under Actions. Specify the following information for the selected LAN port:

Interface Type	Select the connection type: LAN, WAN, or DMZ.
Interface Name	Enter a name to identify this interface.
Bridge Network	Enable or disable bridging with another network. Configure the interface with more settings below if bridging is not enabled.
IP Address/ Subnet Mask	Enter an IP address with subnet mask.
DHCP Mode	Enable or disable DHCP service for IP address assignment.
DHCP Server	Enter the following information if DHCP server is selected. Domain name: Assign a domain name for DHCP service. Starting IP address/Ending IP address: Enter the range of IP addresses that can be assigned dynamically. Default gateway: Assign a default gateway for DHCP service. DNS server: Configure DNS by specifying a static DNS server, DNS setting from the ISP, or using DNS proxy. For static DNS, enter the DNS servers or WIN server IP address. Lease Time: Enter a time value of 1 to 10080 minutes.

Allow Ping from LAN	Enable or disable ping command executed from this port.
DHCP Relay	Enter the remote DHCP server address if DHCP relay is selected.
DNS Proxy	Enable or disable DNS proxy.

For a WAN port (if the device supports this feature), configure the following:

Interface Type	Select the connection type: LAN, WAN, or DMZ.
Connection Type	Select the connection method: DHCP, Static IP, PPPoE, PPTP, or L2TP. For Static IP, enter the IP address/Subnet mask, Gateway IP address and Primary/Secondary DNS servers, and specify whether to keep the original MAC address as well as the MTU size. For PPPoE, select the Address mode: Dynamic IP or Static IP. For static IP, enter the IP address/Subnet mask and PPPoE connection Username and Password. Then specify the Authentication type from one of the following: None, MS-CHAPv2, MS-CHAP, CHAP, PAP, or Auto-negotiate. For Dynamic IP, you don't need to enter the IP address/subnet information but configure all other settings as specified above. For both addressing modes, enter the Service name (optional) and select the Reconnect mode: Always on, or On demand (enter the Maximum idle time to wait before terminating the connection in minutes for this option). Then configure the DNS servers and specify whether to keep the original MAC address as well as the MTU size. For PPTP, if Static IP is selected, enter the following IP address information: IP address/Subnet mask, Gateway IP address, and Static DNS IP address. For both Address modes, enter the PPTP server name and connection Username and Password. For both modes, configure whether MPPE (Microsoft Point-to-Point Encryption (MPPE) will be used and the Reconnect mode: Always on or On demand (enter the Maximum idle time to wait before terminating the connection in minutes for this option). Then configure the DNS servers and specify whether to keep the original MAC address as well as the MTU size. For L2TP, if Static IP is selected, enter the following IP

	address information: IP address/Subnet mask, Gateway IP address, and Static DNS IP address. For both Address modes, enter the L2TP server name and connection Username and Password. For both modes, enter the Secret (optional) and configure the Reconnect mode: Always on or On demand (enter the Maximum idle time to wait before terminating the connection in minutes for this option). Then configure the DNS servers and specify whether to keep the original MAC address as well as the MTU size.
Advanced Settings	Enable or disable the following passthroughs: **Internet Protocol Security (IPsec)** which is used for securing packets exchange at the IP layer. **Point-to-Point Tunneling Protocol (PPTP)** which is used for tunneling the Point-to-Point Protocol (PPP) communication in an IP network. **Layer 2 Tunneling Protocol (L2TP)** which is used for implementing Point-to-Point sessions utilizing multipoint tunneling technique.

5. Click **Save**. Then click **Apply** to apply the settings to the affected device immediately.

Viewing and Configuring VLANs

VLANs allow you to divide the network to different segments. To obtain the current VLAN settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Addressing.** The VLANs are displayed under the VLAN section with the following information:

Name	A name that helps identify this VLAN.
VLAN ID	The assigned VLAN ID.
Untagged/Tagged Ports	The member ports for the untagged VLAN and tagged VLAN .

IP address/Subnet Mask	The IP address/Subnet mask configured for the VLAN.
Captive Portal	The associated Captive Portal page.

To configure a VLAN:

1. Disable the **Use Profile configuration** option.
2. Under **VLAN**, click **Add** to add a new VLAN.
3. Click Apply at the top left to apply the changes to the affected device immediately.

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring IP Management List

The IP Management list displays the IP assignment of the DHCP clients:

Host Name	The host name of the client device.
Interface	The associated interface with the IP assignment.
IP Address	The assigned IP address of the host.
MAC Address	The MAC address of the host.
IPv6 Suffix	The assigned IPv6 suffix, which is the the last 64 bits of an IPv6 address.
IP-MAC Binding	Indicates whether the IP assignment is enforced on the client device with the specified MAC address to prevent the use of other static IP address on this client.
DHCP IP Reservation	Indicates whether this IP assignment is reserved for this client so that it can get the same IP assignment every time it sends a DHCP IP request.

To configure IP management for DHCP clients:

1. Disable the **Use Profile configuration** option.
2. Under **IP Management List**, click **Add** to add a new IP assignment.

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring Routing

Routing determines the path for packet delivery in a network. The routing capabilities vary depending on the device model.

To view the configured routing policies:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Routing**. The configured routing protocols are displayed:

IPv4/IPv6 Static Route

Name	A name that helps identify this route.
Destination	The destination subnetwork IP address.
Subnet Mask	The subnet mask of the destination address. This is only available for IPv4 configuration.
Gateway	The IP address of the gateway or next hop.
Interface	The associated interface for this route.
Metric	The number of hub count.
Active	Enable or disable this route configuration.

IPv4/IPv6 Policy Route

Name	The name that helps identify the route.

Local Gateway	The port of the device that the route would use.
Protocol	The protocols associated with this route.
Source Network	A single IP address or a range of IP addresses that this route will be applied to. “Any” means all source IP addresses.
Destination Network	A single IP address or a range of IP addresses that this route will be applied to. “Any” means all destination IP addresses.
Source Port	The port number used for this type of traffic. ”Any” means all source ports will be used for this service.
Destination Port	The port number used for this type of traffic. ”Any” means all destination ports will be used for this service.
Active	Enable or disable this route configuration.

RIP Configuration

Interface	The interface by which Routing Information Protocol (RIP) information exchange will be performed.
Direction	Indicates inbound, outbound, or traffic for both directions.
Version	The version of the RIP
Authentication	Indicates whether the authentication is enabled.
Active	Enable or disable this route configuration

OSPFV2 Configuration

Interface	The interface assigned to the area defined below.
NSSA	Enable or disable the not-so-stubby area (NSSA) which can import external route information.
Area	The assigned area ID.
Priority	The OSPF priority which is used for determining the OSPF designated router.
Hello Interval	The time interval (seconds) between each hello packet.
Dead Interval	The time (seconds) the device must wait before it declares a neighbor OSPF router down when a hello packet has not been received.
Cost	The cost of the OSPF path.
Authentication	Indicates the authentication method used
LAN Route Exchange	Enable or disable the exchange of LAN routing table.
Active	Enable or disable this OSPF route configuration.

To configure routing policy:

1. Disable the **Use Profile configuration**option.
2. Under each routing protocol supported by the device model, click Add to add a new routing policy.

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring Services

Supported services can be configured individually depending on the features of the gateway.

To view and configure the supported services and network functions:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Network > Services**.

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Managing Traffic

The Traffic Management provides control over certain types of traffic by setting limits on bandwidth and sessions. Note that the availability of this function depends on the capability of the gateway.
To view Traffic Shaping rules configured:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Traffic Management**.

   Under Traffic Shaping, the following is displayed:

Name	The policy name.
Policy Type	Whether the traffic policy is applied to inbound or outbound traffic.
WAN Interface	The WAN port that this policy should be applied to.
Management Type	The metric to define the policy: Rate or Priority. Configure the following if Priority is selected: Low, Medium, or High. Higher priority means the traffic will be allocated with more bandwidth. If Rate is selected, enter the maximum bandwidth and minimum bandwidth (kbps).
Priority/Bandwidth Rate	The priority or the bandwidth configured for the respective management type.

Service	The type of traffic according to the protocol or application service configured.
Traffic Selector Match Type	The criteria for the traffic to which the policy should be applied: IP address, MAC address, or Interface.
Schedule Policy	The schedule policy that makes the policy effective during the designated time frame. Go to **Configure > Schedule policies** for scheduling information and configuration.

Viewing and Managing Session Limiting

To view Session Limiting rules configured:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Traffic Management**.

   Under Session Limiting, the following is displayed:

Name	The policy name.
Source Type	The source address can be configured as a single IP address, an IP address range, or an interface.
Maximum Sessions	The maximum number of sessions allowed (1-999).
Schedule Policy	The schedule policy that makes the policy effective during the designated time frame. Go to **Configure > Schedule policies** for scheduling information and configuration.

Viewing and Managing Custom Warning Pages

To view Custom Warning Page configured:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Traffic Management**.

   Under Custom Warning Page, the following is displayed:

Name	The policy name.
Source Type	The configured warning page to be displayed to users when the maximum limit of sessions has been reached . Go to **Configure > Splash pages** to view all the configured splash pages.
Active	Whether this rule is active or inactive.

To configure Traffic Management:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Traffic Management**.
3. Disable the option **Use Profile configuration.**

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring Captive Portal

The captive portal displays a splash page to wireless users who are required to agree to terms and conditions to use Internet services.
To view Captive Portal configured:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Captive Portal.**

The following information is displayed:

Name	The profile name.
Captive Portal	The authentication method for the users.
Splash Page	The pre-configured splash page which a wireless user must visit prior to using Internet services. The design of the page depends on the use case.
Basic Login	For basic login page, the associated authentication method: a local authentication database or an authentication server system.

3rd party Credentials	The configured third-party credential to be used for login.
SSID/VLANs	A pre-configured SSID/VLAN assigned to this captive portal setting.

To configure Captive Portal:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Captive Portal.**
3. Disable the option **Use Profile configuration.**

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring High Availability

Virtual Router Redundancy Protocol (VRRP) can be utilized to implement fault tolerance and load balancing on a network by designating primary and backup roles among the virtual routers. The primary router is responsible for processing packets sent to a virtual IP address and the backup router takes up the primary role when the primary becomes unavailable. This availability of this feature depends on device model.

To view VRRP settings configured:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > High Availability.** The following is displayed:

VRRP ID	The unique identifier for the VRRP group.
Interface	The interface to which the VRRP configuration would be applied.
IP Address	The virtual IP address.
Node Type	The designated role of the virtual router: Master or Backup.
Priority	The Priority determines the order of selection for a primary virtual router among the backup virtual routers (1-255). Higher number means high priority.

To configure VRRP settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > High Availability.**

3. Disable the option **Use Profile configuration.**

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring Wireless

You can create multiple SSIDs for your wireless network and configure each SSID with unique settings to accommodate different wireless usage scenarios. You can also configure radio settings such as operating mode and channels for different frequencies supported for the device model. Note that this feature is only available for supported models.

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Security Settings

Security features consist of firewall, intrusion prevention, and web content filtering as well as application control.

Note: Changing the Routing mode from Network Address Translation (NAT) to Router (go to Network > Addressing), the Security Firewall's option of Use Profile configuration will be disabled. Moreover, the rules configured for Port forwarding, Port triggering, and 1:1 NAT will be erased.

Firewall

To view a gateway's firewall settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Firewall.**

The following information is displayed:

IPV4/IPv6 FIREWALL RULES

IPv4/Ipv6 Firewall Rules allow or block certain types of traffic that need to be forwarded through the device.

Priority	The assigned priority number (1-998). Lower number means higher priority.
Name	The name of the rule.
Policy	Indicates whether it is a allow or deny rule.

Protocol	The associated protocol for the rule: Any, TCP, UDP, TCP/UDP, or ICMP.
Source Interface	The interface that the traffic is sent from.
Source	A single IP address or a range of IP addresses as the source host. Any means traffic from all IP addresses.
Source Port	The source port number used for this type of traffic. Any means all ports.
Destination	A single IP address or a range of IP addresses as the destination host. Any means traffic destined to all IP addresses.
Destination Port	The destination port number used for this type of traffic. Any means all ports.
Schedule	The associated Schedule Policy.
Active	Indicates whether this rule is enabled or disabled.

Note: The availability of IPv6 Firewall Settings depends on the features of the device model.

Port Forwarding

Port Forwarding redirects traffic entering the WAN to another port on the LAN. This is useful when a certain service is hosted on an interval server on the LAN.

To view Port Forwarding rules:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Firewall.**

The following information is displayed:

Name	The name for the rule.
Mode	Indicates whether the rule is for traffic forwarding or port translation.

Interface	The WAN interface to which this rule should be applied.
Protocol	The associated protocol of this rule: TCP, UDP, or TCP/UDP.
Public Port	The external port associated with this type of traffic or service (1-65535). It can be a single port or a range of ports.
Local IP	The IP address of the local server.
Local Port	The local port used for this service if translation mode is selected.
Allowed Remote IPs	The IP addresses of the remote hosts that this rule will be applied to. Any means all remote hosts.
Active	Indicates whether this rule is enabled or disabled.

Port Triggering

Port Triggering dynamically opens public ports for inbound traffic after certain ports are triggered by a service request.

To view Port Triggering rules:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Firewall.**

The following information is displayed:

Name	The rule's name.
Protocol	The protocol to which the rule is applied: TCP, UDP, or TCP/UDP.
Outgoing Trigger Port	The outgoing port used for this service.
Incoming Trigger Port	The incoming port used for this service.
Active	Indicates whether this rule is enabled or disabled.

1:1 NAT

One-to-one NAT allows a static mapping between an internal IP address and an external IP address.

To configure 1:1 NAT rules:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Firewall.**

   The following information is displayed:

Name	The rule name.
Interface	The WAN interface that this rule should be applied to.
WAN IP	The WAN IP address as the external IP address for translation.
Local IP	The local IP address as the interval IP address for translation.
Protocol	Indicates the associated protocol of this rule: TCP, UDP, or TCP/UDP.
Port	The port used for this traffic type.
Allowed remote IPs	The IP addresses of the remote hosts that this rule will be applied to. Any means to allow all remote hosts.

To configure Firewall rules:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Firewall.**
3. Disable the option **Use Profile configuration.**

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring IPS Settings

To view Intrusion detection and prevention settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security >IPS.**
3. Disable the option **Use Profile configuration.**

If the device is equipped of intrusion detection functions, you can enable or disable the following services:

Intrusion Detection	Enable intrusion detection. And select the WAN and LAN interfaces that the IPS and IDS should be implemented.
Intrusion Prevention	Enable intrusion prevention. And select the WAN and LAN interfaces that the IPS and IDS should be implemented.
Stealth Mode	This mode protects your device from Internet intrusion by not responding to unauthorized requests.
Block TCP Flood	Enable to block TCP flooding to WAN.
Bock UDP Flood	Enable to block UDP flooding to LAN.
Filter Check Mode	Enable the TCP filtering check mode.
Allow ICMP Traffic	Enable to allow packets of Internet Control Message Protocol to pass through.
DoS Attacks	Denial-of-Service (DoS) attacks encompass SYN Flood, ICMP Flood, and Echo storm. Configure the flood rate of each attack in packets/second for detection.

4. Click **Apply** at the top left to apply the settings to the affected devices immediately.

Viewing and Configuring Web Content Filter

The Web Content Filter is used to prevent access to unwanted websites. It allows you to create profiles that can take effective during the designated time frame and block websites belonging to a certain category.

Web Content Filter List

To view the Web Content Filter List:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security >Web Content Filter.**

Under Web Content Filter List, the following is displayed:

Name	The name for the filtering rule.

Policy	State whether this is a allow or block policy.
Schedule	The pre-configured scheduling.
Scope	The specified hosts or the whole network that this rule will be applied to.
Filtering Type	The type consists of a variety of categories, URLs, and custom groups to restrict the access to defined websites.
Active	State whether the rule is active.

Under Custom Warning Page, you can obtain the configured warning page that will display related messages when a restricted webpage is being visited. The following is displayed:

Name	Enter a name for this configuration.
Source Type	The pre-defined warning page to be displayed.
Actions	State whether the rule is active.

Under **Custom Group List,** you can obtain the Custom group which will be used to define the content filtering type above:

Group Name	The name for the custom group.
URLs	If URL filtering is used, it shows the name and keyword for the website. This blocks access to websites based on a website's domain name (e.g. google.com) and keywords with matching URLs. For example, keyword "ABC" will block "www.ABC.com" and "xxx.ABC.com" and other URLs containing ABC.
Category Filtering	If Category filtering is used, it shows the pre-defined categories to block access to.
In Use	State whether this rule has been activated.

To configure Firewall rules:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Web Content Filter.**
3. Disable the option **Use Profile configuration.**

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring Application Control

The Application Control is used to restrict certain communication of applications. It allows you to create profiles that can take effective during the designated time frame and prevent traffic of certain applications from being transferred.

Auto Upgrade

Enable automatic upgrade of application signature database and select the update schedule by entering the upgrade frequency in minutes or setting a specified time of a designated weekday for weekly updates.

To add an application control rule:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Application Control.**
3. Under Application Control List, the following information is displayed:

Name	The policy name.
Policy	State whether this is a allow or block policy.
Schedule	The pre-configured schedule. For configured scheduling methods, go to **Configure > Schedule policies**.
Scope	The specified hosts or the whole network that this rule will be applied to.
Application	State whether the filtering rule is based on a single application, or a single application from a pre-defined category, or a custom group of selected applications.
Active	State whether the application control policy is active or inactive.

Under **Custom Group List,** you can obtain Custom Group defined which will be used to define the application type above:

Group Name	The name of the custom group.
Application List	The selected applications for the custom group.
In Use	State whether this rule has been activated.

To configure Application Control:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Application Control.**
3. Disable the option **Use Profile configuration.**

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

VPN Settings

A Virtual Private Network (VPN) builds an encrypted connection between endpoints over a public network utilizing tunneling techniques. VPN can be configured only if your device supports this feature.

Site to Site VPN

The site-to-site VPN is a technique that allows connectivity between the offices located at multiple locations by setting up an IPsec tunnel over the Internet to access the intranet. In short, a site-to-site VPN builds a secure path over an insecure path. The Nuclias cloud gateway allows users to establish a VPN tunnel without manually entering the tunnel endpoint details and the local/remote networks. Instead, the Nuclias cloud gateway maintains these details and lets users select the networks.

Configuring Quick VPN

Quick VPN is a Nuclias auto-provisioning site-to-site VPN technology that allows you to quickly and easily build VPN tunnels between Nuclias gateway devices without tedious manual VPN configuration. If it is disabled, set up VPN manually at Manual VPN Settings to establish VPN connection with other partners.

To view or configure Quick VPN settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **VPN > Site-to-site VPN**.s
3. Select the topology: Hub-and-Spoke or Full Mesh. If Full Mesh is selected, the VPN establishes the Gateway-to-Gateway IPsec tunnel with other devices registered in the same or different sites of the same organization. To establish a tunnel with a particular remote device, enable the Join member field in the Remote VPN participants table. Once

the tunnel configuration is pushed to the remote peers, traffic gets initiated by the user, and a tunnel is established between the remote peers.

4. If Hub-and-Spoke is selected, specify the role to be either a hub or spoke. If Spoke is selected, you can choose hubs to build VPN tunnels in the Exist hubs table. In addition, it lists the Exist hub devices available with the option of Primary Hub. If you enable the Primary Hub field, the selected hub will be the primary hub for the spoke and can communicate to all the spoke devices linked to this hub. At a time, you can enable only one primary hub. If Hub is selected, then VPN tunnels will be built among hubs and dependent spokes.
5. If Hub mode is selected, enable or disable VPN connection with a remote peer. You may also choose to designate a remote peer as a backup hub.
6. If Spoke mode is selected, you can choose to designate a remote peer as the primary hub.
7. Click **Apply**.

Quick VPN Settings

In the Local networks section, if you have multiple subnets, you can specify which one subnet participates in the VPN, i.e., traffic from the enabled subnet will be encrypted by the IPsec VPN. All local subnets must be unique within the VPN topology

Note: A list of Quick VPN connections will be displayed in the **Summary > VPN Status** page. Select Quick VPN (Full Mesh and Hub-and-Spoke) as the Display VPN type.

Configuring Manual VPN

To view or configure Manual VPN settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **VPN > Site-to-site VPN**. Enter the following:

Connection Name	Enter a name for this VPN connection (1-64 characters).
IKE Profile	Select the IKE profile which contains security settings that will be used for the VPN connection.
Local Network	The scope of the local network to which the VPN connection will apply.
Local Network	Enter a local IP address or subnetwork of the local network to participate in the VPN. If Single IP is selected, enter the IP address. If Subnet is selected, enter the IP address and subnet mask (or prefix for IPv6). Select Any for the entire local network.

Remote Network	Enter a remote IP address or subnetwork of the remote network to participate in the VPN. If Single IP is selected, enter the IP address. If Subnet is selected, enter the IP address and subnet mask (or prefix for IPv6). Select Any for the entire remote network.
Outgoing Interface	Select an interface to which the VPN connection will use.
Remote Gateway	Select FQDN or Static IP for configuring the remote gateway address. Then enter the IP address or FQDN address.
Keep-alive	Enable or disable keep-alive for VPN reconnection. If enabled, enter the source and destination IP address as well as the detection period in seconds (10-199) and retry after the number of failures (3-99).
Idle Timeout	Enter the maximum length of time that the VPN connection can stay active when three is no traffic.
Dead Peer Detection	Enable detection for dead peers. If enabled, enter the detection interval (10-999 seconds) and Retry after failure (3-99 times).
NetBIOS Broadcast	Enable or disable NetBIOS broadcast from one end to be forwarded to the other end of the VPN connection.
Outgoing Backup Interface	Select an interface to which the VPN connection will use as a backup if Dead Peer Detection is enabled.
Remote Backup Gateway	Select FQDN or Static IP for configuring the remote gateway address if Dead Peer Detection is enabled.
IKE Backup Profile	Select the IKE profile which contains security settings that will be used for the backup VPN connection if Dead Peer Detection is enabled.

To add an IKE profile,enter the following:

Profile Name	Enter a name for this IKE profile.

IKE Version	Select the IKE version: v1 or v2.
IKE phase-1 Settings	
Exchange Mode	Select the exchange mode: Aggressive or Main.
Local Identifier Type	Select the identification method: Local WAN IP, FQDN, or User-FQDN. And enter the identifier according to the selected method.
Remote Identifier Type	Select the identification method: Remote WAN IP, FQDN, or User-FQDN. And enter the identifier according to the selected method.
DH Group	Select a Diffie-Hellman (DH) Group for key exchange. These groups vary in prime key lengths.
Encryption Algorithm	Select encryption algorithm(s) for ESP packets encryption.
Authentication Algorithm	Select authentication algorithm(s). And enter the SA lifetime in seconds (300-604800).
Authentication Method	Select the authentication method. Then enter the preshared key or select a certificate depending on the method selected. Go to **Settings > Certificate Management** for Certificate list.
Extended Authentication	Enable this and select extended authentication method: Authentication server, IPsec host, or Local authentication. Depending on the method, select the corresponding RADIUS/ LDAP/POP3/Active Directory/NT Domain server or Local Authentication profile or enter the username and password for IPsec host. Refer to **Configure > Authentication > Local Authentication list** and **Authentication servers** for Authentication profiles and servers.
IKE phase-2 Settings	

Protocol Selection	Select either ESP or AH. If Encapsulating Security Payload (ESP) is selected, select the Encryption algorithm to encrypt or decrypt ESP packets.
Authentication Algorithm	Select the authentication algorithm for header packets validation.
SA Lifetime (sec.)	Enter the SA lifetime (300-604800 seconds) for the active duration of a VPN tunnel.
Perfect Forward Secrecy	Enable or disable the Perfect Forward Secrecy. If enabled, the VPN communication is better protected with renewed negotiation of key values in the exchange.
DH Group	If the above PFS is enabled, select the DH group for key establishment.

3. Click **Apply** at the top.

Note: A list of Quick VPN connections will be displayed in the **Summary > VPN Status** page. Select Quick VPN (Manual) as the Display VPN type.

Client to Site VPN

An IPsec policy can be defined between this router and another gateway to create network-to-network IPsec tunnels. To configure IPsec VPN Server settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **VPN > Client-to-site VPN**. Enter the following:

Connection Name	Enter a name for this configuration
IKE	Select a pre-configured IKE profile for this VPN configuration.
Local Network	Enter the IP address and subnet mask of the local network. Select Any to not restrict to a single subnet.
Tunnel Mode	Select either full or split tunnel for the mode. Select Full tunnel or Split tunnel. The Split mode will split DNS requests among DNS servers. It allows you to create two zones for the same domain, one to be used by the internal network, the other used

	by the external network .For Split tunnel, enter the Split Domain names.
DHCP Relay	Enable or disable DHCP relay. If enabled, enter the IP address of the relay gateway. If disabled, enter the following IP address information.
Starting IP Address/ Ending IP Address	Enter the range of the IP addresses for VPN connections.
Primary/Secondary DNS	Enter the primary and optional secondary DNS servers.
Primary WINS Server/ Secondary WINS Server	Enter the primary and optional secondary Windows Internet Naming Service (WINS) servers.
Outgoing Interface	Select the WAN interface to which the IPsec VPN should apply.
Split DNS	Enable or disable Split DNS if Split tunnel is selected. And enter the domain names if enabled (3-253 characters).
NetBIOS Broadcast	Enable or disable NetBIOS information to be forwarded to the other endpoint of the VPN tunnel. The information is used for name resolution in Windows networking.

To add an IKE profile, enter the following:

Profile Name	Enter a name for this IKE profile.
IKE Version	Select the IKE version: v1 or v2.
IKE phase-1 Settings	
Exchange Mode	Select the exchange mode: Aggressive or Main.

Local Identifier Type	Select the identification method: Local WAN IP, FQDN, or User-FQDN. And enter the identifier according to the selected method.
Remote Identifier Type	Select the identification method: Remote WAN IP, FQDN, or User-FQDN. And enter the identifier according to the selected method.
DH Group	Select a Diffie-Hellman (DH) Group for key exchange. These groups vary in prime key lengths.
Encryption Algorithm	Select encryption algorithm(s) for ESP packets encryption.
Authentication Algorithm	Select authentication algorithm(s). And enter the SA lifetime in seconds (300-604800).
Authentication Method	Select the authentication method. Then enter the preshared key or select a certificate depending on the method selected. Go to **Settings > Certificate Management** for Certificate list (refer to Certificate Management) .
Extended Authentication	Enable this and select extended authentication method: Authentication server, IPsec host, or Local authentication. Depending on the method, select the corresponding RADIUS/ LDAP/POP3/Active Directory/NT Domain server or Local Authentication profile or enter the username and password for IPsec host. Refer to **Configure > Authentication > Local Authentication list** and **Authentication servers** for Authentication profiles and servers.
IKE phase-2 Settings	
Protocol Selection	Select either ESP or AH. If Encapsulating Security Payload (ESP) is selected, select the Encryption algorithm to encrypt or decrypt ESP packets.
Authentication Algorithm	Select the authentication algorithm for header packets validation.

SA Lifetime (sec.)	Enter the SA lifetime (300-604800 seconds) for the active duration of a VPN tunnel.
Perfect Forward Secrecy	Enable or disable the Perfect Forward Secrecy. If enabled, the VPN communication is better protected with renewed negotiation of key values in the exchange.
DH Group	If the above PFS is enabled, select the DH group for key establishment.

3. Click **Apply** at the top.

PPTP/L2TP

A PPTP server is available on the router for LAN and WAN PPTP client users to access.

To configure PPTP/L2TP Server settings

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **VPN > PPTP/L2TP**. Enter the following:

Name	Enter a name for the configuration profile of the server (1-64 characters).
Server Type	Select either PPTP or L2TP.
Routing Mode	Select either NAT or Router.
Starting IP Address/ Ending IP Address	Enter the LAN IP address range to be assigned to the VPN clients.
Authentication Server	Select the authentication server. Depending on the method, select the corresponding RADIUS/LDAP/POP3/Active Directory/NT Domain server or Local Authentication profile. Go to **Configure > Authentication > Local Authentication list** and **Authentication Servers** for Local authentication profiles and authentication servers list.
Authentication Protocol	Select the authentication protocol(s): All, PAP, CHAP, MS-CHAP, and MS-CHAPv2.

Encryption	[PPTP only] Select the encryption method(s) for PPTP: For PPTP, select All, MPPE 40 bit, MPPE 128 bit, or Stateful MPPE. The Microsoft Point-to-Point (MPPE) encrypts data for PPTP VPN.
Idle Timeout	The length of time (seconds) to wait before terminating a VPN session (300-1800).
NetBIOS	[PPTP only] Enable or disable NetBIOS, which is used for name resolution in Windows networking, if there is a WINS server set up in your LAN. If enabled, enter the Windows Internet Naming Service (WINS) server IP address. This option is only available for PPTP.
Enable Secret Key	[L2TP only] Enable or disable the secret key (or preshared key) with 8-63 characters which will be required for client VPN settings.
L2TP over IPsec	[L2TP only] Enable or disable L2TP over Internet Protocol Security (IPsec), on which L2TP relies for secure packets exchange.
IKE Version: Configure Internet Key Exchange (IKE) if L2TP Over IPsec is enabled.	
IKE version	Select the IKE version for configuration.
IKE phase-1 settings	
Exchange Mode	Select the exchange mode: Aggressive or Main.
Local Identifier Type	Select the identification method: Local WAN IP or FQDN. And enter the identifier according to the selected method.
Remote Identifier Type	Select the identification method: Remote WAN IP or FQDN. And enter the identifier according to the selected method.
DH Group	Select a Diffie-Hellman (DH) Group for key exchange. These groups vary in prime key lengths.
Encryption Algorithm	Select encryption algorithm(s) for ESP packets encryption.

Authentication Algorithm	Select authentication algorithm(s). And enter the SA lifetime in seconds (300-604800).
Authentication Method	Select the authentication method. Then enter the preshared key or select a certificate depending on the method selected. Go to **Settings > Certificate Management** for Certificate list.
Extended Authentication	Enable this and select extended authentication method: Authentication server, IPsec host, or Local authentication. Depending on the method, select the corresponding RADIUS/ LDAP/POP3/Active Directory/NT Domain server or Local Authentication profile or enter the username and password for IPsec host. Refer to **Configure > Authentication > Local Authentication list** and **Authentication servers** for Local authentication profiles and authentication servers.
IKE phase-2 settings	
Protocol Selection	Select either ESP or AH. If Encapsulating Security Payload (ESP) is selected, select the Encryption algorithm to encrypt or decrypt ESP packets.
Authentication Algorithm	Select the authentication algorithm for header packets validation.
SA Lifetime (sec.)	Enter the SA lifetime (300-604800 seconds) for the active duration of a VPN tunnel.
Perfect Forward Secrecy	Enable or disable the Perfect Forward Secrecy. If enabled, the VPN communication is better protected with renewed negotiation of key values in the exchange.
DH Group	If the above PFS is enabled, select the DH group for key establishment.

PPTP VPN Client can be configured on this router to access a remote network.

To configure a VPN client,enter the following:

Name	Enter a name for the PPTP/L2TP configuration profile of the client (1-64 characters).
Client Type	Select either PPTP or L2TP.
VPN Server	Enter the IP address or FQDN of the VPN server
Tunnel Type	Select Full tunnel or Split tunnel. Split tunnel mode only sends traffic to the private LAN with pre-specified client routes and give the client access to specific private networks, thereby allowing access control over specific LAN services.
Remote Network/ Netmask	Enter the remote network and netmask if split tunnel is selected.
Username/Password	Enter the username and password required for connection.
Encryption	For L2TP server, enter the Secret key (8-63 characters) if encryption is enabled. This value must match the preshared key value entered on the VPN server.
MPPE	Enable the Microsoft Point-to-Point Encryption (MPPE), which encrypts data for VPN communication.
Idle Timeout	For PPTP, enter the length of time (seconds) to wait before terminating a session.
Reconnect Mode	For L2TP, select On demand or Always on. Enter the Maximum idle time in seconds (300-1800) to wait before dropping an idle connection.
L2TP over IPsec	Enable or disable L2TP over Internet Protocol Security (IPsec), on which L2TP relies for secure packets exchange.
IKE Version: Configure Internet Key Exchange (IKE) if L2TP Over IPsec is enabled.	
IKE version	Select the IKE version for configuration.
IKE phase-1 settings	

Exchange Mode	Select the exchange mode: Aggressive or Main.
Local Identifier Type	Select the identification method: Local WAN IP or FQDN. And enter the identifier according to the selected method.
Remote Identifier Type	Select the identification method: Remote WAN IP or FQDN. And enter the identifier according to the selected method.
DH Group	Select a Diffie-Hellman (DH) Group for key exchange. These groups vary in prime key lengths.
Encryption Algorithm	Select encryption algorithm(s) for ESP packets encryption.
Authentication Algorithm	Select authentication algorithm(s). And enter the SA lifetime in seconds (300-604800).
Authentication Method	Select the authentication method. Then enter the preshared key or select a certificate depending on the method selected. Go to **Settings > Certificate Management** for Certificate list.
Extended Authentication	Enable this and select extended authentication method. Enter the Username and Password if IPsec host is selected.
IKE phase-2 settings	
Protocol Selection	Select either ESP or AH. If Encapsulating Security Payload (ESP) is selected, select the Encryption algorithm to encrypt or decrypt ESP packets.
Authentication Algorithm	Select the authentication algorithm for header packets validation.
SA Lifetime (sec.)	Enter the SA lifetime (300-604800 seconds) for the active duration of a VPN tunnel.
Perfect Forward Secrecy	Enable or disable the Perfect Forward Secrecy. If enabled, the VPN communication is better protected with renewed negotiation of key values in the exchange.

DH Group	If the above PFS is enabled, select the DH group for key establishment.

3. Click **Save**.

Note: A list of PPTP/L2TP connections will be displayed in the **Summary > VPN Status** page.

OpenVPN

OpenVPN allows peers to authenticate each other using certificates, or username/password. When used in a multiclient-server configuration, it allows the server to release an authentication certificate for every client, using signature and Certificate authority. An OpenVPN can be established through this router.

To configure OpenVPN settings

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **VPN > OpenVPN**. Enter the following:

Mode	Select the mode for the OpenVPN: Server, Client, or Access server client.
Upload Access Server Client	[Access Server Client mode only] Upload a configuration file which contains server and client IP address information if Access server client mode is selected. In access server client mode, the user has to download the auto login profile from the OpenVPN Access Server and upload the same to connect.
CRL Certificate	[Access Server Client mode only] Openvpn provides CRL authentication using CRL certificate. You can upload the required certificates by enabling it it first.
VPN Network/Netmask	[Server mode only] Enter the network IP address/netmask of the VPN. This is only available for the Server mode.
Server IP/Failover Server IP	The IP address or FQDN of the VPN server and failover server. This is only available for the Client mode.
Duplicate CN	[Server mode only] Enable or disable the duplicate CN to allow or disallow the same certification for multiple clients. This is only available for the Server mode.

Port	Enter the port number for VPN communication. The default is 1194.
Tunnel Protocol	Select the protocol for tunneling: TCP or UDP.
Encryption Algorithm	Select the encryption method: AES-128, BF-CBC, AES-192, or AES-256.
Hash Algorithm	Select the hash algorithm: SHA1, SHA256, or SHA512.
Tunnel Type	[Server mode only] Select the tunnel type: Full or Split. If Split is selected, enable or disable the client-to-client communication. Full Tunnel mode sends all traffic from the client across the VPN tunnel to the router. Split Tunnel mode only sends traffic to the private LAN with specified client routes. This is only available for Server mode configuration.
User-based Authentication	Enable or disable user-based authentication. If this is enabled, select the user profiles for Local authentication if server mode is used (refer to Local Authentication). If client mode is used, enter the username and password for VPN connection. Also select a certificate for TLS key if TLS authentication is used (refer to Certificate Management).
Certificate Verification	Enable or disable the use of certificate for verification.
Certificate	Select an available certificate from the list. The content of the certificate will be loaded in the field below.
TLS Authentication Key	Enable or disable the TLS authentication. If enabled, select an TLS authentication key from the certificate list. To obtain the certificate list, go to **Settings > Certificate Management**.
DH Key	Select a DH key from the certificate list. This is only available for Server mode configuration. To obtain certificate list, go to **Settings > Certificate Management**
Server Policies	Enable or disable the server policy. Enter the server policy and add a new server policy to permit or block networks for VPN connections. These policies can be applied to a specific IP

	address or IP networks on the LAN and can be enforced on the specified scope according to the supported features of the router. The List of Available Policies can be filtered based on whether it applies to a user, group, or all users (global). To add a new server policy, enter the following: Policy name: Give a name for this policy. Policy: Select whether it is a Deny or Permit policy. Scope: Select whether it is a global policy or to be applied for certain users using Local authentication. Select the user profile if Local authentication is selected. Apply policy to: Select whether to apply this policy to a single IP address or a subnet work and enter the required IP address and/or the Subnet mask and the port number. ICMP: enable or disable Internet Control Message Protocol (ICMP) traffic in VPN connections.
Remote Networks	If this is enabled, click Add to add a remote network configuration: enter a name for the configuration and the remote network IP address and subnet mask.
Port	Enter the port number (1-65535). This can be a single port or a range of ports, e.g. 3000-3200.
ICMP	Enable or disable the use of ICMP in the VPN communication.

OpenVPN provides authentication using certificates. This system will allow you to configure client list using **Local Authentication list (refer to Local Authentication)** and centrally manage the client certificates (refer to Certificate Management).To configure Client list for Server mode configuration:

1. Under Client list, click **Import**. The **Import users from local authentication list** page displays.
2. Select a pre-configured local user profile or click **Add local authentication** and configure a local user profile by specifying the following: the Local Authentication profile name, the Access level, Managed Sites, and the username and password for each new user. You can use the Bulk import function to upload a CSV file containing the user information to add multiple users at once. Refer to **Configure > Authentication > Local Authentication list** for more information.

3. Click **Save.** Once a Local authentication profile is imported successfully, you can manage the clients' certificates in the Certificate Management page (go to **Settings > Certificate management**) .

To configure OmniSSL Portal Layout for Server mode configuration:

OmniSSL facilitates the client installation from the device via the instructions on the portal page and is an enhancement to the existing OpenVPN. The enhancements allow the VPN tool to be used via mobile devices and eliminate browser and Java dependencies.

1. Under OmniSSL Portal Layout, click **Add**. The **Add portal layout configuration** page displays.
2. Enter a name for the profile and select a pre-defined login page for OmniSSL. Refer to **Configure > Splash pages** for more information. The Splash pages allow you to create a custom page that is presented upon authentication to the remote OmniSSL users.
3. Click **Save.**

Note: A list of OpenVPN connections will be displayed in the **Summary > VPN Status** page.

GRE Tunnel

GRE tunnels allow for broadcast traffic on the LAN of the router to be passed over the internet and received by remote LAN hosts.

To view or configure GRE Tunnel settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **VPN > GRE Tunnel**. Enter the following:

Name	The name for the GRE Tunnel configuration.
Interface	Select the WAN interface to create this tunnel with from the drop-down menu.
GRE Tunnel IP/ Subnet Mask	Enter the IP address/subnet mask of this endpoint. It will be referenced in the other router's static route as the Gateway IP address.
Remote IP	Enter the WAN IP address of the endpoint router.
Static Route Configuration	IP address/Subnet mask: Enter the destination IP address/subnet mask of the static route from the remote LAN subnet. Gateway IP address: Enter the GRE tunnel IP of the terminating router that manages the remote LAN.

3. Click **Save.**

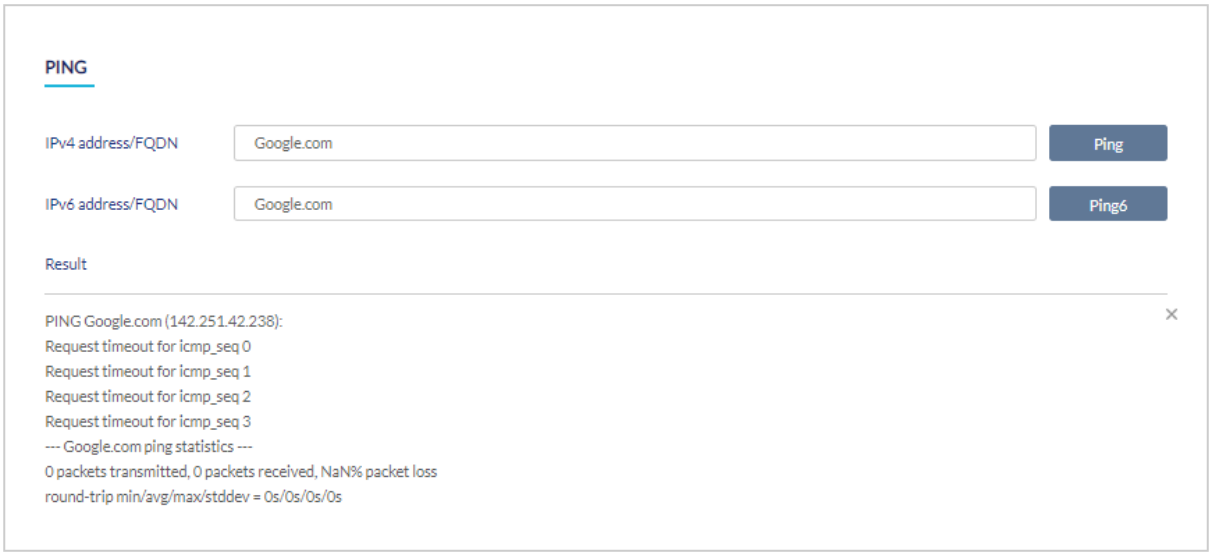
4. Click **Apply** at the top left to apply the settings to the affected device immediately.

Note: The GRE connection status will be displayed in the **Summary > VPN Status** page.

Tools

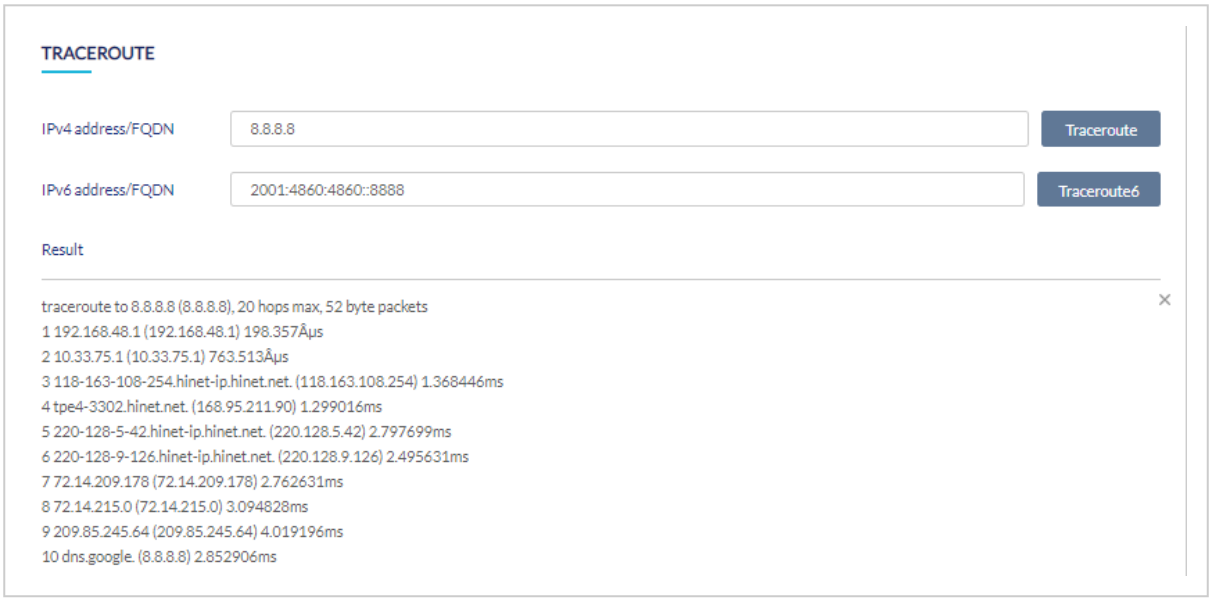
Performing a Device Ping Test

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Tools** tab in the top-right of the screen.
3. In the IPv4 or IPv6 address/FQDN field in the Ping section, enter a valid IP address or FQDN.
4. Click **Ping** for IPv4 addresses or **Ping6** for IPv6 addresses of the remote hosts. The results will be displayed as shown below:



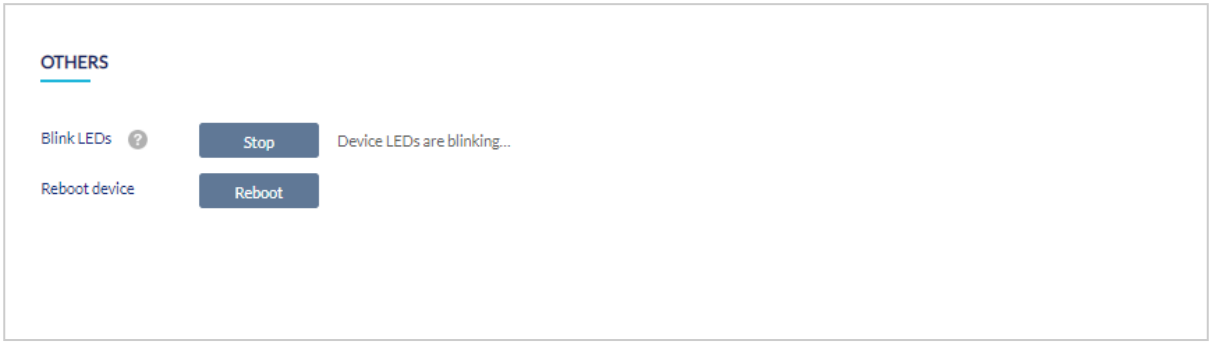
Performing a Traceroute Test

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Tools** tab in the top-right of the screen.
3. Under Traceroute, enter a valid IP address or FQDN in the IP address/FQDN field.
4. Click **Traceroute** for IPv4 addresses or **Traceroute6** for IPv6 addresses of the remote hosts. The results will be displayed as shown below:



Performing LED Blinking and Device Reboot

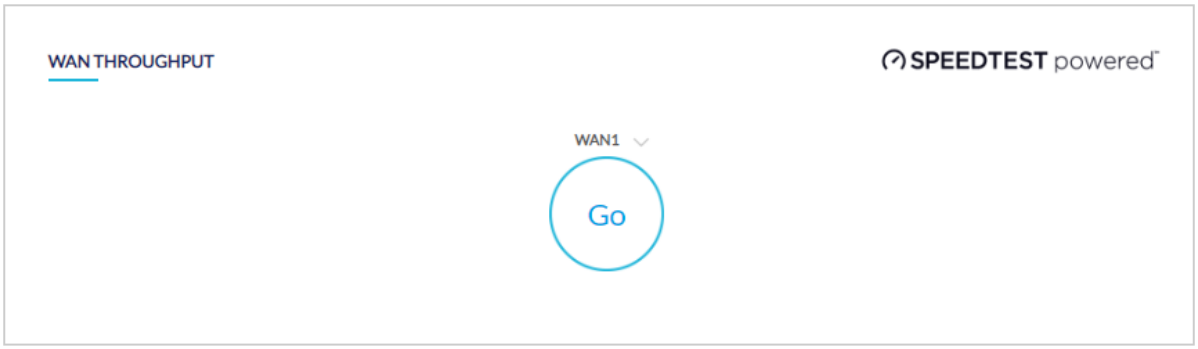
1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Tools** tab in the top-right of the screen.
3. In the Others section, click **Reboot** to reboot the device. Or click **Start** to start blink LEDs on the device. Click **Stop** to top blinking LEDs.



Note: Please refer to the respective device's manual for the status of LED indicators.

Performing WAN Throughput Test

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Tools** tab at the top right of the screen.
3. In the WAN Throughput section, click **Go**. The upload and download speed will be displayed.



Exporting or Importing Device Settings

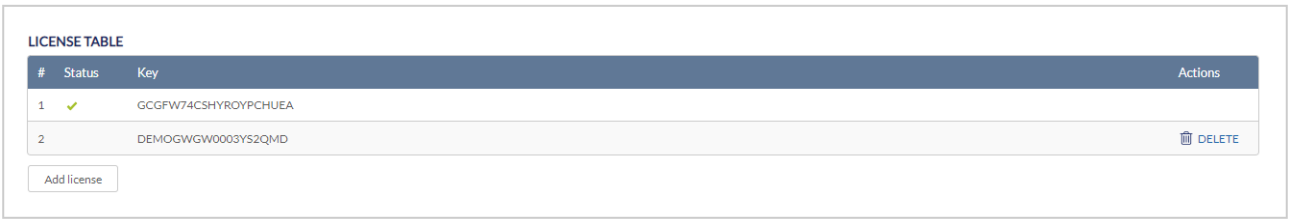
The device setting metadata can be exported as a single CSV file and it can be later imported for configuration restoration. To export device settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Tools** tab at the top right of the screen.
3. In the Export and Import Device Settings section, click **Download**. The exported file will be downloaded to your browser's default download folder.

License

Adding a License Key to a Device

1. Navigate to **Monitor > Gateway > Devices** 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 > Gateway > Devices** 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 reclassify it as Unused in the license

management inventory.

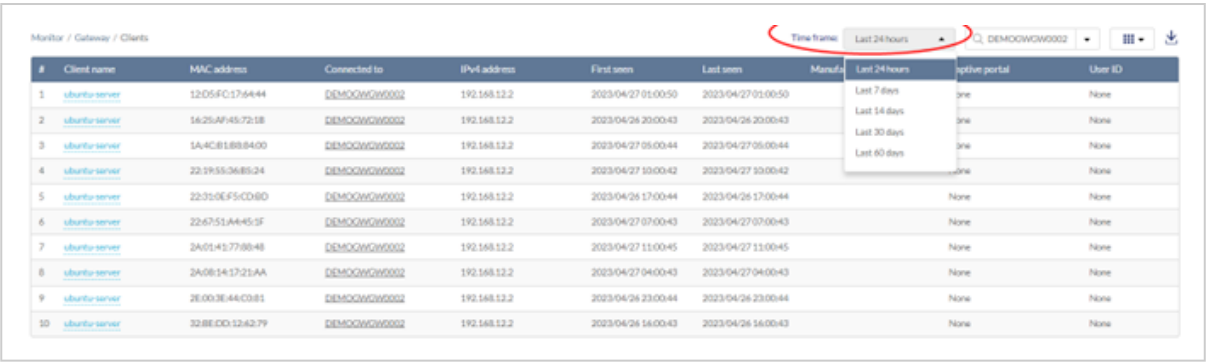


Clients

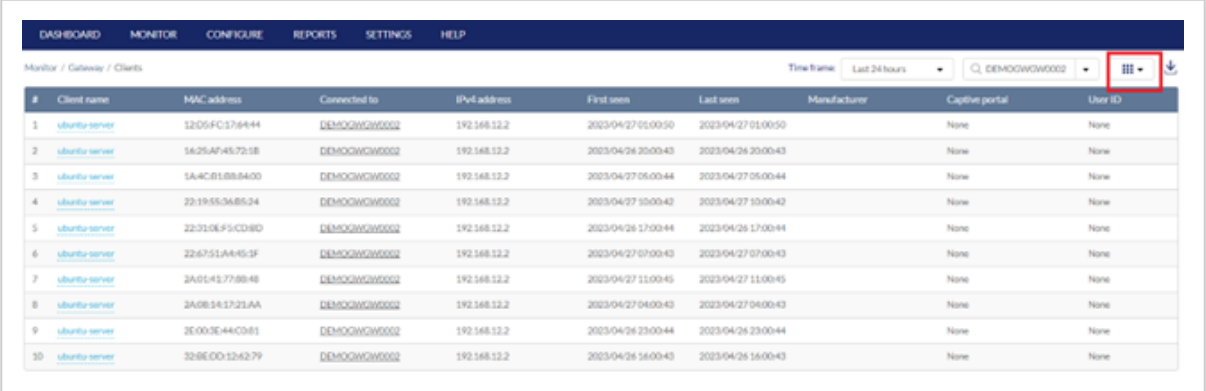
From the Clients window, you can consult a detailed overview of all currently connected devices with additional information including status, VLAN, and general settings.

Customizing the Client Monitor Overview

1. Navigate to **Monitor > Gateway > Clients**. The client list for all gateways will appear.
2. Select a time frame from the drop-down menu to define the time frame that the device was detected online.



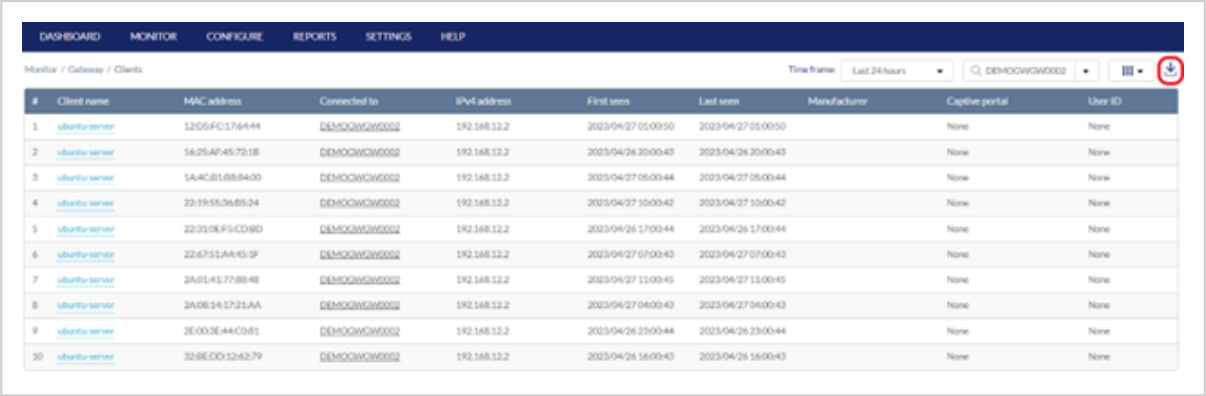
3. Click the parameter filter icon.



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

Downloading Client Monitoring Logs

1. Navigate to **Monitor > Gateway > Clients**.
2. From the client monitoring logs, click the download icon in the top-right.



Event Log

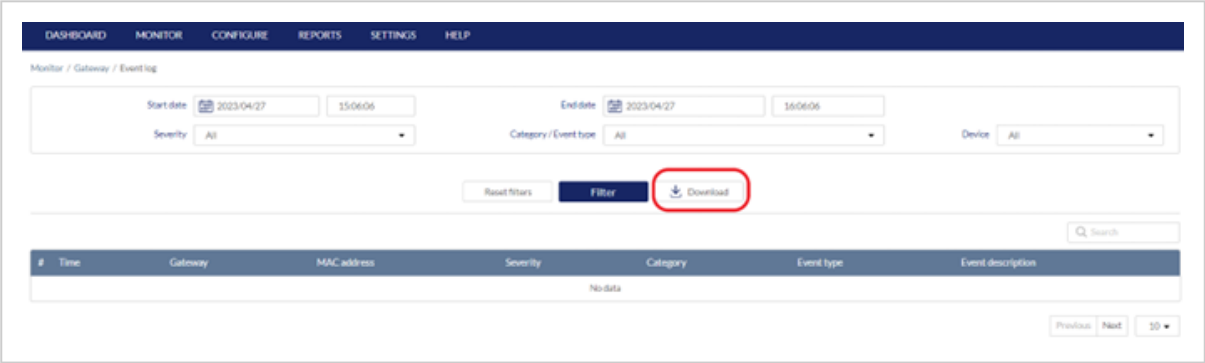
From the Event Logs window, you can consult a detailed log of events occurring on the network. You can also define event filter parameters, including event type and time period.

Filtering Event Log Parameters

1. Navigate to **Monitor > Gateway > Event Log**.
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 Category/Event type drop-down menu and select the event types to display. Select All to show all event types.
6. Click the Device drop-down menu and select a device to filter the results. Select All to show all event logs for all devices.
7. Click **Filter** to display all events matching the defined parameters. Click **Reset filters** to reset all currently set parameters.

Downloading Event Logs

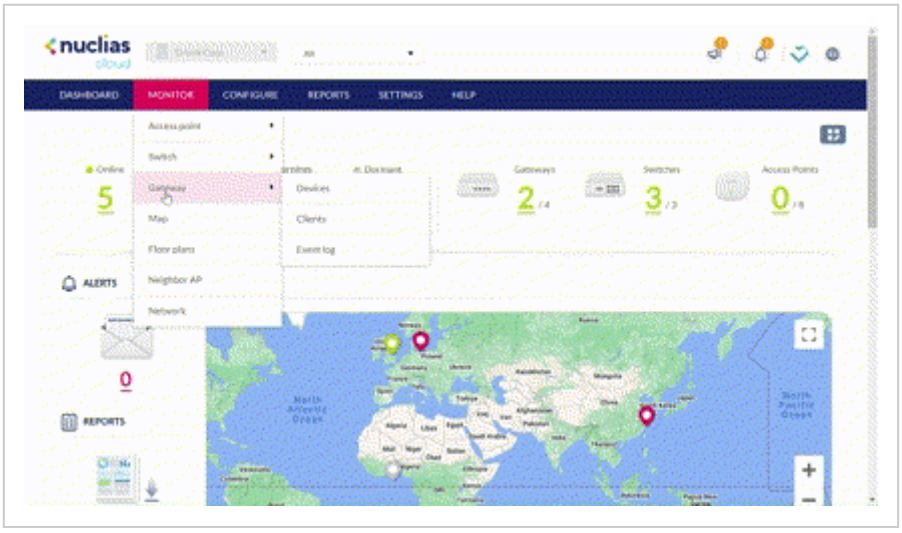
1. Navigate to **Monitor > Gateway > Event Log**.
2. From the event log list, click **Download**.


DASHBOARD
MONITOR
CONFIGURE
REPORTS
SETTINGS
HELP
Monitor / Gateway / Event log
Start date
2023/04/27
15:06:06
End date
2023/04/27
16:06:06
Severity
All
Category / Event type
All
Device
All
Reset filters
Filter
Download
Search
Time
Gateway
MAC address
Severity
Category
Event type
Event description
No data
Previous
Next
10

Event Log

Devices

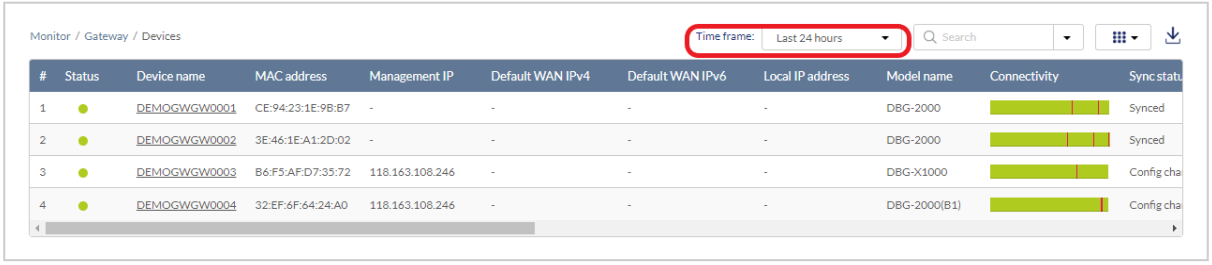
From the Devices window, you can consult a detailed log of events occurring on the network. You can also filter events using specific event filter parameters, including event type and time period.



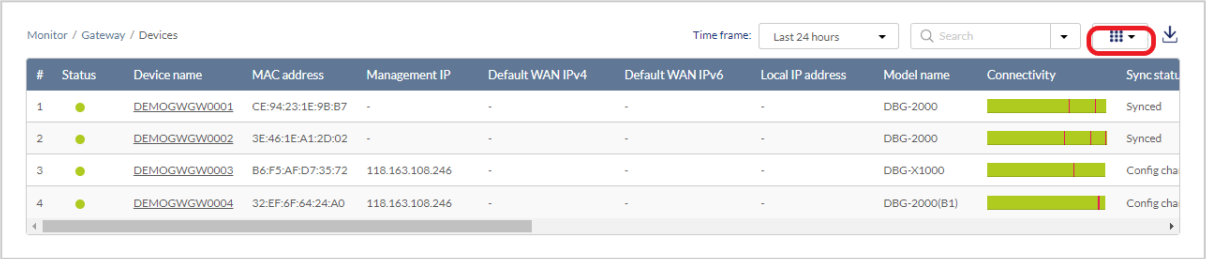
The Device Monitor

Customizing the Device Monitor Overview

1. Navigate to **Monitor > Gateway > Devices**.
2. Select a time frame from the drop-down menu to set the duration for connectivity information.



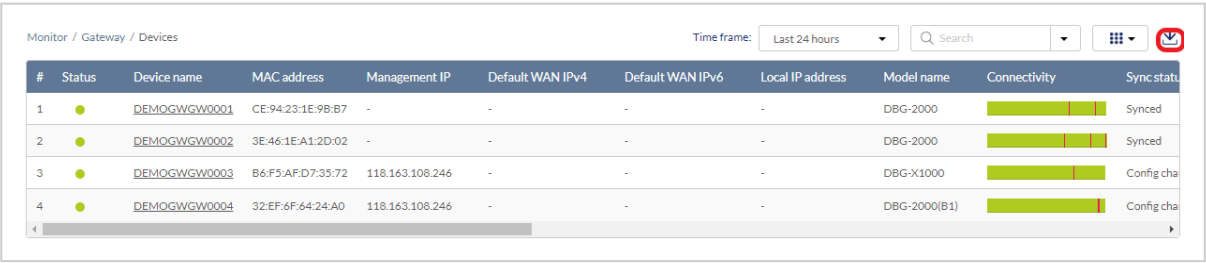
3. Click the filter parameter icon.



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

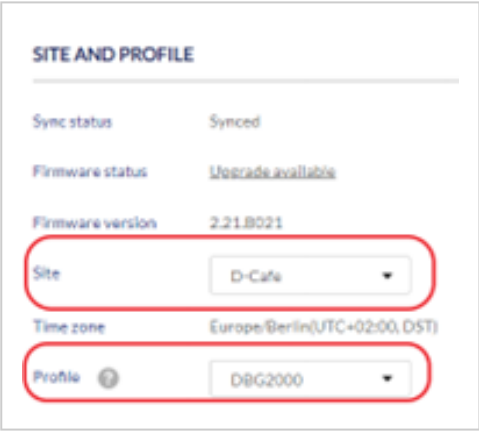
1. Navigate to **Monitor > Gateway > Devices**.
2. From the device list, click the **Download** icon in the top-right to export the table listing as a CSV file.



Device Basic Settings

Changing the Device Site and Profile

1. Navigate to **Monitor >Gateway > Devices** and select a device from the list.
2. Select the **Basic** tab at the top.
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 **Save**.

The Performance Summary

Viewing and Customizing the Gateway Performance Summary

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Summary** tab. Click the tabs at the top to obtain additional information described below:

Status	Provides connection information for the device along with basic port configuration and traffic statistics for each port. You can also obtain Internet usage for both download and upload data in a specified time frame.
Statistics	Provides reports of the number of connected clients in the selected time frame. You can also obtain reports of WAN port usage and the whole Internet usage as well as VPN usage.
DHCP	Provides the utilization rate of each configured DHCP subnet. It also lists the DHCP leases history.
VPN Status	Provides VPN connection statistics. The page lists the active VPN association or connections, the traffic details, and the tunnel state. You can view the status (connect or disconnect) of the gateway's VPN connections as a whole (by selecting Overview for the Display VPN type) or view each VPN separately.

Network Settings

Verifying and Changing the Default WAN Configuration

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Network** tab at the top.
3. Under **WAN Mode Configuration**, verify the WAN mode and the primary WAN port (or Default WAN Configuration) settings. Note that the settings or configurations here depend on the device model and firmware.

To change the Default WAN or WAN Mode Configuration:

1. Disable the option **Use Profile configuration** first at the top of the configuration page to allow changes.
2. Select IPv4 and IPv6 default WAN configuration. Or select a WAN mode from the available options. For **Primary WAN**, designate a WAN port as the primary WAN. For **Auto-rollover using WAN**, select both Primary and Secondary WAN ports as well as the **Health Check** method. For DNS servers and Ping IP address methods, enter the

respective server IP address as the destination to check the connectivity. Also enter the **Retry interval** (seconds) and **Failover after** (number of failed retries). For Load balancing, select the method (either Round robin or Spillover mode).

3. For **Round robin**, configure the Health check method (or none) and enter the **Retry interval** (seconds) and **Failover after** (number of failed retries). Hence, if a WAN interface disconnects, only the alternate WAN ports will transfer traffic flows in a round robin manner. For **Spillover**, enter the **Load tolerance** (%) and **Max bandwidth** (Mbps) as the threshold value. Once the threshold is exceeded, new traffic flows will be allocated to the alternate WAN interfaces. The precedence for selection is based on the configuration of Primary, Secondary, and Tertiary WAN interface.
4. Click **Apply**.

Note: The WAN mode can be configured using Profiles. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Using Dynamic DNS

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Network** tab at the top.
3. Under **Dynamic DNS**, enable or disable the service.
4. > Click **Apply**.

To add a DDNS service:

1. Disable the option Use Profile configuration first at the top of the configuration page.
2. Click **Add**. Enter the following information:

WAN Interface	Select the WAN interface for configuration
Service Provider	Select the DDNS service provider.
Username/Password	Enter the DDNS account name and password.
Hostname	Enter the registered hostname with the DDNS service.
Wildcard	Enable or disable the wildcard option which will resolve *.hostname to the same designated IP address.
Use Public IP	Enable or disable the use of a public IP address.
Force Update Interval	Enter the DDNS update interval (days).

3. Click **Save** to close the screen. Then click **Apply**.

Using IP Alias for the WAN

Note: The IP Alias function is only available on supported models.

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Network** tab at the top.

3. Under **IP Aliasing** , click **Add** to bind one or multiple IP addresses to a WAN interface.

   Enter the following information:

WAN Interface	Select the WAN interface for configuration
IP Address/Subnet Mask	Enter the IP address and subnet mask to bind to the WAN interface.

4. Click **Save** to close the screen. Then click **Apply**.

Viewing and Customizing the Gateway Port Status Overview

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Summary** tab at the top. The ports of the gateway device are displayed along with their detailed information shown in the table below:

Port Number	Numbering of the ports on the connector panel.
Interface Name	The name that identifies the port.
Port Status	Displays the link state of the port.
MAC Address	The MAC address of the port.
IP Address/ Subnet Mask	The IP address and subnet mask assigned to the port
Gateway	The gateway IP address if it has been assigned.
DHCP Mode	Displays if DHCP service has been enabled on the device.
Sent Bytes	The amount of data sent out of the port (bytes).
Received Bytes	The amount of data received through the port (bytes).

Total Bytes	The total amount of sent and received data volume (bytes).

To configure a port's basic settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Network** tab at the top.
3. Disable **Use Profile Configuration** to allow modification.
4. Under **Port Configuration** , select a port and click **EDIT** under Actions. Specify the following information for the selected LAN port:

Interface Type	Select the connection type: LAN, WAN, or DMZ.
Interface Name	Enter a name to identify this interface.
Bridge Network	Enable or disable bridging with another network. Configure the interface with more settings below if bridging is not enabled.
IP Address/ Subnet Mask	Enter an IP address with subnet mask.
DHCP Mode	Enable or disable DHCP service for IP address assignment.
DHCP Server	Enter the following information if DHCP server is selected. Domain name: Assign a domain name for DHCP service. Starting IP address/Ending IP address: Enter the range of IP addresses that can be assigned dynamically. Default gateway: Assign a default gateway for DHCP service. DNS server: Configure DNS by specifying a static DNS server, DNS setting from the ISP, or using DNS proxy. For static DNS, enter the DNS servers or WIN server IP address. Lease Time: Enter a time value of 1 to 10080 minutes.

Allow Ping from LAN	Enable or disable ping command executed from this port.
DHCP Relay	Enter the remote DHCP server address if DHCP relay is selected.
DNS Proxy	Enable or disable DNS proxy.

For a WAN port (if the device supports this feature), configure the following:

Interface Type	Select the connection type: LAN, WAN, or DMZ.
Connection Type	Select the connection method: DHCP, Static IP, PPPoE, PPTP, or L2TP. For Static IP, enter the IP address/Subnet mask, Gateway IP address and Primary/Secondary DNS servers, and specify whether to keep the original MAC address as well as the MTU size. For PPPoE, select the Address mode: Dynamic IP or Static IP. For static IP, enter the IP address/Subnet mask and PPPoE connection Username and Password. Then specify the Authentication type from one of the following: None, MS-CHAPv2, MS-CHAP, CHAP, PAP, or Auto-negotiate. For Dynamic IP, you don't need to enter the IP address/subnet information but configure all other settings as specified above. For both addressing modes, enter the Service name (optional) and select the Reconnect mode: Always on, or On demand (enter the Maximum idle time to wait before terminating the connection in minutes for this option). Then configure the DNS servers and specify whether to keep the original MAC address as well as the MTU size. For PPTP, if Static IP is selected, enter the following IP address information: IP address/Subnet mask, Gateway IP address, and Static DNS IP address. For both Address modes, enter the PPTP server name and connection Username and Password. For both modes, configure whether MPPE (Microsoft Point-to-Point Encryption (MPPE) will be used and the Reconnect mode: Always on or On demand (enter the Maximum idle time to wait before terminating the connection in minutes for this option). Then configure the DNS servers and specify whether to keep the original MAC address as well as the MTU size. For L2TP, if Static IP is selected, enter the following IP

	address information: IP address/Subnet mask, Gateway IP address, and Static DNS IP address. For both Address modes, enter the L2TP server name and connection Username and Password. For both modes, enter the Secret (optional) and configure the Reconnect mode: Always on or On demand (enter the Maximum idle time to wait before terminating the connection in minutes for this option). Then configure the DNS servers and specify whether to keep the original MAC address as well as the MTU size.
Advanced Settings	Enable or disable the following passthroughs: **Internet Protocol Security (IPsec)** which is used for securing packets exchange at the IP layer. **Point-to-Point Tunneling Protocol (PPTP)** which is used for tunneling the Point-to-Point Protocol (PPP) communication in an IP network. **Layer 2 Tunneling Protocol (L2TP)** which is used for implementing Point-to-Point sessions utilizing multipoint tunneling technique.

5. Click **Save**. Then click **Apply** to apply the settings to the affected device immediately.

Viewing and Configuring VLANs

VLANs allow you to divide the network to different segments. To obtain the current VLAN settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Addressing.** The VLANs are displayed under the VLAN section with the following information:

Name	A name that helps identify this VLAN.
VLAN ID	The assigned VLAN ID.
Untagged/Tagged Ports	The member ports for the untagged VLAN and tagged VLAN .

IP address/Subnet Mask	The IP address/Subnet mask configured for the VLAN.
Captive Portal	The associated Captive Portal page.

To configure a VLAN:

1. Disable the **Use Profile configuration** option.
2. Under **VLAN**, click **Add** to add a new VLAN.
3. Click Apply at the top left to apply the changes to the affected device immediately.

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring IP Management List

The IP Management list displays the IP assignment of the DHCP clients:

Host Name	The host name of the client device.
Interface	The associated interface with the IP assignment.
IP Address	The assigned IP address of the host.
MAC Address	The MAC address of the host.
IPv6 Suffix	The assigned IPv6 suffix, which is the the last 64 bits of an IPv6 address.
IP-MAC Binding	Indicates whether the IP assignment is enforced on the client device with the specified MAC address to prevent the use of other static IP address on this client.
DHCP IP Reservation	Indicates whether this IP assignment is reserved for this client so that it can get the same IP assignment every time it sends a DHCP IP request.

To configure IP management for DHCP clients:

1. Disable the **Use Profile configuration** option.
2. Under **IP Management List**, click **Add** to add a new IP assignment.

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring Routing

Routing determines the path for packet delivery in a network. The routing capabilities vary depending on the device model.

To view the configured routing policies:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Routing**. The configured routing protocols are displayed:

IPv4/IPv6 Static Route

Name	A name that helps identify this route.
Destination	The destination subnetwork IP address.
Subnet Mask	The subnet mask of the destination address. This is only available for IPv4 configuration.
Gateway	The IP address of the gateway or next hop.
Interface	The associated interface for this route.
Metric	The number of hub count.
Active	Enable or disable this route configuration.

IPv4/IPv6 Policy Route

Name	The name that helps identify the route.

Local Gateway	The port of the device that the route would use.
Protocol	The protocols associated with this route.
Source Network	A single IP address or a range of IP addresses that this route will be applied to. “Any” means all source IP addresses.
Destination Network	A single IP address or a range of IP addresses that this route will be applied to. “Any” means all destination IP addresses.
Source Port	The port number used for this type of traffic. ”Any” means all source ports will be used for this service.
Destination Port	The port number used for this type of traffic. ”Any” means all destination ports will be used for this service.
Active	Enable or disable this route configuration.

RIP Configuration

Interface	The interface by which Routing Information Protocol (RIP) information exchange will be performed.
Direction	Indicates inbound, outbound, or traffic for both directions.
Version	The version of the RIP
Authentication	Indicates whether the authentication is enabled.
Active	Enable or disable this route configuration

OSPFV2 Configuration

Interface	The interface assigned to the area defined below.
NSSA	Enable or disable the not-so-stubby area (NSSA) which can import external route information.
Area	The assigned area ID.
Priority	The OSPF priority which is used for determining the OSPF designated router.
Hello Interval	The time interval (seconds) between each hello packet.
Dead Interval	The time (seconds) the device must wait before it declares a neighbor OSPF router down when a hello packet has not been received.
Cost	The cost of the OSPF path.
Authentication	Indicates the authentication method used
LAN Route Exchange	Enable or disable the exchange of LAN routing table.
Active	Enable or disable this OSPF route configuration.

To configure routing policy:

1. Disable the **Use Profile configuration**option.
2. Under each routing protocol supported by the device model, click Add to add a new routing policy.

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring Services

Supported services can be configured individually depending on the features of the gateway.

To view and configure the supported services and network functions:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Network > Services**.

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Managing Traffic

The Traffic Management provides control over certain types of traffic by setting limits on bandwidth and sessions. Note that the availability of this function depends on the capability of the gateway.
To view Traffic Shaping rules configured:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Traffic Management**.

   Under Traffic Shaping, the following is displayed:

Name	The policy name.
Policy Type	Whether the traffic policy is applied to inbound or outbound traffic.
WAN Interface	The WAN port that this policy should be applied to.
Management Type	The metric to define the policy: Rate or Priority. Configure the following if Priority is selected: Low, Medium, or High. Higher priority means the traffic will be allocated with more bandwidth. If Rate is selected, enter the maximum bandwidth and minimum bandwidth (kbps).
Priority/Bandwidth Rate	The priority or the bandwidth configured for the respective management type.

Service	The type of traffic according to the protocol or application service configured.
Traffic Selector Match Type	The criteria for the traffic to which the policy should be applied: IP address, MAC address, or Interface.
Schedule Policy	The schedule policy that makes the policy effective during the designated time frame. Go to **Configure > Schedule policies** for scheduling information and configuration.

Viewing and Managing Session Limiting

To view Session Limiting rules configured:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Traffic Management**.

   Under Session Limiting, the following is displayed:

Name	The policy name.
Source Type	The source address can be configured as a single IP address, an IP address range, or an interface.
Maximum Sessions	The maximum number of sessions allowed (1-999).
Schedule Policy	The schedule policy that makes the policy effective during the designated time frame. Go to **Configure > Schedule policies** for scheduling information and configuration.

Viewing and Managing Custom Warning Pages

To view Custom Warning Page configured:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Traffic Management**.

   Under Custom Warning Page, the following is displayed:

Name	The policy name.
Source Type	The configured warning page to be displayed to users when the maximum limit of sessions has been reached . Go to **Configure > Splash pages** to view all the configured splash pages.
Active	Whether this rule is active or inactive.

To configure Traffic Management:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Traffic Management**.
3. Disable the option **Use Profile configuration.**

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring Captive Portal

The captive portal displays a splash page to wireless users who are required to agree to terms and conditions to use Internet services.
To view Captive Portal configured:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Captive Portal.**

The following information is displayed:

Name	The profile name.
Captive Portal	The authentication method for the users.
Splash Page	The pre-configured splash page which a wireless user must visit prior to using Internet services. The design of the page depends on the use case.
Basic Login	For basic login page, the associated authentication method: a local authentication database or an authentication server system.

3rd party Credentials	The configured third-party credential to be used for login.
SSID/VLANs	A pre-configured SSID/VLAN assigned to this captive portal setting.

To configure Captive Portal:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > Captive Portal.**
3. Disable the option **Use Profile configuration.**

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring High Availability

Virtual Router Redundancy Protocol (VRRP) can be utilized to implement fault tolerance and load balancing on a network by designating primary and backup roles among the virtual routers. The primary router is responsible for processing packets sent to a virtual IP address and the backup router takes up the primary role when the primary becomes unavailable. This availability of this feature depends on device model.

To view VRRP settings configured:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > High Availability.** The following is displayed:

VRRP ID	The unique identifier for the VRRP group.
Interface	The interface to which the VRRP configuration would be applied.
IP Address	The virtual IP address.
Node Type	The designated role of the virtual router: Master or Backup.
Priority	The Priority determines the order of selection for a primary virtual router among the backup virtual routers (1-255). Higher number means high priority.

To configure VRRP settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Network > High Availability.**

3. Disable the option **Use Profile configuration.**

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring Wireless

You can create multiple SSIDs for your wireless network and configure each SSID with unique settings to accommodate different wireless usage scenarios. You can also configure radio settings such as operating mode and channels for different frequencies supported for the device model. Note that this feature is only available for supported models.

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Security Settings

Security features consist of firewall, intrusion prevention, and web content filtering as well as application control.

Note: Changing the Routing mode from Network Address Translation (NAT) to Router (go to Network > Addressing), the Security Firewall's option of Use Profile configuration will be disabled. Moreover, the rules configured for Port forwarding, Port triggering, and 1:1 NAT will be erased.

Firewall

To view a gateway's firewall settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Firewall.**

The following information is displayed:

IPV4/IPv6 FIREWALL RULES

IPv4/Ipv6 Firewall Rules allow or block certain types of traffic that need to be forwarded through the device.

Priority	The assigned priority number (1-998). Lower number means higher priority.
Name	The name of the rule.
Policy	Indicates whether it is a allow or deny rule.

Protocol	The associated protocol for the rule: Any, TCP, UDP, TCP/UDP, or ICMP.
Source Interface	The interface that the traffic is sent from.
Source	A single IP address or a range of IP addresses as the source host. Any means traffic from all IP addresses.
Source Port	The source port number used for this type of traffic. Any means all ports.
Destination	A single IP address or a range of IP addresses as the destination host. Any means traffic destined to all IP addresses.
Destination Port	The destination port number used for this type of traffic. Any means all ports.
Schedule	The associated Schedule Policy.
Active	Indicates whether this rule is enabled or disabled.

Note: The availability of IPv6 Firewall Settings depends on the features of the device model.

Port Forwarding

Port Forwarding redirects traffic entering the WAN to another port on the LAN. This is useful when a certain service is hosted on an interval server on the LAN.

To view Port Forwarding rules:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Firewall.**

The following information is displayed:

Name	The name for the rule.
Mode	Indicates whether the rule is for traffic forwarding or port translation.

Interface	The WAN interface to which this rule should be applied.
Protocol	The associated protocol of this rule: TCP, UDP, or TCP/UDP.
Public Port	The external port associated with this type of traffic or service (1-65535). It can be a single port or a range of ports.
Local IP	The IP address of the local server.
Local Port	The local port used for this service if translation mode is selected.
Allowed Remote IPs	The IP addresses of the remote hosts that this rule will be applied to. Any means all remote hosts.
Active	Indicates whether this rule is enabled or disabled.

Port Triggering

Port Triggering dynamically opens public ports for inbound traffic after certain ports are triggered by a service request.

To view Port Triggering rules:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Firewall.**

The following information is displayed:

Name	The rule's name.
Protocol	The protocol to which the rule is applied: TCP, UDP, or TCP/UDP.
Outgoing Trigger Port	The outgoing port used for this service.
Incoming Trigger Port	The incoming port used for this service.
Active	Indicates whether this rule is enabled or disabled.

1:1 NAT

One-to-one NAT allows a static mapping between an internal IP address and an external IP address.

To configure 1:1 NAT rules:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Firewall.**

   The following information is displayed:

Name	The rule name.
Interface	The WAN interface that this rule should be applied to.
WAN IP	The WAN IP address as the external IP address for translation.
Local IP	The local IP address as the interval IP address for translation.
Protocol	Indicates the associated protocol of this rule: TCP, UDP, or TCP/UDP.
Port	The port used for this traffic type.
Allowed remote IPs	The IP addresses of the remote hosts that this rule will be applied to. Any means to allow all remote hosts.

To configure Firewall rules:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Firewall.**
3. Disable the option **Use Profile configuration.**

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring IPS Settings

To view Intrusion detection and prevention settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security >IPS.**
3. Disable the option **Use Profile configuration.**

If the device is equipped of intrusion detection functions, you can enable or disable the following services:

Intrusion Detection	Enable intrusion detection. And select the WAN and LAN interfaces that the IPS and IDS should be implemented.
Intrusion Prevention	Enable intrusion prevention. And select the WAN and LAN interfaces that the IPS and IDS should be implemented.
Stealth Mode	This mode protects your device from Internet intrusion by not responding to unauthorized requests.
Block TCP Flood	Enable to block TCP flooding to WAN.
Bock UDP Flood	Enable to block UDP flooding to LAN.
Filter Check Mode	Enable the TCP filtering check mode.
Allow ICMP Traffic	Enable to allow packets of Internet Control Message Protocol to pass through.
DoS Attacks	Denial-of-Service (DoS) attacks encompass SYN Flood, ICMP Flood, and Echo storm. Configure the flood rate of each attack in packets/second for detection.

4. Click **Apply** at the top left to apply the settings to the affected devices immediately.

Viewing and Configuring Web Content Filter

The Web Content Filter is used to prevent access to unwanted websites. It allows you to create profiles that can take effective during the designated time frame and block websites belonging to a certain category.

Web Content Filter List

To view the Web Content Filter List:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security >Web Content Filter.**

Under Web Content Filter List, the following is displayed:

Name	The name for the filtering rule.

Policy	State whether this is a allow or block policy.
Schedule	The pre-configured scheduling.
Scope	The specified hosts or the whole network that this rule will be applied to.
Filtering Type	The type consists of a variety of categories, URLs, and custom groups to restrict the access to defined websites.
Active	State whether the rule is active.

Under Custom Warning Page, you can obtain the configured warning page that will display related messages when a restricted webpage is being visited. The following is displayed:

Name	Enter a name for this configuration.
Source Type	The pre-defined warning page to be displayed.
Actions	State whether the rule is active.

Under **Custom Group List,** you can obtain the Custom group which will be used to define the content filtering type above:

Group Name	The name for the custom group.
URLs	If URL filtering is used, it shows the name and keyword for the website. This blocks access to websites based on a website's domain name (e.g. google.com) and keywords with matching URLs. For example, keyword "ABC" will block "www.ABC.com" and "xxx.ABC.com" and other URLs containing ABC.
Category Filtering	If Category filtering is used, it shows the pre-defined categories to block access to.
In Use	State whether this rule has been activated.

To configure Firewall rules:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Web Content Filter.**
3. Disable the option **Use Profile configuration.**

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

Viewing and Configuring Application Control

The Application Control is used to restrict certain communication of applications. It allows you to create profiles that can take effective during the designated time frame and prevent traffic of certain applications from being transferred.

Auto Upgrade

Enable automatic upgrade of application signature database and select the update schedule by entering the upgrade frequency in minutes or setting a specified time of a designated weekday for weekly updates.

To add an application control rule:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Application Control.**
3. Under Application Control List, the following information is displayed:

Name	The policy name.
Policy	State whether this is a allow or block policy.
Schedule	The pre-configured schedule. For configured scheduling methods, go to **Configure > Schedule policies**.
Scope	The specified hosts or the whole network that this rule will be applied to.
Application	State whether the filtering rule is based on a single application, or a single application from a pre-defined category, or a custom group of selected applications.
Active	State whether the application control policy is active or inactive.

Under **Custom Group List,** you can obtain Custom Group defined which will be used to define the application type above:

Group Name	The name of the custom group.
Application List	The selected applications for the custom group.
In Use	State whether this rule has been activated.

To configure Application Control:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **Security > Application Control.**
3. Disable the option **Use Profile configuration.**

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section.

VPN Settings

A Virtual Private Network (VPN) builds an encrypted connection between endpoints over a public network utilizing tunneling techniques. VPN can be configured only if your device supports this feature.

Site to Site VPN

The site-to-site VPN is a technique that allows connectivity between the offices located at multiple locations by setting up an IPsec tunnel over the Internet to access the intranet. In short, a site-to-site VPN builds a secure path over an insecure path. The Nuclias cloud gateway allows users to establish a VPN tunnel without manually entering the tunnel endpoint details and the local/remote networks. Instead, the Nuclias cloud gateway maintains these details and lets users select the networks.

Configuring Quick VPN

Quick VPN is a Nuclias auto-provisioning site-to-site VPN technology that allows you to quickly and easily build VPN tunnels between Nuclias gateway devices without tedious manual VPN configuration. If it is disabled, set up VPN manually at Manual VPN Settings to establish VPN connection with other partners.

To view or configure Quick VPN settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **VPN > Site-to-site VPN**.s
3. Select the topology: Hub-and-Spoke or Full Mesh. If Full Mesh is selected, the VPN establishes the Gateway-to-Gateway IPsec tunnel with other devices registered in the same or different sites of the same organization. To establish a tunnel with a particular remote device, enable the Join member field in the Remote VPN participants table. Once

the tunnel configuration is pushed to the remote peers, traffic gets initiated by the user, and a tunnel is established between the remote peers.

4. If Hub-and-Spoke is selected, specify the role to be either a hub or spoke. If Spoke is selected, you can choose hubs to build VPN tunnels in the Exist hubs table. In addition, it lists the Exist hub devices available with the option of Primary Hub. If you enable the Primary Hub field, the selected hub will be the primary hub for the spoke and can communicate to all the spoke devices linked to this hub. At a time, you can enable only one primary hub. If Hub is selected, then VPN tunnels will be built among hubs and dependent spokes.
5. If Hub mode is selected, enable or disable VPN connection with a remote peer. You may also choose to designate a remote peer as a backup hub.
6. If Spoke mode is selected, you can choose to designate a remote peer as the primary hub.
7. Click **Apply**.

Quick VPN Settings

In the Local networks section, if you have multiple subnets, you can specify which one subnet participates in the VPN, i.e., traffic from the enabled subnet will be encrypted by the IPsec VPN. All local subnets must be unique within the VPN topology

Note: A list of Quick VPN connections will be displayed in the **Summary > VPN Status** page. Select Quick VPN (Full Mesh and Hub-and-Spoke) as the Display VPN type.

Configuring Manual VPN

To view or configure Manual VPN settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **VPN > Site-to-site VPN**. Enter the following:

Connection Name	Enter a name for this VPN connection (1-64 characters).
IKE Profile	Select the IKE profile which contains security settings that will be used for the VPN connection.
Local Network	The scope of the local network to which the VPN connection will apply.
Local Network	Enter a local IP address or subnetwork of the local network to participate in the VPN. If Single IP is selected, enter the IP address. If Subnet is selected, enter the IP address and subnet mask (or prefix for IPv6). Select Any for the entire local network.

Remote Network	Enter a remote IP address or subnetwork of the remote network to participate in the VPN. If Single IP is selected, enter the IP address. If Subnet is selected, enter the IP address and subnet mask (or prefix for IPv6). Select Any for the entire remote network.
Outgoing Interface	Select an interface to which the VPN connection will use.
Remote Gateway	Select FQDN or Static IP for configuring the remote gateway address. Then enter the IP address or FQDN address.
Keep-alive	Enable or disable keep-alive for VPN reconnection. If enabled, enter the source and destination IP address as well as the detection period in seconds (10-199) and retry after the number of failures (3-99).
Idle Timeout	Enter the maximum length of time that the VPN connection can stay active when three is no traffic.
Dead Peer Detection	Enable detection for dead peers. If enabled, enter the detection interval (10-999 seconds) and Retry after failure (3-99 times).
NetBIOS Broadcast	Enable or disable NetBIOS broadcast from one end to be forwarded to the other end of the VPN connection.
Outgoing Backup Interface	Select an interface to which the VPN connection will use as a backup if Dead Peer Detection is enabled.
Remote Backup Gateway	Select FQDN or Static IP for configuring the remote gateway address if Dead Peer Detection is enabled.
IKE Backup Profile	Select the IKE profile which contains security settings that will be used for the backup VPN connection if Dead Peer Detection is enabled.

To add an IKE profile,enter the following:

Profile Name	Enter a name for this IKE profile.

IKE Version	Select the IKE version: v1 or v2.
IKE phase-1 Settings	
Exchange Mode	Select the exchange mode: Aggressive or Main.
Local Identifier Type	Select the identification method: Local WAN IP, FQDN, or User-FQDN. And enter the identifier according to the selected method.
Remote Identifier Type	Select the identification method: Remote WAN IP, FQDN, or User-FQDN. And enter the identifier according to the selected method.
DH Group	Select a Diffie-Hellman (DH) Group for key exchange. These groups vary in prime key lengths.
Encryption Algorithm	Select encryption algorithm(s) for ESP packets encryption.
Authentication Algorithm	Select authentication algorithm(s). And enter the SA lifetime in seconds (300-604800).
Authentication Method	Select the authentication method. Then enter the preshared key or select a certificate depending on the method selected. Go to **Settings > Certificate Management** for Certificate list.
Extended Authentication	Enable this and select extended authentication method: Authentication server, IPsec host, or Local authentication. Depending on the method, select the corresponding RADIUS/ LDAP/POP3/Active Directory/NT Domain server or Local Authentication profile or enter the username and password for IPsec host. Refer to **Configure > Authentication > Local Authentication list** and **Authentication servers** for Authentication profiles and servers.
IKE phase-2 Settings	

Protocol Selection	Select either ESP or AH. If Encapsulating Security Payload (ESP) is selected, select the Encryption algorithm to encrypt or decrypt ESP packets.
Authentication Algorithm	Select the authentication algorithm for header packets validation.
SA Lifetime (sec.)	Enter the SA lifetime (300-604800 seconds) for the active duration of a VPN tunnel.
Perfect Forward Secrecy	Enable or disable the Perfect Forward Secrecy. If enabled, the VPN communication is better protected with renewed negotiation of key values in the exchange.
DH Group	If the above PFS is enabled, select the DH group for key establishment.

3. Click **Apply** at the top.

Note: A list of Quick VPN connections will be displayed in the **Summary > VPN Status** page. Select Quick VPN (Manual) as the Display VPN type.

Client to Site VPN

An IPsec policy can be defined between this router and another gateway to create network-to-network IPsec tunnels. To configure IPsec VPN Server settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **VPN > Client-to-site VPN**. Enter the following:

Connection Name	Enter a name for this configuration
IKE	Select a pre-configured IKE profile for this VPN configuration.
Local Network	Enter the IP address and subnet mask of the local network. Select Any to not restrict to a single subnet.
Tunnel Mode	Select either full or split tunnel for the mode. Select Full tunnel or Split tunnel. The Split mode will split DNS requests among DNS servers. It allows you to create two zones for the same domain, one to be used by the internal network, the other used

	by the external network .For Split tunnel, enter the Split Domain names.
DHCP Relay	Enable or disable DHCP relay. If enabled, enter the IP address of the relay gateway. If disabled, enter the following IP address information.
Starting IP Address/ Ending IP Address	Enter the range of the IP addresses for VPN connections.
Primary/Secondary DNS	Enter the primary and optional secondary DNS servers.
Primary WINS Server/ Secondary WINS Server	Enter the primary and optional secondary Windows Internet Naming Service (WINS) servers.
Outgoing Interface	Select the WAN interface to which the IPsec VPN should apply.
Split DNS	Enable or disable Split DNS if Split tunnel is selected. And enter the domain names if enabled (3-253 characters).
NetBIOS Broadcast	Enable or disable NetBIOS information to be forwarded to the other endpoint of the VPN tunnel. The information is used for name resolution in Windows networking.

To add an IKE profile, enter the following:

Profile Name	Enter a name for this IKE profile.
IKE Version	Select the IKE version: v1 or v2.
IKE phase-1 Settings	
Exchange Mode	Select the exchange mode: Aggressive or Main.

Local Identifier Type	Select the identification method: Local WAN IP, FQDN, or User-FQDN. And enter the identifier according to the selected method.
Remote Identifier Type	Select the identification method: Remote WAN IP, FQDN, or User-FQDN. And enter the identifier according to the selected method.
DH Group	Select a Diffie-Hellman (DH) Group for key exchange. These groups vary in prime key lengths.
Encryption Algorithm	Select encryption algorithm(s) for ESP packets encryption.
Authentication Algorithm	Select authentication algorithm(s). And enter the SA lifetime in seconds (300-604800).
Authentication Method	Select the authentication method. Then enter the preshared key or select a certificate depending on the method selected. Go to **Settings > Certificate Management** for Certificate list (refer to Certificate Management) .
Extended Authentication	Enable this and select extended authentication method: Authentication server, IPsec host, or Local authentication. Depending on the method, select the corresponding RADIUS/ LDAP/POP3/Active Directory/NT Domain server or Local Authentication profile or enter the username and password for IPsec host. Refer to **Configure > Authentication > Local Authentication list** and **Authentication servers** for Authentication profiles and servers.
IKE phase-2 Settings	
Protocol Selection	Select either ESP or AH. If Encapsulating Security Payload (ESP) is selected, select the Encryption algorithm to encrypt or decrypt ESP packets.
Authentication Algorithm	Select the authentication algorithm for header packets validation.

SA Lifetime (sec.)	Enter the SA lifetime (300-604800 seconds) for the active duration of a VPN tunnel.
Perfect Forward Secrecy	Enable or disable the Perfect Forward Secrecy. If enabled, the VPN communication is better protected with renewed negotiation of key values in the exchange.
DH Group	If the above PFS is enabled, select the DH group for key establishment.

3. Click **Apply** at the top.

PPTP/L2TP

A PPTP server is available on the router for LAN and WAN PPTP client users to access.

To configure PPTP/L2TP Server settings

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **VPN > PPTP/L2TP**. Enter the following:

Name	Enter a name for the configuration profile of the server (1-64 characters).
Server Type	Select either PPTP or L2TP.
Routing Mode	Select either NAT or Router.
Starting IP Address/ Ending IP Address	Enter the LAN IP address range to be assigned to the VPN clients.
Authentication Server	Select the authentication server. Depending on the method, select the corresponding RADIUS/LDAP/POP3/Active Directory/NT Domain server or Local Authentication profile. Go to **Configure > Authentication > Local Authentication list** and **Authentication Servers** for Local authentication profiles and authentication servers list.
Authentication Protocol	Select the authentication protocol(s): All, PAP, CHAP, MS-CHAP, and MS-CHAPv2.

Encryption	[PPTP only] Select the encryption method(s) for PPTP: For PPTP, select All, MPPE 40 bit, MPPE 128 bit, or Stateful MPPE. The Microsoft Point-to-Point (MPPE) encrypts data for PPTP VPN.
Idle Timeout	The length of time (seconds) to wait before terminating a VPN session (300-1800).
NetBIOS	[PPTP only] Enable or disable NetBIOS, which is used for name resolution in Windows networking, if there is a WINS server set up in your LAN. If enabled, enter the Windows Internet Naming Service (WINS) server IP address. This option is only available for PPTP.
Enable Secret Key	[L2TP only] Enable or disable the secret key (or preshared key) with 8-63 characters which will be required for client VPN settings.
L2TP over IPsec	[L2TP only] Enable or disable L2TP over Internet Protocol Security (IPsec), on which L2TP relies for secure packets exchange.
IKE Version: Configure Internet Key Exchange (IKE) if L2TP Over IPsec is enabled.	
IKE version	Select the IKE version for configuration.
IKE phase-1 settings	
Exchange Mode	Select the exchange mode: Aggressive or Main.
Local Identifier Type	Select the identification method: Local WAN IP or FQDN. And enter the identifier according to the selected method.
Remote Identifier Type	Select the identification method: Remote WAN IP or FQDN. And enter the identifier according to the selected method.
DH Group	Select a Diffie-Hellman (DH) Group for key exchange. These groups vary in prime key lengths.
Encryption Algorithm	Select encryption algorithm(s) for ESP packets encryption.

Authentication Algorithm	Select authentication algorithm(s). And enter the SA lifetime in seconds (300-604800).
Authentication Method	Select the authentication method. Then enter the preshared key or select a certificate depending on the method selected. Go to **Settings > Certificate Management** for Certificate list.
Extended Authentication	Enable this and select extended authentication method: Authentication server, IPsec host, or Local authentication. Depending on the method, select the corresponding RADIUS/ LDAP/POP3/Active Directory/NT Domain server or Local Authentication profile or enter the username and password for IPsec host. Refer to **Configure > Authentication > Local Authentication list** and **Authentication servers** for Local authentication profiles and authentication servers.
IKE phase-2 settings	
Protocol Selection	Select either ESP or AH. If Encapsulating Security Payload (ESP) is selected, select the Encryption algorithm to encrypt or decrypt ESP packets.
Authentication Algorithm	Select the authentication algorithm for header packets validation.
SA Lifetime (sec.)	Enter the SA lifetime (300-604800 seconds) for the active duration of a VPN tunnel.
Perfect Forward Secrecy	Enable or disable the Perfect Forward Secrecy. If enabled, the VPN communication is better protected with renewed negotiation of key values in the exchange.
DH Group	If the above PFS is enabled, select the DH group for key establishment.

PPTP VPN Client can be configured on this router to access a remote network.

To configure a VPN client,enter the following:

Name	Enter a name for the PPTP/L2TP configuration profile of the client (1-64 characters).
Client Type	Select either PPTP or L2TP.
VPN Server	Enter the IP address or FQDN of the VPN server
Tunnel Type	Select Full tunnel or Split tunnel. Split tunnel mode only sends traffic to the private LAN with pre-specified client routes and give the client access to specific private networks, thereby allowing access control over specific LAN services.
Remote Network/ Netmask	Enter the remote network and netmask if split tunnel is selected.
Username/Password	Enter the username and password required for connection.
Encryption	For L2TP server, enter the Secret key (8-63 characters) if encryption is enabled. This value must match the preshared key value entered on the VPN server.
MPPE	Enable the Microsoft Point-to-Point Encryption (MPPE), which encrypts data for VPN communication.
Idle Timeout	For PPTP, enter the length of time (seconds) to wait before terminating a session.
Reconnect Mode	For L2TP, select On demand or Always on. Enter the Maximum idle time in seconds (300-1800) to wait before dropping an idle connection.
L2TP over IPsec	Enable or disable L2TP over Internet Protocol Security (IPsec), on which L2TP relies for secure packets exchange.
IKE Version: Configure Internet Key Exchange (IKE) if L2TP Over IPsec is enabled.	
IKE version	Select the IKE version for configuration.
IKE phase-1 settings	

Exchange Mode	Select the exchange mode: Aggressive or Main.
Local Identifier Type	Select the identification method: Local WAN IP or FQDN. And enter the identifier according to the selected method.
Remote Identifier Type	Select the identification method: Remote WAN IP or FQDN. And enter the identifier according to the selected method.
DH Group	Select a Diffie-Hellman (DH) Group for key exchange. These groups vary in prime key lengths.
Encryption Algorithm	Select encryption algorithm(s) for ESP packets encryption.
Authentication Algorithm	Select authentication algorithm(s). And enter the SA lifetime in seconds (300-604800).
Authentication Method	Select the authentication method. Then enter the preshared key or select a certificate depending on the method selected. Go to **Settings > Certificate Management** for Certificate list.
Extended Authentication	Enable this and select extended authentication method. Enter the Username and Password if IPsec host is selected.
IKE phase-2 settings	
Protocol Selection	Select either ESP or AH. If Encapsulating Security Payload (ESP) is selected, select the Encryption algorithm to encrypt or decrypt ESP packets.
Authentication Algorithm	Select the authentication algorithm for header packets validation.
SA Lifetime (sec.)	Enter the SA lifetime (300-604800 seconds) for the active duration of a VPN tunnel.
Perfect Forward Secrecy	Enable or disable the Perfect Forward Secrecy. If enabled, the VPN communication is better protected with renewed negotiation of key values in the exchange.

DH Group	If the above PFS is enabled, select the DH group for key establishment.

3. Click **Save**.

Note: A list of PPTP/L2TP connections will be displayed in the **Summary > VPN Status** page.

OpenVPN

OpenVPN allows peers to authenticate each other using certificates, or username/password. When used in a multiclient-server configuration, it allows the server to release an authentication certificate for every client, using signature and Certificate authority. An OpenVPN can be established through this router.

To configure OpenVPN settings

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **VPN > OpenVPN**. Enter the following:

Mode	Select the mode for the OpenVPN: Server, Client, or Access server client.
Upload Access Server Client	[Access Server Client mode only] Upload a configuration file which contains server and client IP address information if Access server client mode is selected. In access server client mode, the user has to download the auto login profile from the OpenVPN Access Server and upload the same to connect.
CRL Certificate	[Access Server Client mode only] Openvpn provides CRL authentication using CRL certificate. You can upload the required certificates by enabling it it first.
VPN Network/Netmask	[Server mode only] Enter the network IP address/netmask of the VPN. This is only available for the Server mode.
Server IP/Failover Server IP	The IP address or FQDN of the VPN server and failover server. This is only available for the Client mode.
Duplicate CN	[Server mode only] Enable or disable the duplicate CN to allow or disallow the same certification for multiple clients. This is only available for the Server mode.

Port	Enter the port number for VPN communication. The default is 1194.
Tunnel Protocol	Select the protocol for tunneling: TCP or UDP.
Encryption Algorithm	Select the encryption method: AES-128, BF-CBC, AES-192, or AES-256.
Hash Algorithm	Select the hash algorithm: SHA1, SHA256, or SHA512.
Tunnel Type	[Server mode only] Select the tunnel type: Full or Split. If Split is selected, enable or disable the client-to-client communication. Full Tunnel mode sends all traffic from the client across the VPN tunnel to the router. Split Tunnel mode only sends traffic to the private LAN with specified client routes. This is only available for Server mode configuration.
User-based Authentication	Enable or disable user-based authentication. If this is enabled, select the user profiles for Local authentication if server mode is used (refer to Local Authentication). If client mode is used, enter the username and password for VPN connection. Also select a certificate for TLS key if TLS authentication is used (refer to Certificate Management).
Certificate Verification	Enable or disable the use of certificate for verification.
Certificate	Select an available certificate from the list. The content of the certificate will be loaded in the field below.
TLS Authentication Key	Enable or disable the TLS authentication. If enabled, select an TLS authentication key from the certificate list. To obtain the certificate list, go to **Settings > Certificate Management**.
DH Key	Select a DH key from the certificate list. This is only available for Server mode configuration. To obtain certificate list, go to **Settings > Certificate Management**
Server Policies	Enable or disable the server policy. Enter the server policy and add a new server policy to permit or block networks for VPN connections. These policies can be applied to a specific IP

	address or IP networks on the LAN and can be enforced on the specified scope according to the supported features of the router. The List of Available Policies can be filtered based on whether it applies to a user, group, or all users (global). To add a new server policy, enter the following: Policy name: Give a name for this policy. Policy: Select whether it is a Deny or Permit policy. Scope: Select whether it is a global policy or to be applied for certain users using Local authentication. Select the user profile if Local authentication is selected. Apply policy to: Select whether to apply this policy to a single IP address or a subnet work and enter the required IP address and/or the Subnet mask and the port number. ICMP: enable or disable Internet Control Message Protocol (ICMP) traffic in VPN connections.
Remote Networks	If this is enabled, click Add to add a remote network configuration: enter a name for the configuration and the remote network IP address and subnet mask.
Port	Enter the port number (1-65535). This can be a single port or a range of ports, e.g. 3000-3200.
ICMP	Enable or disable the use of ICMP in the VPN communication.

OpenVPN provides authentication using certificates. This system will allow you to configure client list using **Local Authentication list (refer to Local Authentication)** and centrally manage the client certificates (refer to Certificate Management).To configure Client list for Server mode configuration:

1. Under Client list, click **Import**. The **Import users from local authentication list** page displays.
2. Select a pre-configured local user profile or click **Add local authentication** and configure a local user profile by specifying the following: the Local Authentication profile name, the Access level, Managed Sites, and the username and password for each new user. You can use the Bulk import function to upload a CSV file containing the user information to add multiple users at once. Refer to **Configure > Authentication > Local Authentication list** for more information.

3. Click **Save.** Once a Local authentication profile is imported successfully, you can manage the clients' certificates in the Certificate Management page (go to **Settings > Certificate management**) .

To configure OmniSSL Portal Layout for Server mode configuration:

OmniSSL facilitates the client installation from the device via the instructions on the portal page and is an enhancement to the existing OpenVPN. The enhancements allow the VPN tool to be used via mobile devices and eliminate browser and Java dependencies.

1. Under OmniSSL Portal Layout, click **Add**. The **Add portal layout configuration** page displays.
2. Enter a name for the profile and select a pre-defined login page for OmniSSL. Refer to **Configure > Splash pages** for more information. The Splash pages allow you to create a custom page that is presented upon authentication to the remote OmniSSL users.
3. Click **Save.**

Note: A list of OpenVPN connections will be displayed in the **Summary > VPN Status** page.

GRE Tunnel

GRE tunnels allow for broadcast traffic on the LAN of the router to be passed over the internet and received by remote LAN hosts.

To view or configure GRE Tunnel settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select **VPN > GRE Tunnel**. Enter the following:

Name	The name for the GRE Tunnel configuration.
Interface	Select the WAN interface to create this tunnel with from the drop-down menu.
GRE Tunnel IP/ Subnet Mask	Enter the IP address/subnet mask of this endpoint. It will be referenced in the other router's static route as the Gateway IP address.
Remote IP	Enter the WAN IP address of the endpoint router.
Static Route Configuration	IP address/Subnet mask: Enter the destination IP address/subnet mask of the static route from the remote LAN subnet. Gateway IP address: Enter the GRE tunnel IP of the terminating router that manages the remote LAN.

3. Click **Save.**

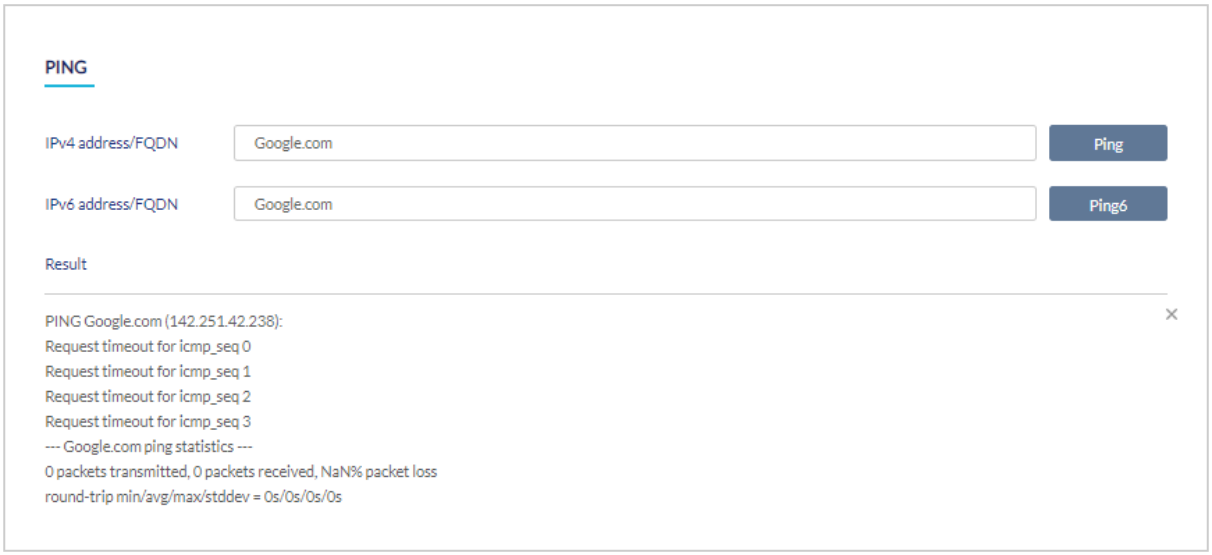
4. Click **Apply** at the top left to apply the settings to the affected device immediately.

Note: The GRE connection status will be displayed in the **Summary > VPN Status** page.

Tools

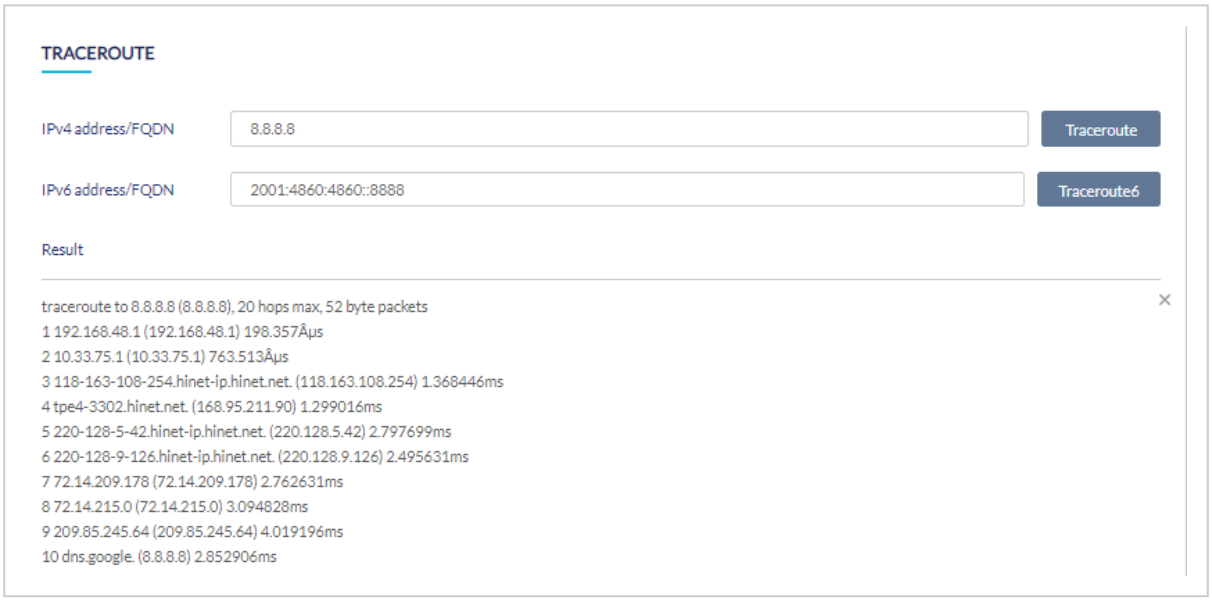
Performing a Device Ping Test

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Tools** tab in the top-right of the screen.
3. In the IPv4 or IPv6 address/FQDN field in the Ping section, enter a valid IP address or FQDN.
4. Click **Ping** for IPv4 addresses or **Ping6** for IPv6 addresses of the remote hosts. The results will be displayed as shown below:



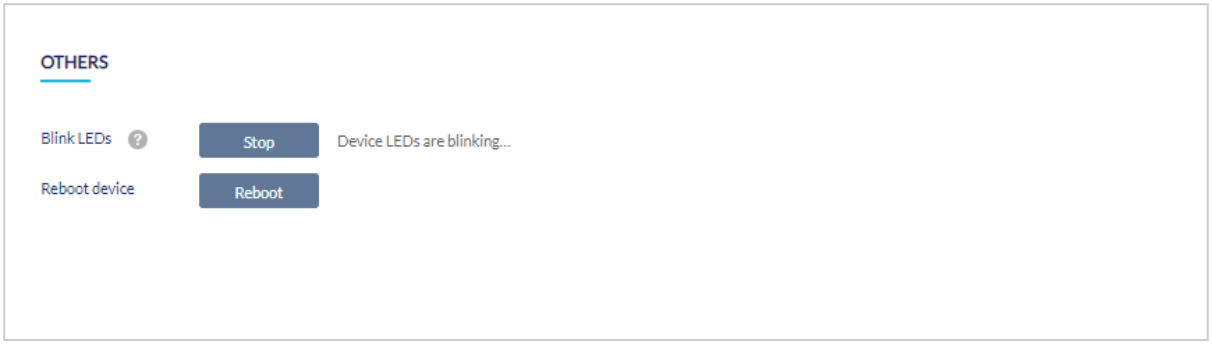
Performing a Traceroute Test

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Tools** tab in the top-right of the screen.
3. Under Traceroute, enter a valid IP address or FQDN in the IP address/FQDN field.
4. Click **Traceroute** for IPv4 addresses or **Traceroute6** for IPv6 addresses of the remote hosts. The results will be displayed as shown below:



Performing LED Blinking and Device Reboot

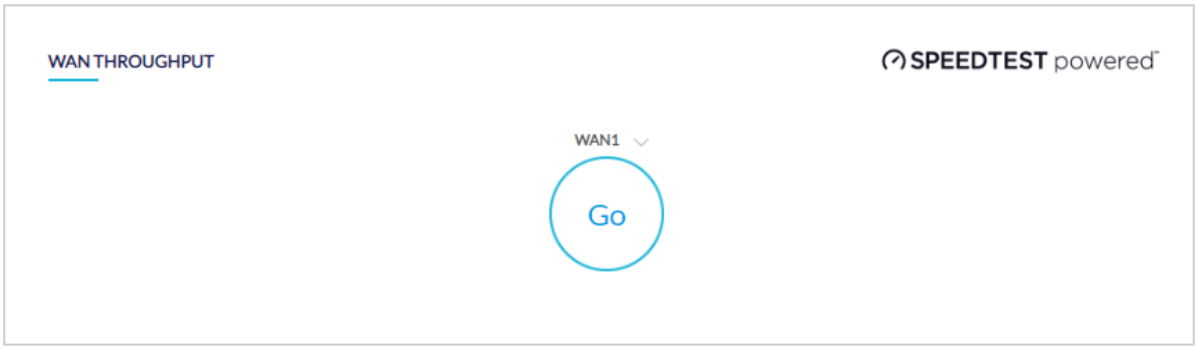
1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Tools** tab in the top-right of the screen.
3. In the Others section, click **Reboot** to reboot the device. Or click **Start** to start blink LEDs on the device. Click **Stop** to top blinking LEDs.



Note: Please refer to the respective device's manual for the status of LED indicators.

Performing WAN Throughput Test

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Tools** tab at the top right of the screen.
3. In the WAN Throughput section, click **Go**. The upload and download speed will be displayed.



Exporting or Importing Device Settings

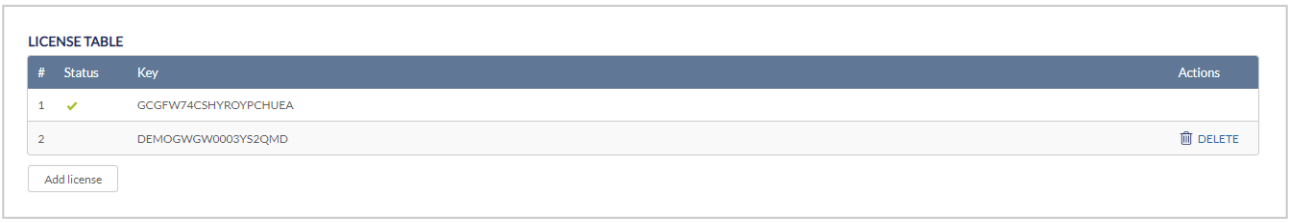
The device setting metadata can be exported as a single CSV file and it can be later imported for configuration restoration. To export device settings:

1. Navigate to **Monitor > Gateway > Devices** and select a device from the list.
2. Select the **Tools** tab at the top right of the screen.
3. In the Export and Import Device Settings section, click **Download**. The exported file will be downloaded to your browser's default download folder.

License

Adding a License Key to a Device

1. Navigate to **Monitor > Gateway > Devices** 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 > Gateway > Devices** 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 reclassify it as Unused in the license

management inventory.

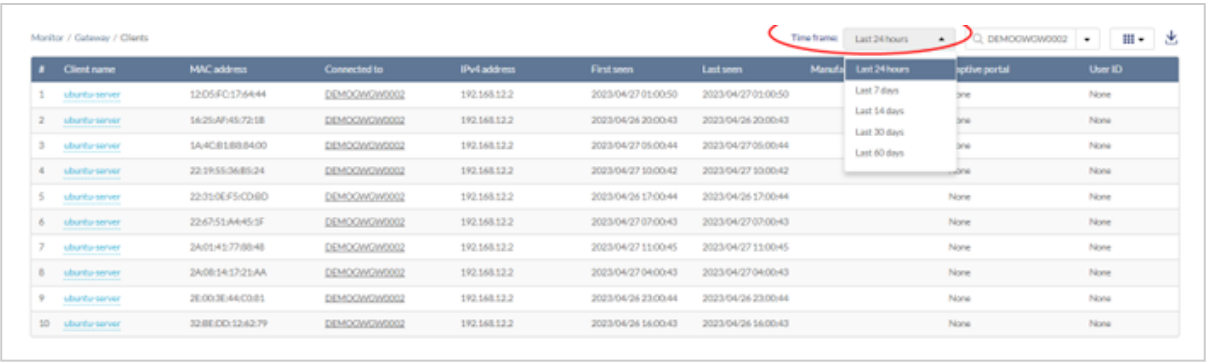


Clients

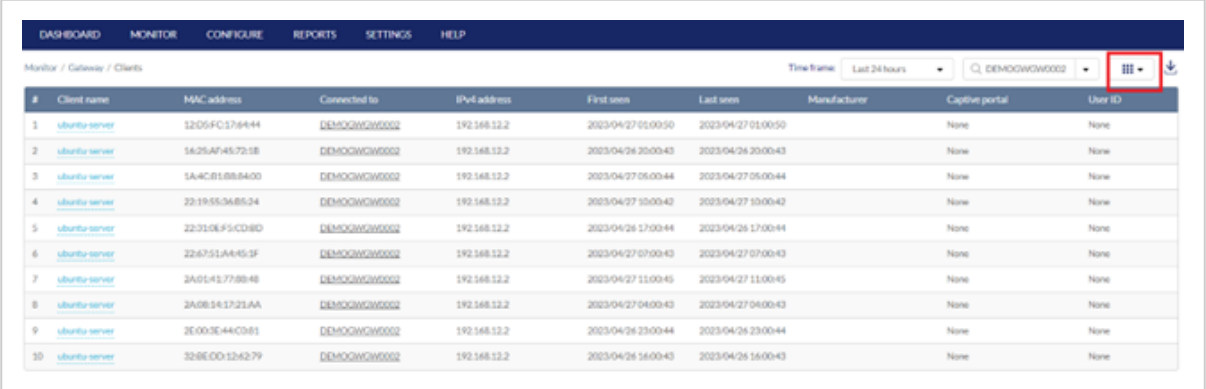
From the Clients window, you can consult a detailed overview of all currently connected devices with additional information including status, VLAN, and general settings.

Customizing the Client Monitor Overview

1. Navigate to **Monitor > Gateway > Clients**. The client list for all gateways will appear.
2. Select a time frame from the drop-down menu to define the time frame that the device was detected online.



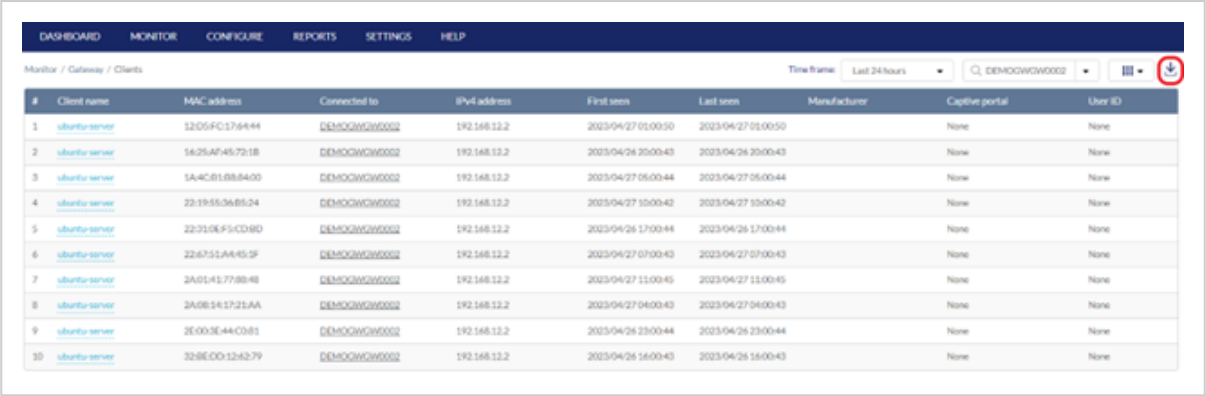
3. Click the parameter filter icon.



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

Downloading Client Monitoring Logs

1. Navigate to **Monitor > Gateway > Clients**.
2. From the client monitoring logs, click the download icon in the top-right.



Event Log

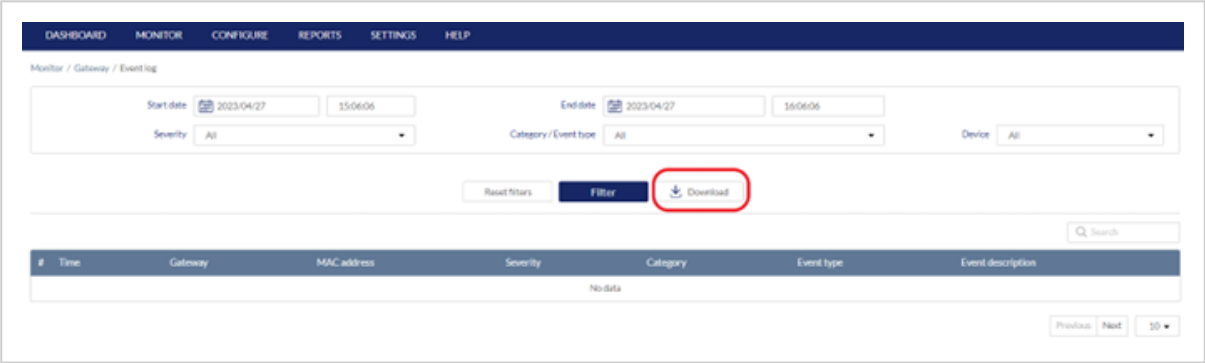
From the Event Logs window, you can consult a detailed log of events occurring on the network. You can also define event filter parameters, including event type and time period.

Filtering Event Log Parameters

1. Navigate to **Monitor > Gateway > Event Log**.
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 Category/Event type drop-down menu and select the event types to display. Select All to show all event types.
6. Click the Device drop-down menu and select a device to filter the results. Select All to show all event logs for all devices.
7. Click **Filter** to display all events matching the defined parameters. Click **Reset filters** to reset all currently set parameters.

Downloading Event Logs

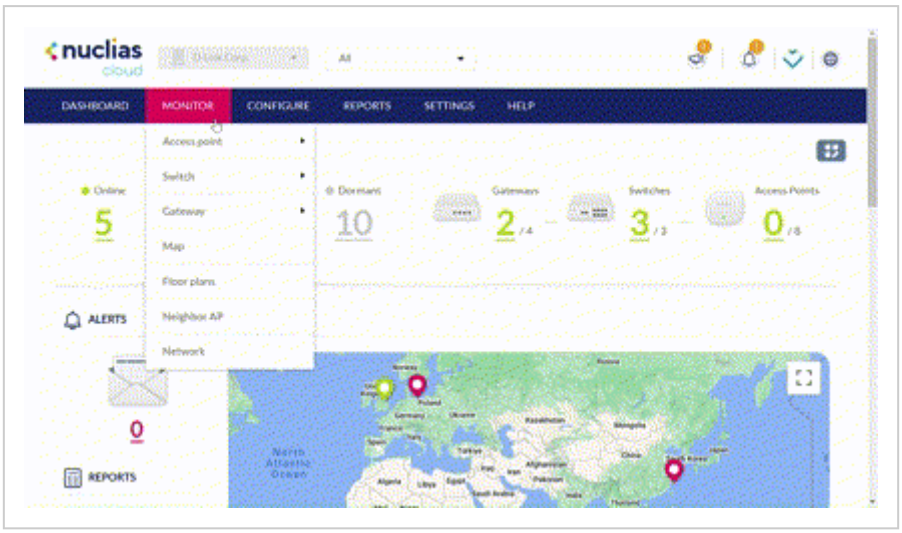
1. Navigate to **Monitor > Gateway > Event Log**.
2. From the event log list, click **Download**.


DASHBOARD
MONITOR
CONFIGURE
REPORTS
SETTINGS
HELP
Monitor / Gateway / Event log
Start date
2023/04/27
15:06:06
End date
2023/04/27
16:06:06
Severity
All
Category / Event type
All
Device
All
Reset filters
Filter
Download
Search
Time
Gateway
MAC address
Severity
Category
Event type
Event description
No data
Previous
Next
10

Map

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

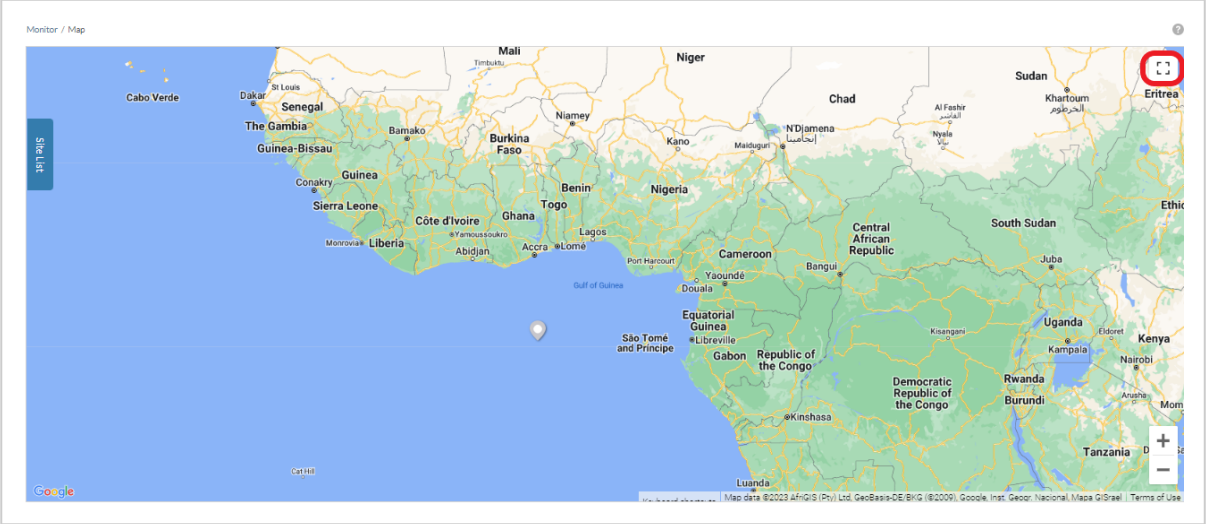
Note: Sites must be linked to a valid address in order to show up on the map.



Navigating the Map

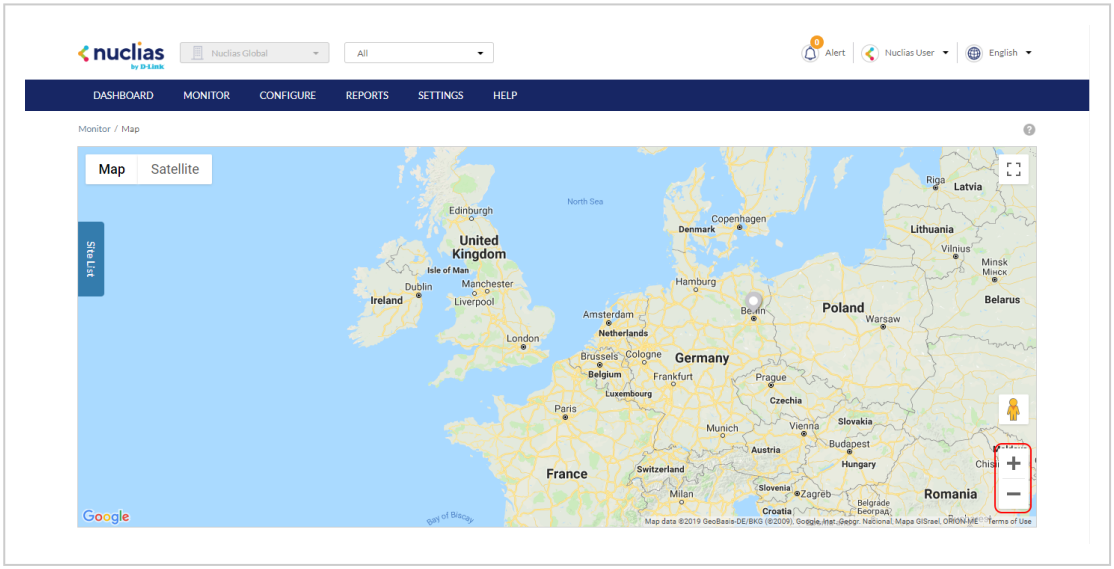
From the interactive map, you can view a geographical representation of the Site's physical location as well as view basic information and the current status of the Site and its devices.

1. Navigate to **Monitor > Map**.
2. 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.

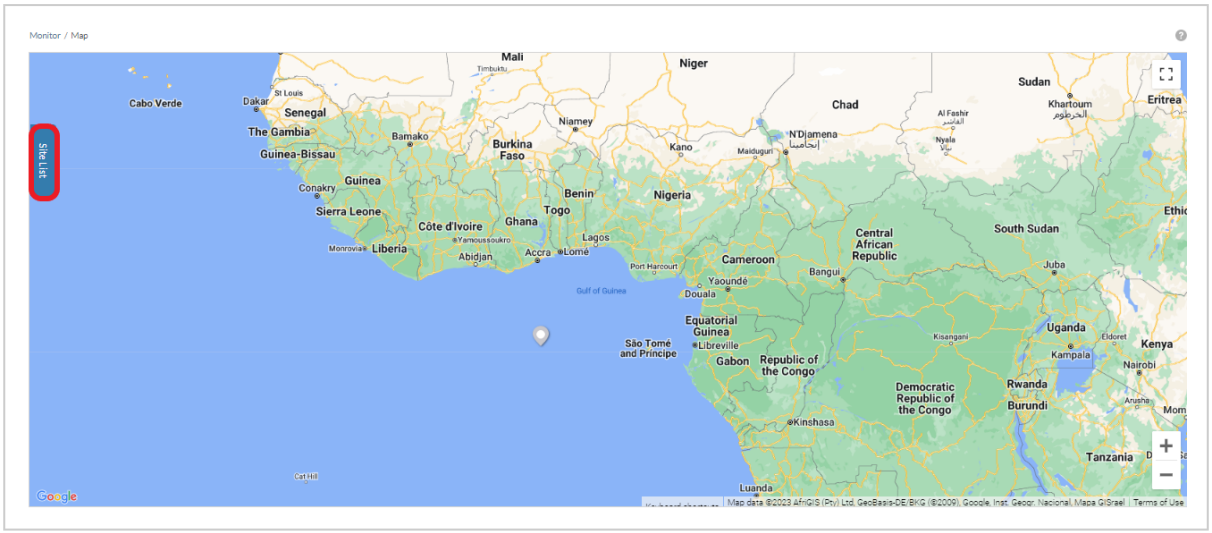
3. Click and drag the left-mouse button to move around on the map.
4. Click the + and – buttons in the bottom-right corner of the map to zoom in and out on the map. Alternatively, hold Ctrl and scroll the mouse wheel up and down to zoom in and out.



Navigating Sites on the Map Using the Site List

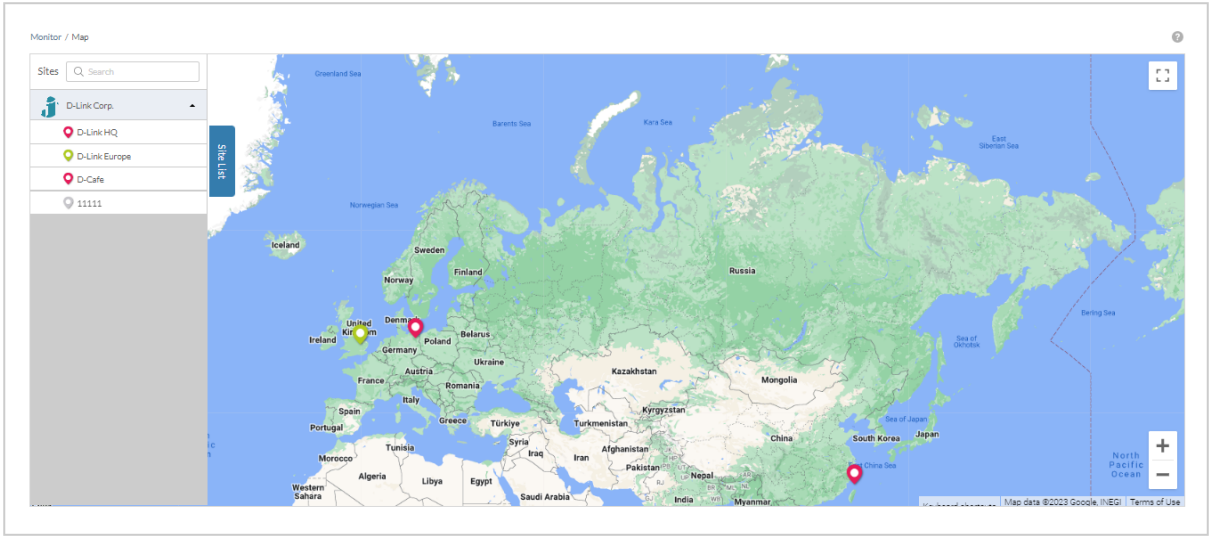
From the Site List, you can view all the Sites created under your organization that you have been authorized to access.

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.

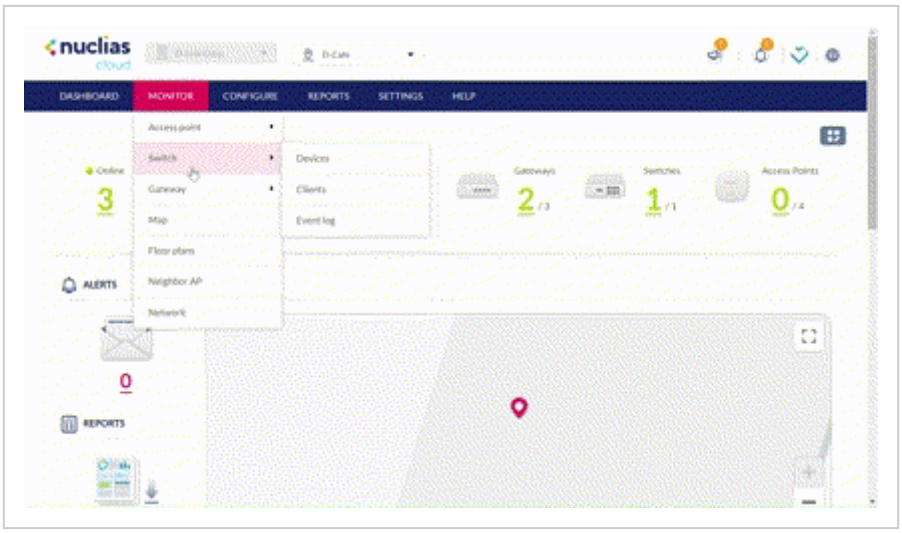
5. From the expanded Site list, click the Site name. The map will automatically navigate to the Site's location on the map.



6. Hover the cursor over the Site icon to view basic information and general device status.
7. [Optional] Click the Site name in the Site window to open the Dashboard view for that Site.
8. [Optional] Click the Floor Plan name in the Site window to be directed to the floor plan setting for the Site (you can also go to **Monitor > Floor Plans** to obtain the list of configured floor plans).

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.



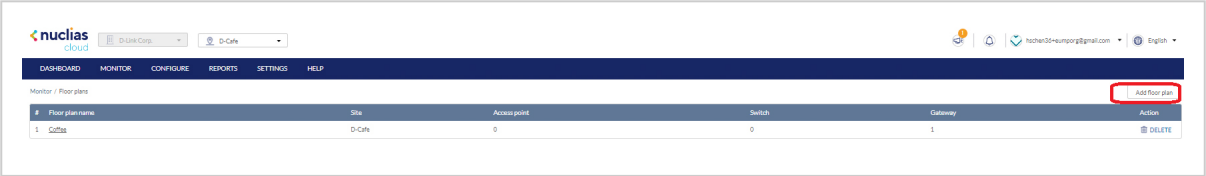
Adding a Floor Plan

You 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 Plans**.
2. Select a Site from the Site menu.



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

You can add 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.

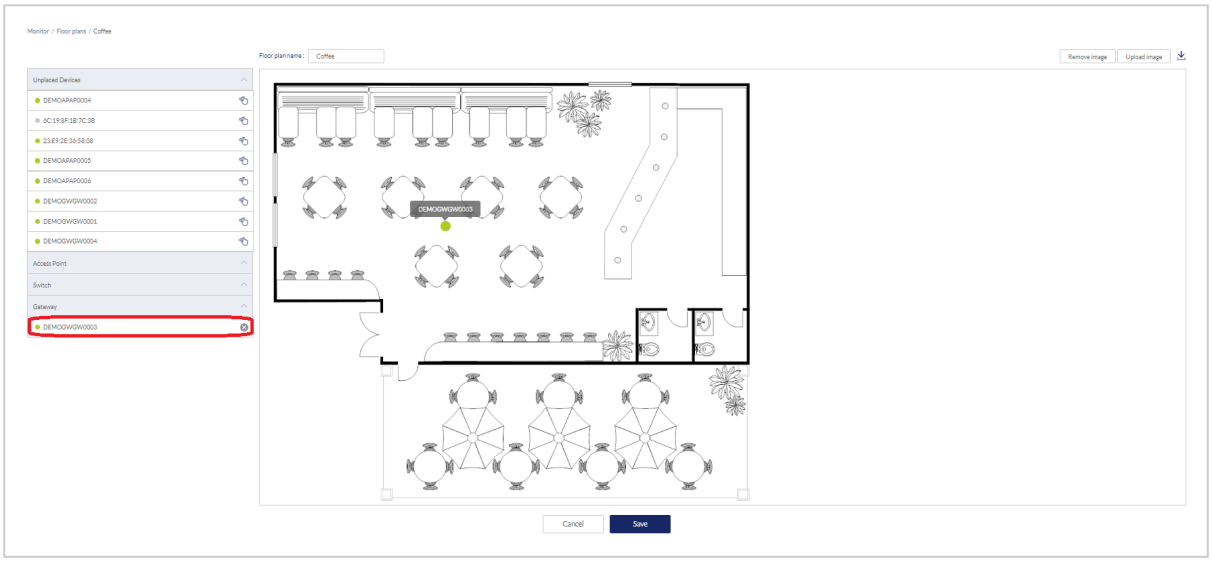
Adding Devices to a Floor Plan

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

Removing Devices from a Floor Plan

1. Navigate to **Monitor > Floor Plan**.
2. Select a Site from the Site menu.
3. From the floor plan list, click on the floor plan name.
4. Click the **X** icon next to the device in the device category list that you wish to remove.
   Note: Devices removed from the floor plan will automatically be moved to the Unplaced Devices list.



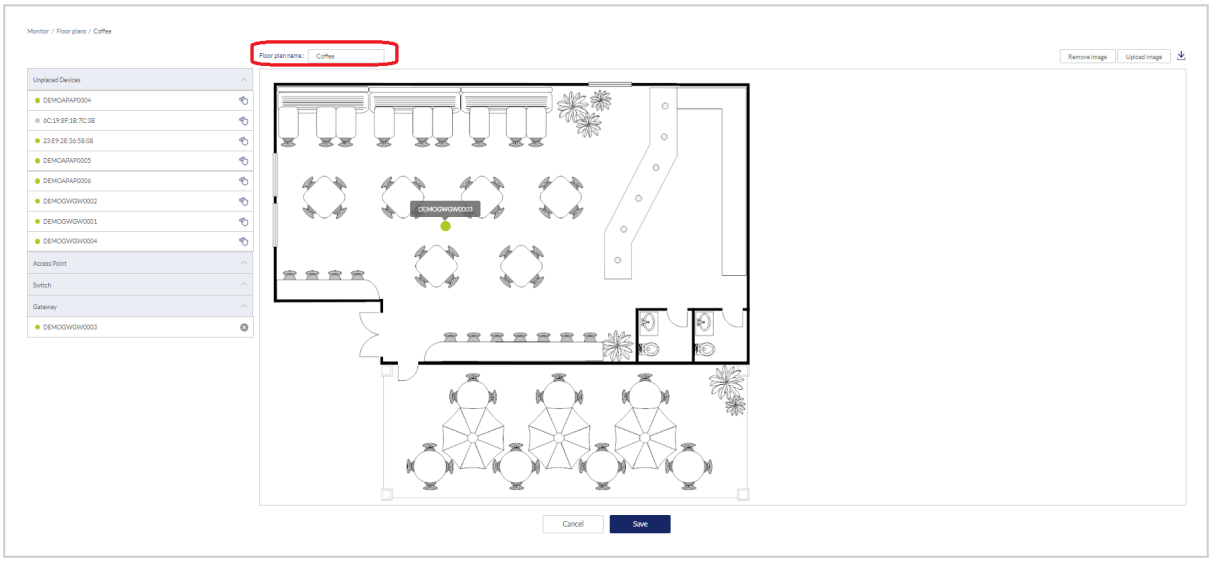
5. Click **Save**.

Editing a Floor Plan Name

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.
4. Click the floor plan name in the Floor Plan Name field.



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

Adding a Custom Floor Plan Image

1. Navigate to **Monitor > Floor Plans**.
2. Select a Site from the Site menu.
3. From the floor plan list, click on the floor plan name.
4. On the floor plan page, click **Upload image**.
5. In the Upload Image window click Browse and navigate to the floor plan image you want to use. You may upload PNG, GIF, BMP, TIFF, JPEG, JPG files up to 1MB.
6. Click **Upload**.
7. Click **Save**.

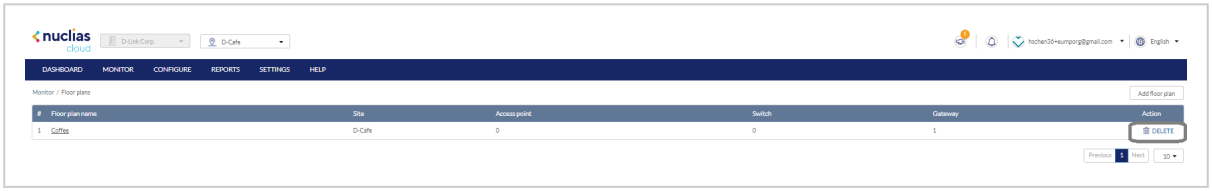
Removing a Custom Floor Plan Image

1. Navigate to **Monitor > Floor Plans**.
2. Select a Site from the Site menu.
3. From the floor plan list, click on the floor plan name.
4. On the floor plan page, click **Remove image**.
5. When prompted to confirm, click **Delete**.
   Note: Deleting a custom image will restore the default floor plan image.
6. Click **Save**.

Deleting a Floor Plan

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

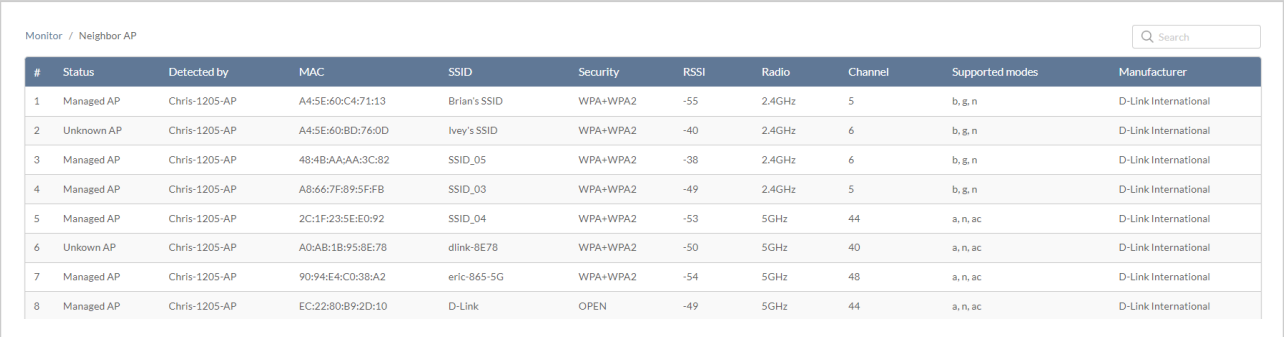
3. From the floor plan list, click the Delete icon under the Actions column of the floor plan you wish to delete.



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

Neighbor AP

The Neighbor AP page provides information about detected APs in the neighborhood for the detection of unexpected APs and deployment of APs to suit the coverage goal. Note that you can only view devices in your authorized level of access.



#	Status	Detected by	MAC	SSID	Security	RSSI	Radio	Channel	Supported modes	Manufacturer
1	Managed AP	Chris-1205-AP	A4:5E:60:C4:71:13	Brian's SSID	WPA+WPA2	-55	2.4GHz	5	b, g, n	D-Link International
2	Unknown AP	Chris-1205-AP	A4:5E:60:BD:76:0D	Ivey's SSID	WPA+WPA2	-40	2.4GHz	6	b, g, n	D-Link International
3	Managed AP	Chris-1205-AP	48:4B:AA:AA:3C:82	SSID_05	WPA+WPA2	-38	2.4GHz	6	b, g, n	D-Link International
4	Managed AP	Chris-1205-AP	A8:66:7F:89:5F:FB	SSID_03	WPA+WPA2	-49	2.4GHz	5	b, g, n	D-Link International
5	Managed AP	Chris-1205-AP	2C:1F:23:5E:E0:92	SSID_04	WPA+WPA2	-53	5GHz	44	a, n, ac	D-Link International
6	Unkown AP	Chris-1205-AP	A0:AB:1B:95:8E:78	dlink-8E78	WPA+WPA2	-50	5GHz	40	a, n, ac	D-Link International
7	Managed AP	Chris-1205-AP	90:94:E4:C0:38:A2	eric-865-5G	WPA+WPA2	-54	5GHz	48	a, n, ac	D-Link International
8	Managed AP	Chris-1205-AP	EC:22:80:B9:2D:10	D-Link	OPEN	-49	5GHz	44	a, n, ac	D-Link International

Wireless Neighbor AP Report

1. Navigate to **Monitor > Neighbor AP**.

The following information is displayed:

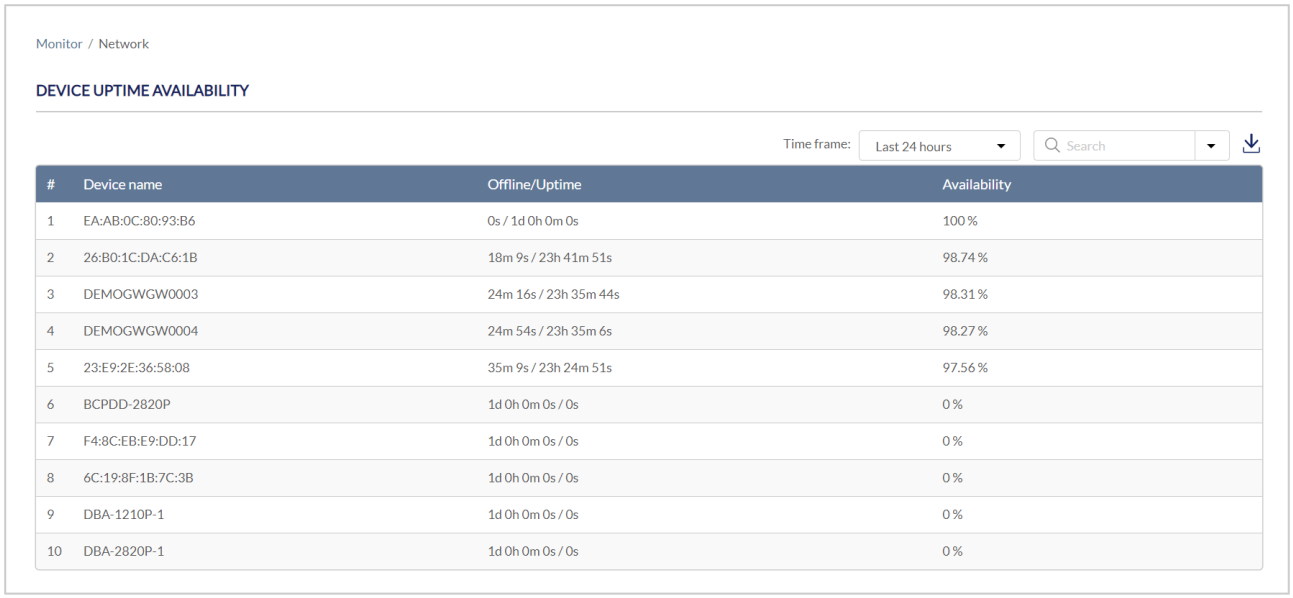
Status	State whether the AP is managed or unknown in the defined site. The site can be selected at the top.
Detected by	The device that detected this neighbor AP.
MAC	The MAC address of this neighbor AP.
SSID	The SSID name of this neighbor AP.
Security	The security method configured on the neighbor AP.
RSSI	Received Signal Strength Indication (RSSI), which measures the power of a received radio signal.
Radio	The radio frequency that the neighbor AP is operating on.
Channel	The channel on which the access point is currently broadcasting.

Supported Modes	The wireless standards that the neighbor AP supports.
Manufacturer	The manufacturer of the neighbor AP.

2. [Optional] Enter a keyword in the Search field to filter the table listing.

Network

The Network page provides information about device availability statistics, bandwidth consumption and connected clients for all types of devices in your organization. For wireless networks, the channel interference information is also provided. Note that you can only view devices in your authorized access level.



#	Device name	Offline/Uptime	Availability
1	EA:AB:0C:80:93:B6	0s / 1d 0h 0m 0s	100 %
2	26:B0:1C:DA:C6:1B	18m 9s / 23h 41m 51s	98.74 %
3	DEMOGWGW0003	24m 16s / 23h 35m 44s	98.31 %
4	DEMOGWGW0004	24m 54s / 23h 35m 6s	98.27 %
5	23:E9:2E:36:58:08	35m 9s / 23h 24m 51s	97.56 %
6	BCPDD-2820P	1d 0h 0m 0s / 0s	0 %
7	F4:8C:EB:E9:DD:17	1d 0h 0m 0s / 0s	0 %
8	6C:19:8F:1B:7C:3B	1d 0h 0m 0s / 0s	0 %
9	DBA-1210P-1	1d 0h 0m 0s / 0s	0 %
10	DBA-2820P-1	1d 0h 0m 0s / 0s	0 %

Device Availability Report

1. Navigate to **Monitor > Network**.
2. Under **Device Uptime Availability**, the following information is displayed:

Device Name	The device in your organization.
Offline/Uptime	The offline duration/uptime duration in the defined time frame. Select the time frame drop-down menu to display the data in last 24 hours, last 7 days, last 14 days, last 30 days, or last 60 days.
Availability	The percentage that a device is up and running during the defined time frame.

1. [Optional] To download the availability report, click **Download** to download it as a CSV file in your browser's default download folder.

2. [Optional] Select a Site from the Search menu to display the devices assigned to the specified site.

Bandwidth Usage Report

The Bandwidth Usage Report displays the following information:

Site Name	The site in your organization.
Usage	The total consumption of Internet bandwidth in the defined time frame. Select the time frame drop-down menu to display the data in last 24 hours, last 7 days, last 14 days, last 30 days, or last 60 days.

1. [Optional] To download the usage report, click **Download** to download it as a CSV file in your browser's default download folder.
2. [Optional] Select a Site from the Search menu to filter the site in your organization.

Clients Overview

The Clients Overview Report displays the following information:

Type	State whether the client is connected through an Ethernet port or wirelessly.
Client Name	The connected client's name in the defined time frame. Select the time frame drop-down menu to display the data in last 24 hours, last 7 days, last 14 days, last 30 days, or last 60 days.
Site	The site of your organization.
MAC Address	The MAC address of the client.
IPv4 Address	The IP address of the client.
Connected to	The device of the organization that the client is connected to.
Usage	The Internet bandwidth consumption.

RSSI	Received Signal Strength Indication, which measures the power of a received radio signal. Range: 0 to -120dB.
SNR	Signal-to-Noise Ratio, which measures the quality of wireless signal by also taking the noise level into account. Range: 0 to 120dB.

1. [Optional] To download the client report, click **Download** to download it as a CSV file in your browser's default download folder.
2. [Optional] Select a Site from the Site drop-down menu.

Channel Overview

The Channel Overview report displays the following information:

Channel	The channel that has been detected having interference.
Interference	The number of unmanaged wireless networks (SSIDs) operating on this channel.
Using	The Nuclias device that uses this channel.

1. [Optional] To download the usage report, click **Download** to download it as a CSV file in your browser's default download folder.
2. [Optional] Select a wireless Device (grouped by Site) from the Device drop-down menu to display only the device in your organization.

Configure

From the Configure menu, you can configure profiles for different device types and models.

The Configure menu also provides management of authentication servers and local authentication database for connection and access control. The Schedule Policies provides scheduling methods for a variety of functions, for example, Traffic Management, Firewall, and Port Schedule. It also allows you to customize splash pages to present to clients in different use cases.

Note: The availability of the menus of the Configuration page depends on the access privilege.

Access Point	The AP section provides configuration menus for AP devices. It allows you to configure profiles based on device model or devices individually. The access management of wireless network using IP ACLs can also be configured. Refer to the Access Point section for more information.
Switch	The Switch section provides configuration menus for switch devices. It allows you to configure profiles based on device model or devices individually. It also allows operations on selected groups of ports such as bandwidth aggregation and port mirroring. Refer to the Switch section for more information.
Gateway	The Gateway section provides configuration menus for gateway devices. It allows you to configure profiles based on device model or devices individually. Refer to the Gateway section for more information.
Authentication	The Authentication section provides Local Authentication database and Authentication Server management to facilitate a variety of authentication methods or infrastructures for Wi-Fi and VPN connectivity. Refer to the Authentication section for more information.

MAC ACLs	The MAC ACLs provides access control by filtering devices' MAC addresses of an Ethernet frame. Refer to the MAC ACLs section for more information.
Walled Garden	The Walled Garden restricts or redirects clients to certain web addresses before they are authenticated for network access. Refer to the Walled Garden section for more information.
Schedule Policies	The Schedule Policies facilitate scheduling for access control and security functions such as port availability for switches, and firewall functions and application control for gateways. Refer to the Schedule Policies section for more information.
Splash Pages	The Splash Pages allow configuration and customization of splash pages to use with the SSID. This can be configured to have users click through or enter credentials to access the network. You can either customize any of the default splash pages or create your own unique splash pages. Refer to the Splash Pages section for more information.

Configure - Access Point

Configure - Access Points

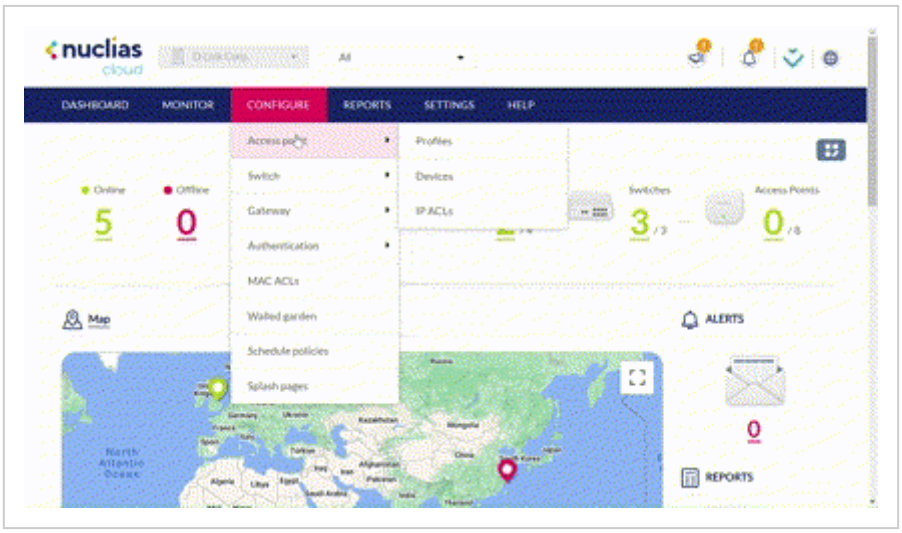
From the Configure section, you can manage Profiles and devices for the organization.

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

Profiles	From the Profiles section, you can create new and edit existing profiles of wireless properties such as SSID and radio settings, and apply profile configuration settings to associated devices.
Devices	From the Devices section, you can add and register devices and configure individual device settings.
IP ACLs	From the IP ACLs section, you can create, manage, and delete IP access control lists used to manage wireless users' network access using their IP addresses.

Profiles

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.



Creating a Profile

After a profile is created, you can configure SSID and wireless settings, set up captive portal pages, and configure other general settings within each profile, .

1. Navigate to **Configure > Access Point > Profiles**.
2. Click **Create Profile**.
3. Enter a name for the Profile and choose the device model.

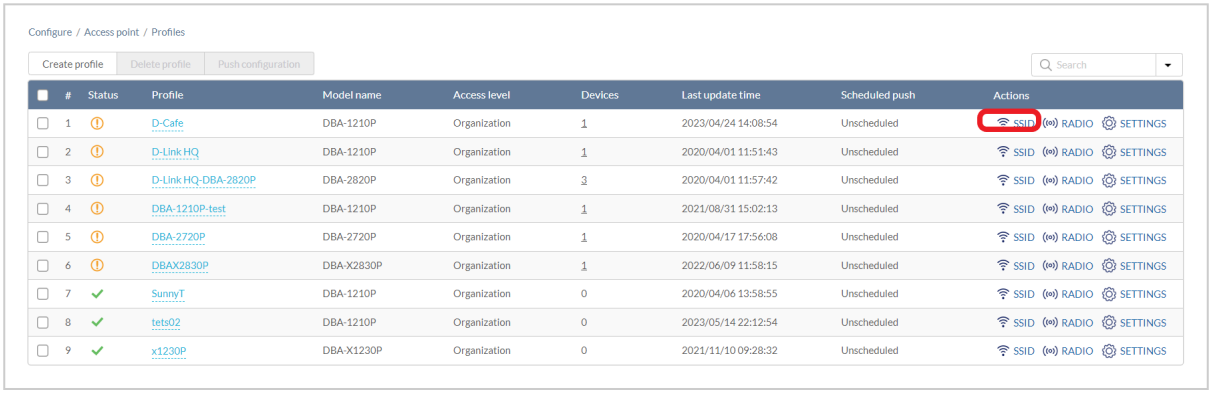
   Note: The Profile can only be used for the selected device model type.
4. Select **Clone** from exist profile and choose a Profile from the drop-down menu to clone an existing Profile. Or select **Use default configuration** to use pre-defined settings. You can modify the settings with the Edit function later.
5. Click **Create Profile**.

Creating an SSID

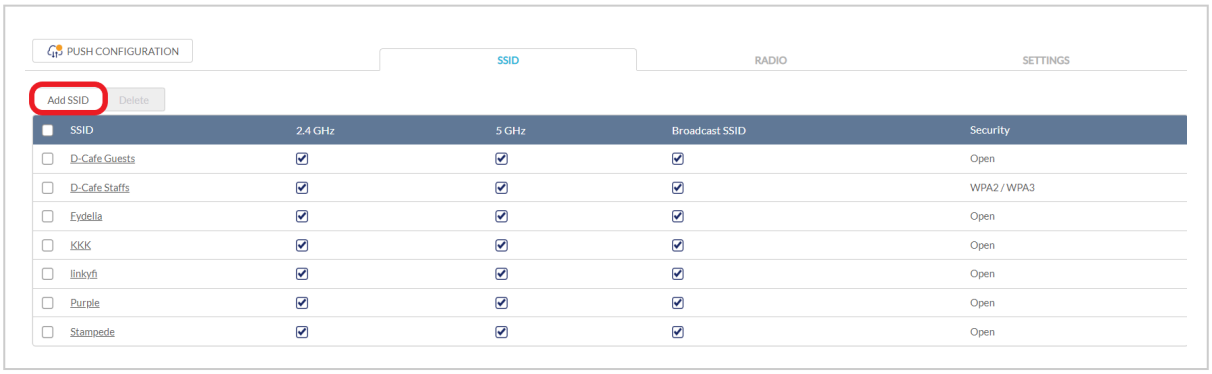
You can create multiple SSIDs under a single Profile and configure each SSID with unique settings to accommodate different wireless usage scenarios.

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

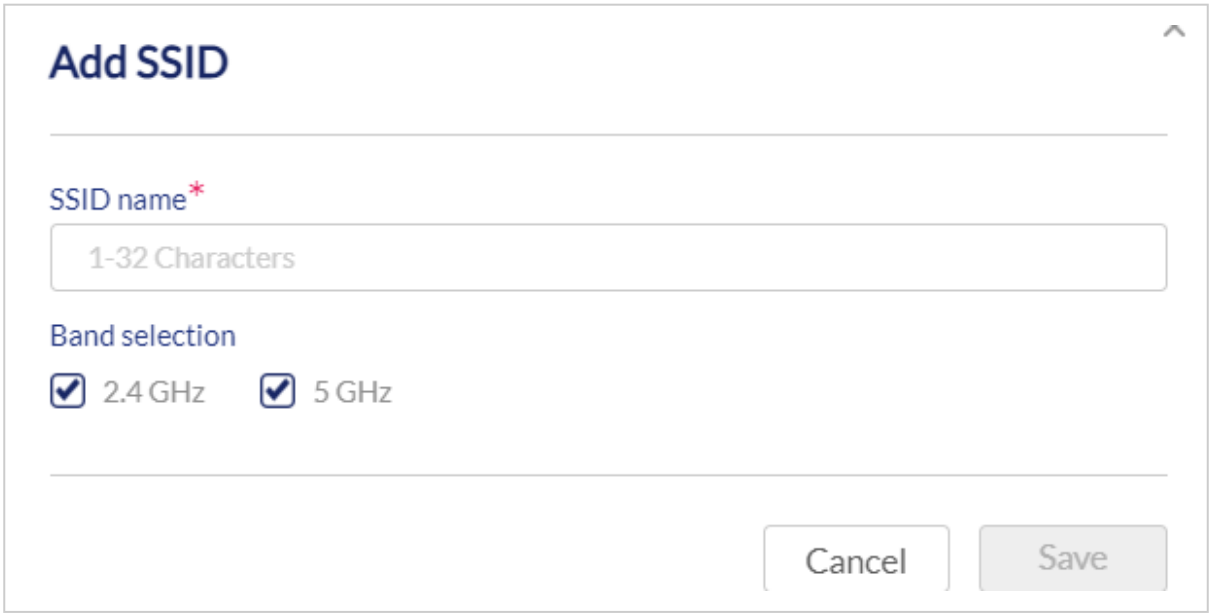
2. From the Profile list, click **SSID** under the Actions column of the Profile you wish to create an SSID for.



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



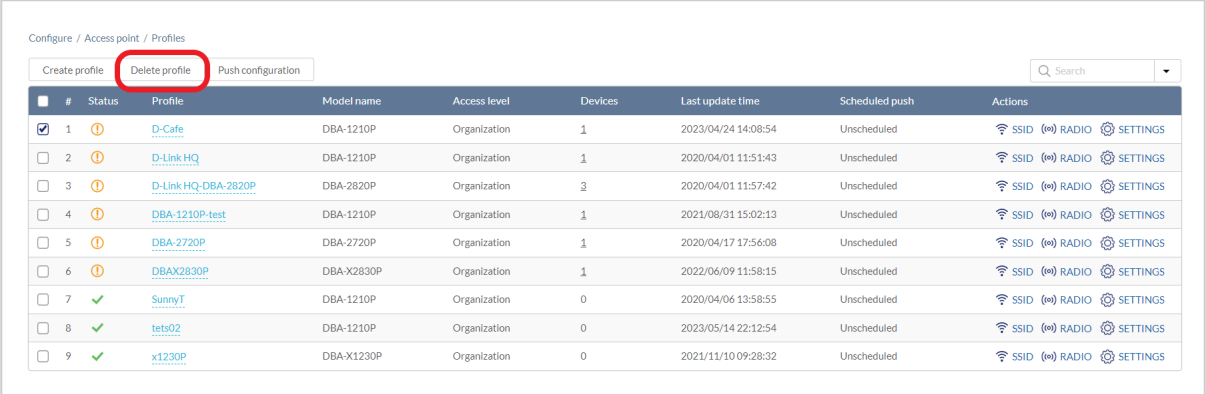
4. Enter a name for the SSID and choose which wireless bands to enable.



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

Deleting Profiles

1. Navigate to **Configure > Access Point > Profiles**.
2. From the Profile list, click the checkbox next to the profiles you which to delete and click **Delete Profile**.



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

Configuring Basic SSID Settings

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

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, Enhanced Open,** or **Enhanced Open+Open, WPA2, WPA/WPA2, WPA3, or WPA2/WPA3**.

   Note: This Open option 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. The Enhanced Open enables better security using encryption and privacy on open networks. The Enhanced Open+Open allows both types of open networks.

Using WPA Security with PSK

For **WPA2, WPA/WPA2, WPA3, or WPA2/WPA3,** specify the following information if **Pre-shared Key (PSK)** or **Simultaneous Authentication of Equals (SAE)** is selected as the Auth method:

Encryption	Select an encryption method.

Passphrase	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.

Using WPA Security with RADIUS Server

For **WPA2, WPA/WPA2, WPA3, or WPA2/WPA3**, select a Primary RADIUS server and an optional secondary server if **RADIUS** is selected as the Auth method. Also select the **Encryption** method and specify the **Group Key Update Interval.** If you have no pre-configured RADIUS servers, click **Add a RADIUS server** and specify the following information:

Server Name	Enter the name of the RADIUS server.
IP Address	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. **Note**: Must be between 2-32 characters.
Authentication Method	[Optional] Select the Authentication Method. The options are PAP, MS-CHAP/MS-CHAPv2, EAP-MD5 or CHAP.
RADIUS Accounting	[Optional] Enable or disable the accounting mechanism. If enabled, enter the IP Address, Port number, Secret and Accounting Interim Interval in seconds.

6. Choose to enable or disable SSID broadcasting.
   Note: If SSID broadcasting is disabled, users will not see the SSID when they scan for available networks 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 guest users 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.
Search Domain	Enter the DNS search domain.

12. Choose to enable or disable VLAN.

13. If VLAN is enabled, specify the following information:
    Note: If the NAT mode is enabled, the VLAN settings will follow the Management VLAN setting instead. Refer to the Configuring_General_Profile_Settings 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	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. Enter the NAS-ID (network access server identifier) to be sent in the RADIUS access request so that the RADIUS server can be notified and choose a policy for that request. If this is left empty, the device UID will be used instead.
16. Click **Save**.
17. 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 available Splash page menu.
7. [Optional] Click **Splash page editor**. Refer to Splash Pages for more information.
8. Specify the following information:

Session Timeout	Enter a duration (in minutes) before the connection session automatically times out. The default is 120 minutes.
Idle timeout	Enter a duration (in minutes) of allowed inactivity before the captive portal page times out.
Session Limited	[Optional] Enter the maximum amount of sessions limited (unlimited, or 1-5).
Traffic Limited	[Optional] Specify how much data (MB/session) a client can transfer in a session. Enter 0 to disable the limitation.
URL Redirection	[Optional] If URL redirection is enabled, users will be redirected to the chosen URL after access to the SSID is granted.
Redirection interval	Enter the time (in minutes) clients will be periodically redirected to the URL.

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. Or click Local authentication List to view the Local authentication database.
12. Specify the following information:

Session Timeout	Enter a duration (in minutes) before the connection session automatically times out. The default is 120 minutes.
Idle timeout	Enter a duration (in minutes) of allowed inactivity before the captive portal page times out. The default is 30 minutes.
Session Limited	[Optional] Enter the maximum amount of sessions limited (unlimited, or 1-5).
Traffic Limited	[Optional] Specify how much data (MB/session) a client can transfer in a session. Enter 0 to not restrict the data amount.
Walled Garden	[Optional] Add a walled garden configuration to the captive portal.
URL Redirection	[Optional]If URL redirection is enabled, users will be redirected to the chosen URL after access to the SSID is granted.

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

Configuring an SSID Captive Portal with Basic Login Page Using a RADIUS or LDAP 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 Pages section for more information.
8. Select **RADIUS or LDAP** as the Basic Login Page type.

Note: Authentication servers can be configured separately. Refer to the Local Authentication section for more information.

9. [Optional] If you have no pre-configured RADIUS or LDAP servers, click **Add a RADIUS server** or **Add an LDAP server** and specify the following information:

Server Name	Enter a name for the server.
IP Address	Enter the IP address of the server.
Port	Enter a port for the server. The range is between 1 and 65535. (Default: 1812 for RADIUS server; 389 for LDAP server).
Base DN	Enter the domain for LDAP, for example, cn=admin, dc=mydomain, dc=local.
Encryption	[Optional] Select SSL or TLS or disable this option for LDAP.
Secret	Enter a shared secret for RADIUS. **Note**: Must be between 2-32 characters.
Authentication Method	[Optional] Select the Authentication Method. The options are PAP, MS-CHAP/MS-CHAPv2, EAP-MD5 or CHAP.
RADIUS Accounting	[Optional] Enable or disable the accounting mechanism. If enabled, enter the IP Address, Port number, Secret and Accounting Interim Interval in seconds.

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

Simultaneous Login	[Optional] Enable to allow the same account to be reused during multiple concurrent sessions. **Note**: Different authentication methods are unrelated regardless if using the same email or not.
Session Timeout	[Optional] Enter a duration (in minutes) before the connection session automatically times out. The default is 120 minutes.

Idle timeout	[Optional] Enter a duration (in minutes) of allowed inactivity before the captive portal page times out.
Session Limited	[Optional] Enter the maximum amount of sessions limited (Unlimited, or 1-5).
Traffic Limited	[Optional] Specify how much data (MB/session) a client can transfer in a session. Enter 0 to not restrict the data amount.
Walled Garden	[Optional] Add a walled garden configuration to the captive portal.
URL Redirection	[Optional] If URL redirection is enabled, users will be redirected to the chosen URL after access to the SSID is granted.
Redirection interval	Enter the time (in minutes) clients will be periodically redirected to the URL.

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 Splash page from the drop-down menu.
7. [Optional] Click Splash page editor to open the splash page editor window. Refer to Splash Pages for more information.
8. Select the required information:

3rd party credentials	Check to the box next to Facebook, Google, Weibo, Line and Twitter to enable logging in using respective account credentials.

Session Timeout	Enter a duration (in minutes) before the connection session automatically times out. The range is 2-1440 minutes.
Idle timeout	Enter a duration (in minutes) of allowed inactivity before the captive portal page times out. The range is 1-1439 minutes.
Simultaneous Login	[Optional] Enable to allow the same account to reuse during multiple concurrent sessions. **Note**: Different authentication methods are unrelated regardless if using the same email or not.
Session Limited	[Optional] Enter the maximum amount of sessions limited. The range is unlimited or 1-5.
Traffic Limited	[Optional] Specify how much data (MB/session) a client can transfer in a session. Enter 0 to disable the limitation.
Walled Garden	[Optional] Add a walled garden configuration to the captive portal.
URL Redirection	[Optional] If URL redirection is enabled, users will be redirected to the chosen URL after access to the SSID is granted.
Redirection interval	Enter the time (in minutes) clients will be periodically redirected to the URL.

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 Pages section for more information.
8. Select **Local authentication** as the Basic Login Page type.
9. 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.
10. [Optional] Click **Add authentication users** to create a new local authentication database. Or select Local authentication list to view the Local authentication database.
11. Specify the following information:

3rd party credentials	Check to the box next to Facebook, Google, Weibo, Line and Twitter to enable logging in using respective account credentials.
Simultaneous Login	Enable to allow the same account to be reused during multiple concurrent sessions. **Note**: Different authentication methods are unrelated regardless if using the same email or not.
Session Timeout	Enter a duration (in minutes) before the connection session automatically times out. The default is 120 minutes.
Idle timeout	Enter a duration (in minutes) of allowed inactivity before the captive portal page times out. The default is 30 minutes.
Session Limited	Enter the maximum amount of sessions limited (unlimited or 1-5).
Traffic Limited	[Optional] Specify how much data (MB/session) a client can transfer in a session. Enter 0 to not restrict the data amount.
Walled Garden	[Optional] Add a walled garden configuration to the captive portal.
URL Redirection	[Optional] If URL redirection is enabled, users will be redirected to the chosen URL after access to the SSID is granted.
Redirection interval	Enter the time (in minutes) clients will be periodically redirected to the URL.

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

Configuring an SSID Captive Portal with Basic and Third Party Login Using a RADIUS or LDAP 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 Pages section for more information.
8. Select **RADIUS** or **LDAP Server** as the Basic Login Page type.

   Note: Authentication servers can be configured separately. Refer to the Local Authentication section for more information.

9. [Optional] If you have no pre-configured RADIUS or LDAP servers, click **Add a RADIUS server** or **Add an LDAP server** and specify the following information:

Server Name	Enter a name for the server.
IP Address	Enter the IP address of the server.
Port	Enter a port for the server. The range is between 1 and 65535. (Default: 1812 for RADIUS server; 389 for LDAP server).
Base DN	Enter the domain for LDAP, for example, cn=admin, dc=mydomain, dc=local.
Encryption	[Optional] Select SSL or TLS or disable this option for LDAP.
Secret	Enter a shared secret for RADIUS. **Note**: Must be between 2-32 characters.
Authentication Method	[Optional] Select the Authentication Method. The options are PAP, MS-CHAP/MS-CHAPv2, EAP-MD5 or CHAP.

RADIUS Accounting	[Optional] Enable or disable the accounting mechanism. If enabled, enter the IP Address, Port number, Secret and Accounting Interim Interval in seconds.

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

3rd party credentials	Check to the box next to Facebook, Google, Weibo, Line and Twitter to enable logging in using respective account credentials.
Simultaneous Login	Enable to allow the same account to be reused during multiple concurrent sessions. **Note**: Different authentication methods are unrelated regardless if using the same email or not.
Session Timeout	Enter a duration (in minutes) before the connection session automatically times out. The default is 120 minutes.
Idle timeout	Enter a duration (in minutes) of allowed inactivity before the captive portal page times out. The default is 30 minutes.
Session Limited	Enter the maximum amount of sessions limited (unlimited or 1-5).
Traffic Limited	[Optional] Specify how much data (MB/session) a client can transfer in a session. Enter 0 to not restrict the data amount.
Walled Garden	[Optional] Add a walled garden configuration to the captive portal.
URL Redirection	[Optional] If URL redirection is enabled, users will be redirected to the chosen URL after access to the SSID is granted.
Redirection interval	Enter the time (in minutes) clients will be periodically redirected to the URL.

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

Configuring an SSID Captive Portal with SMS 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 SMS Authentication** as the splash page type.
6. Select an SMS 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 Pages section for more information.
8. Select an SMS configuration from the drop-down menu.

Note: SMS settings can be configured separately. Refer to the SMS Configuration section for more information.

9. If you do not yet have an SMS configuration, click **Add Twilio SMS Settings** and add the following information:

Name	Enter a name for the Twilio service profile.
Twilio Account SID	Enter your Twilio account SID.
Twilio Auth Token	Enter the authentication token for your Twilio account.
Twilio from Number	Enter the number of your Twilio account.
Resend after (minutes)	The elapse time for sending another SMS. Enter 0 to disable the limitation.
Maximum Resend (times)	The maximum number of times that an SMS can be resent. Enter 0 to restrict it to one time only.
Maximum Request (times)	The maximum number of times that an SMS for password purposes can be requested. Enter 0 to disable the restriction.

Denial Period	The amount of waiting time for another request after the Maximum Resend or Request limit has been reached. Enter 0 to disable the restriction.
OTP Expires (minutes)	The amount of time that a password sent through SMS is valid.
Allowed Phone Prefix	Country calling codes that are allowed to use SMS service for sending password. Use "," to separate code list, e.g. +886,+91. The default is "*" which means all country codes are allowed.

1. Specify the following information:

Simultaneous Login	Enable to allow the same account to be reused during multiple concurrent sessions. **Note**: Different authentication methods are unrelated regardless if using the same email or not.
Session Timeout	Enter a duration (in minutes) before the connection session automatically times out. The default is 120 minutes.
Idle timeout	Enter a duration (in minutes) of allowed inactivity before the captive portal page times out. The default is 30 minutes.
Traffic limited	[Optional] Specify how much data (MB/session) a client can transfer in a session. Enter 0 to disable the limitation.
Walled Garden	[Optional] Add a walled garden configuration to the captive portal.
URL Redirection	If URL redirection is enabled, users will be redirected to the chosen URL after access to the SSID is granted.
Redirection interval	Enter the time (in minutes) clients will be periodically redirected to the URL.

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

Configuring an SSID Captive Portal with Email Authentication, SMS Authentication and Third Party 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 **email authentication, SMS authentication and third party credentials** as the Splash page type.
6. [Optional] Click Splash page editor to open the splash page editor window. Refer to the Splash Pages section for more information.
7. Select a Grace Period from the drop-down menu to define how much time users have for email verification before timing out. The default is 5 minutes.
8. Select the amount of times a guest user can be authenticated on Wi-Fi in one day. The default time is 2.
9. Enter a time limit for guest users to request another email authentication if they previously failed to connect and/or their grace period expired. The default is 30 minutes.
10. Select an SMS configuration from the drop-down menu.

    Note: SMS settings can be configured separately. Refer to the SMS Configuration section for more information.

11. If you do not yet have an SMS configuration, click **Add Twilio SMS Settings** and add the following information:

Name	Enter a name for the Twilio service profile.
Twilio Account SID	Enter your Twilio account SID.
Twilio Auth Token	Enter the authentication token for your Twilio account.
Twilio from Number	Enter the number of your Twilio account.
Resend after (minutes)	The elapse time for sending another SMS. Enter 0 to disable the limitation.
Maximum Resend (times)	The maximum number of times that an SMS can be resent. Enter 0 to restrict it to one time only.

Maximum Request (times)	The maximum number of times that an SMS for password purposes can be requested. Enter 0 to disable the restriction.
Denial Period	The amount of waiting time for another request after the Maximum Resend or Request limit has been reached. Enter 0 to disable the restriction.
OTP Expires (minutes)	The amount of time that a password sent through SMS is valid.
Allowed Phone Prefix	Country calling codes that are allowed to use SMS service for sending password. Use "," to separate code list, e.g. +886,+91. The default is "*" which means all country codes are allowed.

12. Specify the following information:

3rd party credentials	Check to the box next to Facebook, Google, Weibo, Line and Twitter to enable logging in using respective account credentials.
Simultaneous Login	[Optional] Enable to allow the same account to be reused during multiple concurrent sessions. **Note**: Different authentication methods are unrelated regardless if using the same email or not.
Session Timeout	Enter a duration (in minutes) before the connection session automatically times out. The default is 120 minutes.
Idle timeout	[Optional] Enter a duration (in minutes) of allowed inactivity before the captive portal page times out. The default is 30 minutes.
Session Limited	[Optional] Enter the maximum amount of sessions limited (unlimited or 1-5).
Traffic limited	[Optional] Specify how much data (MB/session) a client can transfer in a session. Enter 0 to not restrict the data amount.
Walled Garden	[Optional] Add a walled garden configuration to the captive portal.

URL Redirection	[Optional] If URL redirection is enabled, users will be redirected to the chosen URL after access to the SSID is granted.
Redirection interval	Enter the time (in minutes) clients will be periodically redirected to the URL.

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

Configuring an SSID with an External Captive Portal

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 External Captive Portal** as the Splash page type.
6. Enter your custom external captive portal splash page URL.
7. Enter the IP address for your primary RADIUS server.
8. [Optional] Enter a secondary RADIUS server.
9. [Optional] Enable or disable MAC authentication.
10. Specify the following information:

Session Timeout	Enter a duration (in minutes) before the connection session automatically times out. The default is 120 minutes.
Idle timeout	Enter a duration (in minutes) of allowed inactivity before the captive portal page times out. The default is 30 minutes.
Session Limited	Enter the maximum amount of sessions limited (unlimited or 1-5).
Walled Garden	[Optional] Add a walled garden configuration to the captive portal.

11. Click **Save**.

12. Click **Push Configuration**.

Configuring an SSID with Facebook Wi-Fi

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 Facebook Wi-Fi** to redirect users to visit a designated Facebook page and check in.
6. Click **Configure** to configure your Facebook Wi-Fi settings.
7. Click **Save**. If you want to delete a connected Facebook page, click **Delete**.
8. Click **Push Configuration**.

Configuring SSID Access Control Settings

Configuring SSID MAC Filtering Settings Using MAC ACL

Using MAC Access Control Lists (ACL), you 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. Select **MAC ACLs** as the Filter type.
7. 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

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

Select a primary RADIUS server database from the drop-down menu.

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 Server** as the Filter type.

Note: Authentication servers can be configured separately. Refer to the Local Authentication section for more information.

7. [Optional] If you have no pre-configured RADIUS servers, click **Add a RADIUS server** and specify the following information:

Server Name	Enter a name for the RADIUS server.
IP Address	Enter the IP address of the RADIUS server.
Port	Enter a port for the RADIUS server. The range is between 1 and 65535 and default is 1812.
Secret	Enter a shared secret. **Note**: Must be between 2-32 characters.
Authentication Method	[Optional] Select the Authentication Method. The options are PAP, MS-CHAP/MS-CHAPv2, EAP-MD5 or CHAP.
RADIUS Accounting	[Optional] Enable or disable the accounting mechanism. If enabled, enter the IP Address, Port number, Secret and Accounting Interim Interval in seconds.

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), you can manage access to external resources using the clients' IP addresses. Clients with IP addresses corresponding to IP addresses in the ACL can be allowed or denied access to IP addresses outside the current wireless 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.
8. [Optional] Click **Add an IP ACL** to create a new IP ACL.
9. Click **Save**.
10. Click **Push Configuration**.

Configuring SSID Schedule 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 **Scheduled Availability** tab.
5. Select a desired Schedule policy.
6. [Optional] Click the 24 Hours or AM/PM tabs to change the time display format.
7. To create a new Schedule Policy, click **Schedule Policy**. Click **Add Schedule Policy** and click the corresponding radio button to enable or disable the SSID during the selected day of the week. If Off is selected, the SSID will not be available for use that day.
8. If On is selected, enter times in the From and To fields to define at what hours of the day the SSID will be available to connect to.

Note: To create a Schedule Policy, refer to Schedule Policies for more information.

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

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:

Client Limit	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.

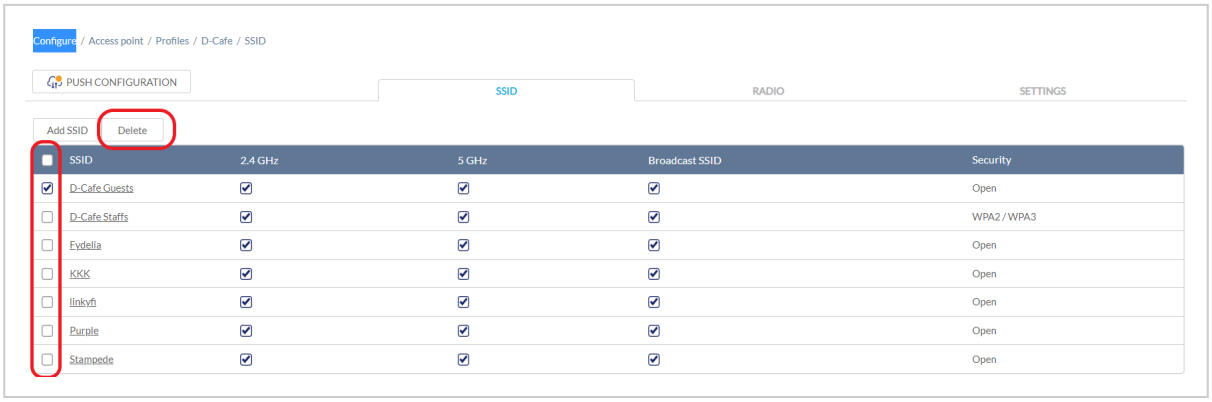
Max Downstream	Enter a maximum downloading bandwidth limit (in Kbps) for this SSID.
Max Client Upstream	Enter a maximum uploading bandwidth limit (in Kbps) for each client connected to this SSID.
Max Client Downstream	Enter a maximum downloading bandwidth limit (in Kbps) for each client connected to 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 Multicast 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.
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.
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.

Weak RSSI Client Associations Attempts	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**.



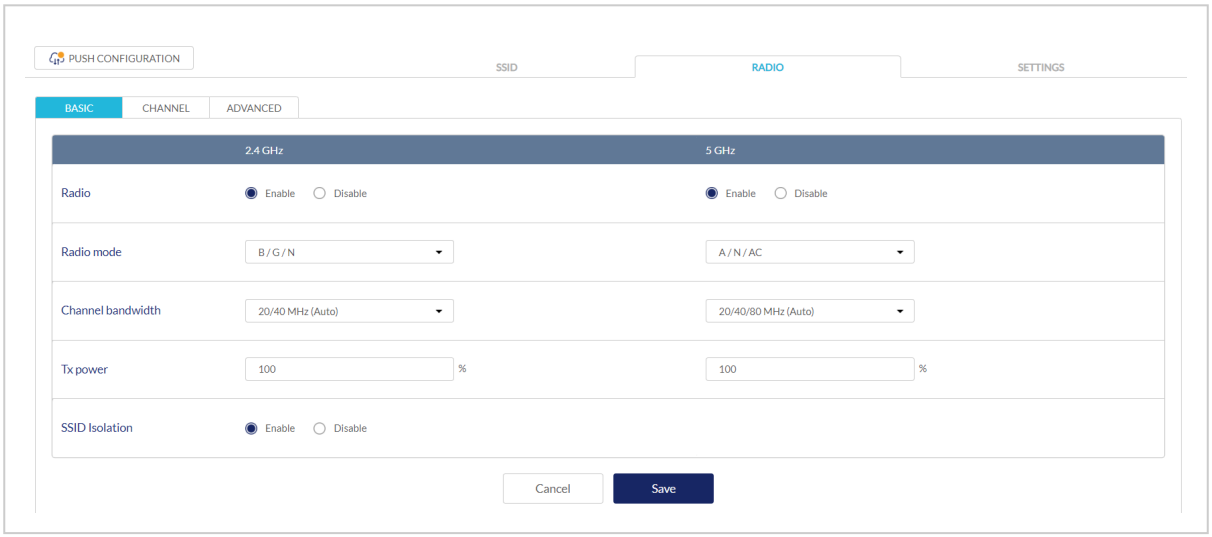
5. When prompted to confirm, click **Yes**.

Configuring Profile Radio Settings

From the Radio window, you 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. **Note**: The available channels may vary based on the country of operation.
Force auto channel scan	Choose to enable or disable the auto channel scan to be forced. Forcing the scan is more accurate, but wireless clients may be disconnected during the scan.
Auto channel interval	Specify the interval (in hours) at which the auto-channel scan is performed.

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

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.

Multicast 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.
UAPSD	Choose to enable or disable Unscheduled Automatic Power Save Delivery (UAPSD). This feature allows connected clients to save power.
Short guard interval	Choose to enable or disable Short Guard Interval. This reduces signal loss from the multipath effect where multiple signals reach the receiving antenna at different times.

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

Configuring General Profile Settings

From the General Profile settings, you 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.
Fast Roaming	Chose to enable or disable the Fast Roaming feature. **Note**: This feature cannot be enabled for SSIDs which enable NAT mode or WPA3 security.
Management VLAN	Enable or disable the Management VLAN function. If enabled, enter the VLAN tag for the Management VLAN. Once it is enabled, make sure that the device administering the wireless network is a member of this VLAN. Note that the management VLAN setting applies to the SSID when NAT mode is enabled. Go to the Basic tab for the NAT mode setting.

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 settings, the changes need to be pushed to all associated devices in order to apply these changes.

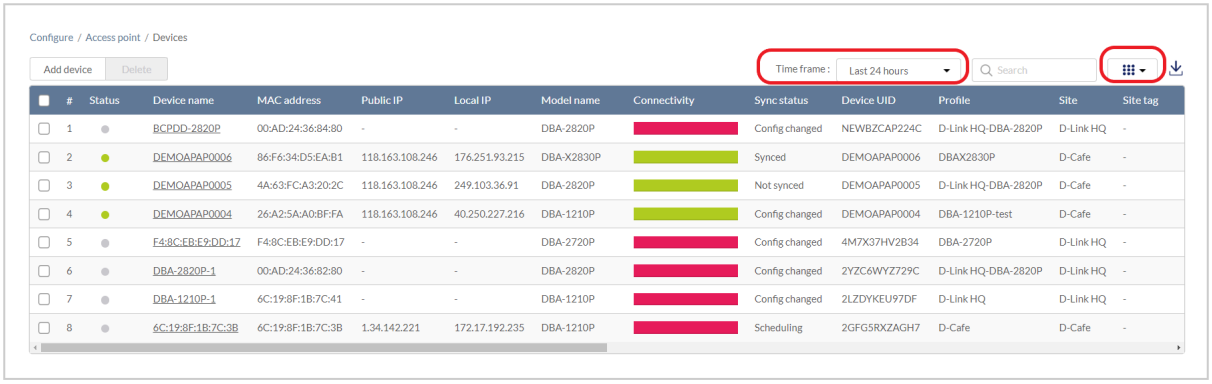
1. Navigate to **Configure > Access Point > Profiles**.
2. Check the profiles that you wish to update the configuration settings from the list.
3. Click **Push Configuration** at the top.
4. You can choose to Push the Configuration now or Schedule the push at a later time.
5. Click **Schedule Changes**.
   Note: A result window will appear providing a summary of the update status. The Status column will also reflect the status of the profile configuration changes.

Devices

From the Devices page, you can add 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 **Configure > Access Point > Devices**.
2. Select a time frame from the drop-down menu.
3. Click the filter selection in the top-right.

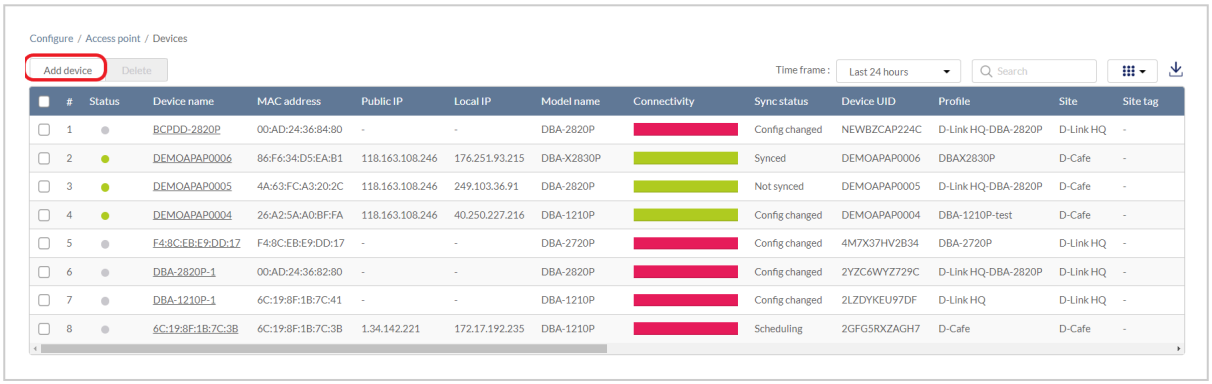


#	Status	Device name	MAC address	Public IP	Local IP	Model name	Connectivity	Sync status	Device UID	Profile	Site	Site tag
1		BCPDD-2820P	00:AD:24:36:84:80	-	-	DBA-2820P		Config changed	NEWBZCAP224C	D-Link HQ-DBA-2820P	D-Link HQ	-
2		DEMOAPAP0006	86:F6:34:D5:EA:B1	118.163.108.246	176.251.93.215	DBA-X2830P		Synced	DEMOAPAP0006	DBAX2830P	D-Cafe	-
3		DEMOAPAP0005	4A:63:FC:A3:20:2C	118.163.108.246	249.103.36.91	DBA-2820P		Not synced	DEMOAPAP0005	D-Link HQ-DBA-2820P	D-Cafe	-
4		DEMOAPAP0004	26:A2:5A:A0:BF:FA	118.163.108.246	40.250.227.216	DBA-1210P		Config changed	DEMOAPAP0004	DBA-1210P-test	D-Cafe	-
5		F4:8C:EB:E9:DD:17	F4:8C:EB:E9:DD:17	-	-	DBA-2720P		Config changed	4M7X37HV2B34	DBA-2720P	D-Link HQ	-
6		DBA-2820P-1	00:AD:24:36:82:80	-	-	DBA-2820P		Config changed	2YZC6WYZ729C	D-Link HQ-DBA-2820P	D-Link HQ	-
7		DBA-1210P-1	6C:19:8F:1B:7C:41	-	-	DBA-1210P		Config changed	2LZDYKEU97DF	D-Link HQ	D-Link HQ	-
8		6C:19:8F:1B:7C:3B	6C:19:8F:1B:7C:3B	1.34.142.221	172.17.192.235	DBA-1210P		Scheduling	2GFG5RXZAGH7	D-Cafe	D-Cafe	-

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

Adding and Registering Devices

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



#	Status	Device name	MAC address	Public IP	Local IP	Model name	Connectivity	Sync status	Device UID	Profile	Site	Site tag
1		BCPDD-2820P	00:AD:24:36:84:80	-	-	DBA-2820P		Config changed	NEWBZCAP224C	D-Link HQ-DBA-2820P	D-Link HQ	-
2		DEMOAPAP0006	86:F6:34:D5:EA:B1	118.163.108.246	176.251.93.215	DBA-X2830P		Synced	DEMOAPAP0006	DBAX2830P	D-Cafe	-
3		DEMOAPAP0005	4A:63:FC:A3:20:2C	118.163.108.246	249.103.36.91	DBA-2820P		Not synced	DEMOAPAP0005	D-Link HQ-DBA-2820P	D-Cafe	-
4		DEMOAPAP0004	26:A2:5A:A0:BF:FA	118.163.108.246	40.250.227.216	DBA-1210P		Config changed	DEMOAPAP0004	DBA-1210P-test	D-Cafe	-
5		F4:8C:EB:E9:DD:17	F4:8C:EB:E9:DD:17	-	-	DBA-2720P		Config changed	4M7X37HV2B34	DBA-2720P	D-Link HQ	-
6		DBA-2820P-1	00:AD:24:36:82:80	-	-	DBA-2820P		Config changed	2YZC6WYZ729C	D-Link HQ-DBA-2820P	D-Link HQ	-
7		DBA-1210P-1	6C:19:8F:1B:7C:41	-	-	DBA-1210P		Config changed	2LZDYKEU97DF	D-Link HQ	D-Link HQ	-
8		6C:19:8F:1B:7C:3B	6C:19:8F:1B:7C:3B	1.34.142.221	172.17.192.235	DBA-1210P		Scheduling	2GFG5RXZAGH7	D-Cafe	D-Cafe	-

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 **XXXXXXXXXXXX**. When entering the UID, do not include dashes.
Device name	Enter a name for the device.
Site	Select a Site to link this device to.
Profile	Select a Profile for this device. The device will use the settings configured in that profile.
License Key	[Optional] Enter the device license key. Note: Every new device will be issued a one year free license key. Once expired, an additional license must be purchased to continue using the device.

4. Click **Save**.

Editing a Device

Editing the Device Name

1. Navigate to **Configure > Access Point > Devices**.
2. From the device list, click the device name link. The Device Information page appears.
3. Click the device name in the Device 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 link.
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 link.
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 link.
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 server #1	Enter a DNS server address.

DNS server #2, #3	Enter the optional DNS server addresses.

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, you 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 link.
3. Click the **SSID** tab.
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, you 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 link.
3. Click the **Radio** tab.
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 link.
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 link.
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 link.
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 link.
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 link.
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 link.
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**.
6. **Note**: Deleting a license key from a device will reclassify it as Unused in the license management inventory until it is reassigned to another device.

Deleting Devices

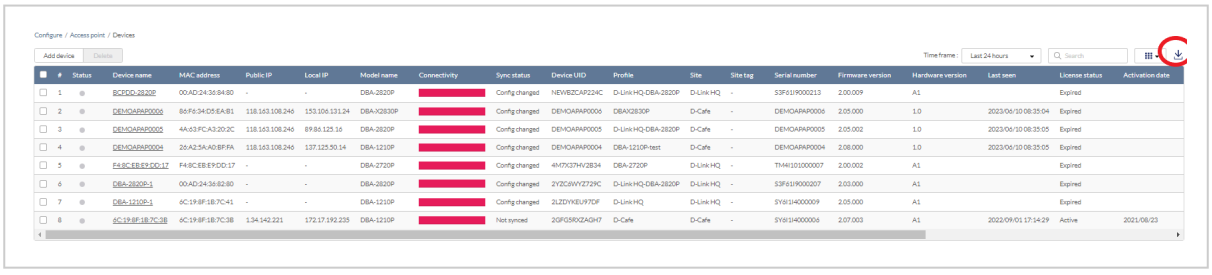
Assigned devices can be unassigned and remain in the device inventory so they can be reassigned at a later point.

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. You will be asked whether you would like to delete the device permanently or move it to the inventory.

Downloading 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 > Devices**.
2. From the device list, click the **Download** icon in the top-right.



IP ACLs

The IP ACLs restrict wireless clients' access to resources outside of the wireless network.

Creating an IP ACL Using Single Entries

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

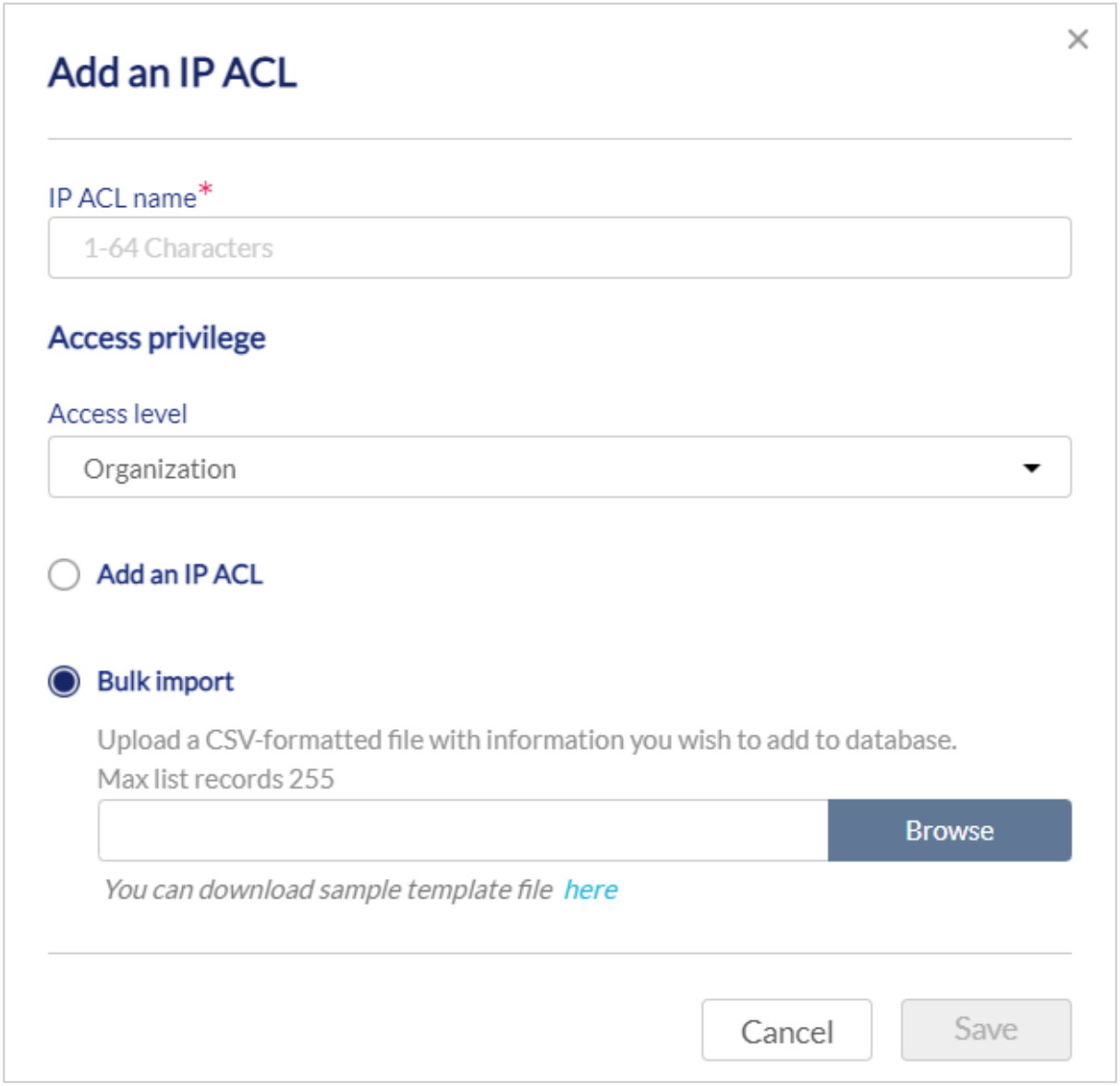
IP address [#]	Enter a valid IP address.
Subnet Mask [#]	Enter a valid subnet mask.

6. [Optional] Click **Add** to add additional IP entries. Repeat step 2 to 5 for each new entry.
7. Click **Save**.

Creating an IP ACL Using Bulk Import

1. Navigate to **Configure > Access Point > IP ACLs**.
2. Click **Add an IP ACL**.
3. In the Add an IP ACL address window, enter a name for the IP ACL.
4. Select **Bulk import**.

5. [Optional] Download the reference sample template.

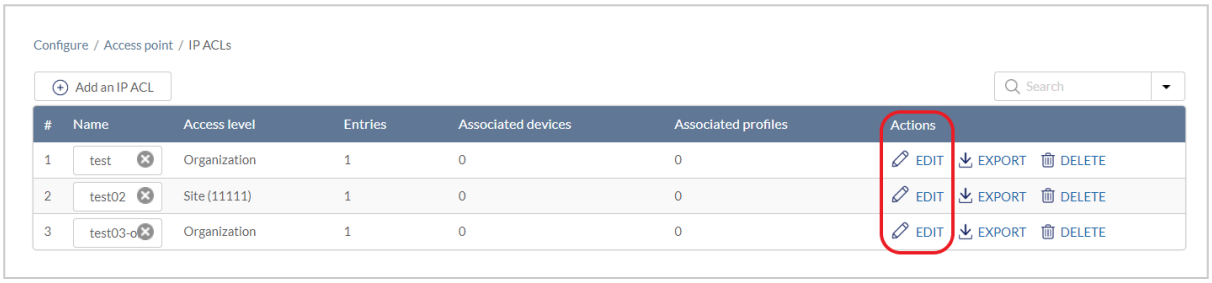


6. Click **Browse**.
7. Locate the CSV-formatted file containing the IP addresses and subnet masks using the following format:
   [IP address][subnet mask]
8. Click **Save**.

Editing Existing IP ACLs

Adding IP Addresses to an Existing IP ACL

1. Navigate to **Configure > Access Point > IP ACLs**.
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** to add more IP addresses.
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 ACLs**.
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, enter the correct IP address and subnet mask for the IP entry you wish to edit.
4. Click **Save**.

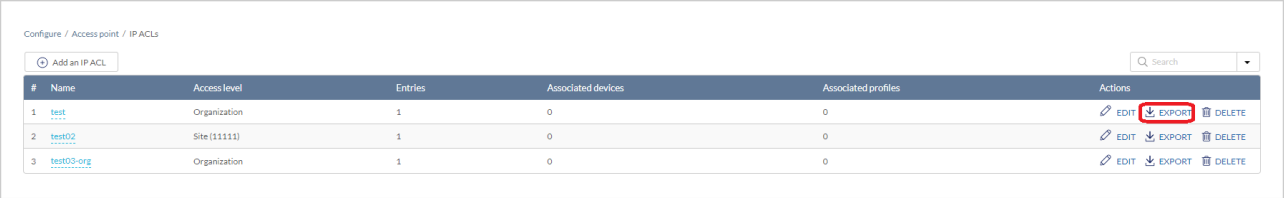
Deleting an IP Address From an Existing IP ACL

1. Navigate to **Configure > Access Point > IP ACLs**.
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 ACLs**.
2. From the IP ACL list, click **Export** to export the desired IP ACL entry.



Deleting an IP ACL

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

Configure - Switch

Overview

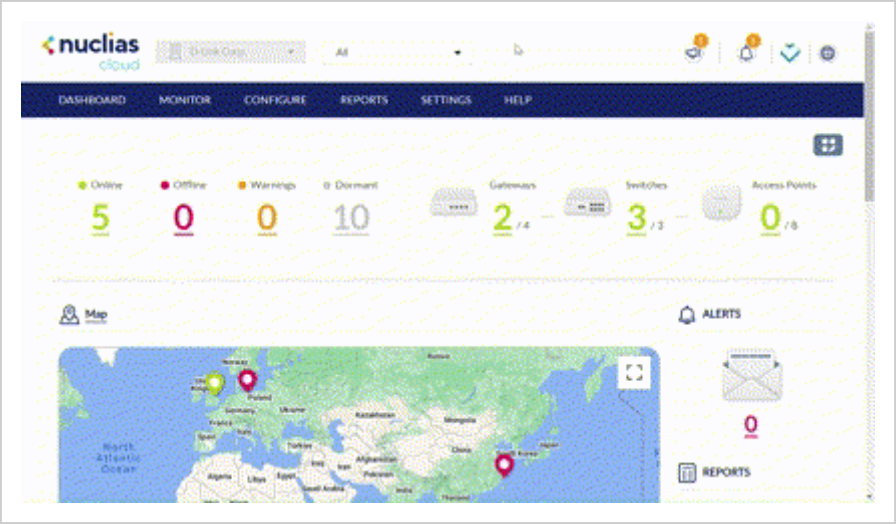
From the Configure section, you can manage profiles and devices for organizations. Because profiles and devices are managed on the organization level and are not shared between organizations, you must select a specific organization from the organization drop-down menu.

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

Profiles	From the Profiles section, you can create new and edit existing profiles, and push profile configuration settings to device groups.
Devices	From the Devices section, you can add a single device and configure and register individual devices.
Switch Ports	From the Switch Ports section, you can configure features on a single port or a group of selected ports.

Profiles

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.



Creating a Profile

After a profile is created, you can configure switch port functionality, port activity schedules, and advanced features including VLAN, Quality of Service, and access control functions in each profile.

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. Select the Access Level for the accessibility level of the profile.
5. [Optional] Select **Clone from existing profile** and choose a Profile from the drop-down menu to clone an existing Profile.
6. Click **Create Profile**.

Deleting Profiles

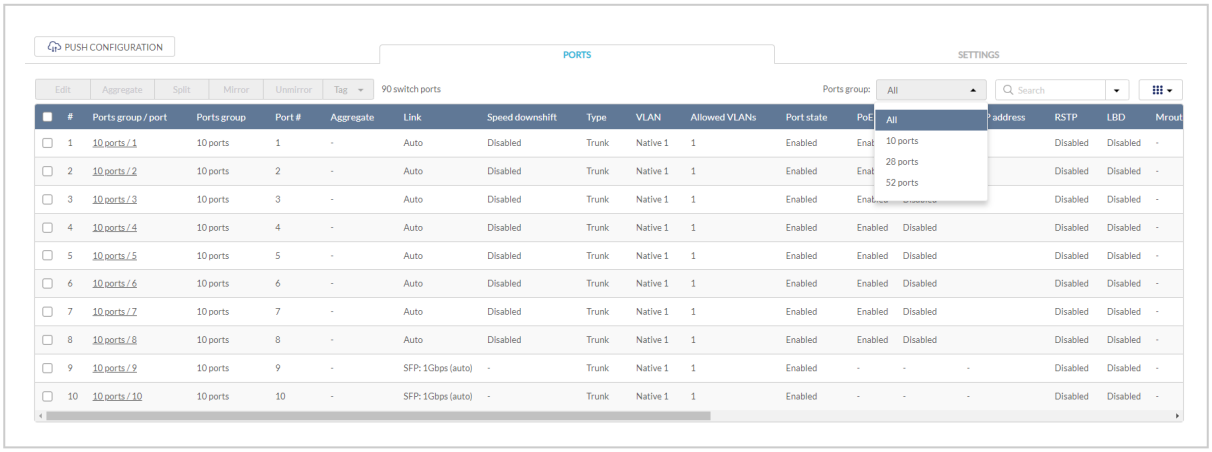
1. Navigate to **Configure > Switch > Profiles**.
2. Click the checkbox next to the Profiles you wish to delete.
3. From the Profile list, click **Delete profile** at the top of the table.
4. When prompted to confirm, click **Yes**.

Configuring Switch Port Settings

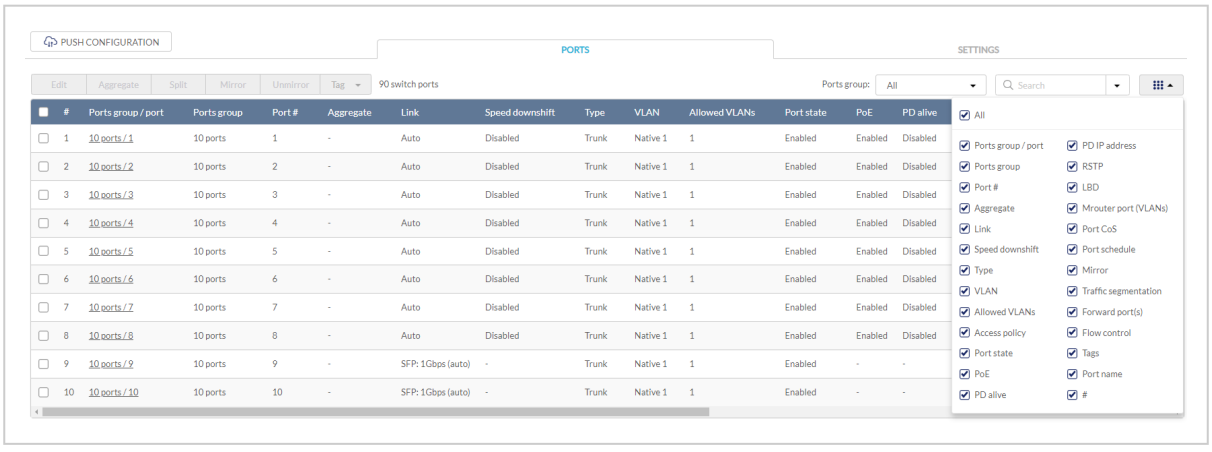
From the Ports window, you can configure basic and advanced settings for individual ports or groups of ports. Switch ports are categorized into group ports, with each group referring to the number of ports on the physical switch model. For example, port group 10 configures port settings for 10-port switches. 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 **Ports group** 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 individual ports 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 RSTP. **Note**: RSTP cannot be used in conjunction with LBD. **Note**: 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.

	Note: LBD cannot be used in conjunction with RSTP.
Port CoS	Select the Class of Service (CoS) value (0-7) to mark the packets transmitting out of this port.
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 if the Trunk type is selected.
Allowed VLANs	Enter the IDs of the VLANs that can route traffic through this port if the Trunk type is selected. Enter **All** to allow all traffic from all VLANs to pass through this port.
Access VLAN	Enter the ID of the VLAN the port belongs to if the Access type is selected.
Access Policy	Select the Access Policy for this port if the Access type is selected. The options include Disabled, MAC Whitelist, Port Security Delete-on-Time Mode, and Port Security Permanent Mode.
Static Whitelisted MACs	Enter the MAC addresses that can access this port to restrict access to this port to devices with specific MAC addresses. If entering multiple MAC addresses, enter only one address per line.
Dynamic Whitelist Size Limit	Enter the maximum number of allowed MAC addresses that the device should learn dynamically for the Port Security Delete-on-time Mode or Port Security Permanent Mode.
Dynamic Whitelisted MACs	Display the learned MAC addresses for the Port Security Delete-on-time mode and Port Security Permanent Mode.

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.
Link (SFP)	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.
Speed downshift	Enables/disables automatic speed downshift on the supported interface when the designated maximum speed cannot be established.
PoE	Choose to enable or disable Power over Ethernet (PoE) functionality on this port. **Note**: The PoE setting will only apply to ports that support Power over Ethernet.
PD Alive	Enable or disable the automatic detection of the Powered Devices status.
PD IP address	Enter the IP address of the Powered Device.
Port Schedule	Choose a port schedule. Port schedules are separately configured. Refer to the Creating a Switch Port Schedule section.
Traffic segmentation	Enable or disable traffic segmentation on this port to further restrict traffic flow in your network. If enabled, select the forward ports.
Forward Ports	Select the forward ports if traffic segmentation is enabled.
Flow control	Enable or disable the flow control on the port to regulate the data transfer rate between two devices.

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

Aggregating Multiple Switch Profile Ports

Port aggregation allows you 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.

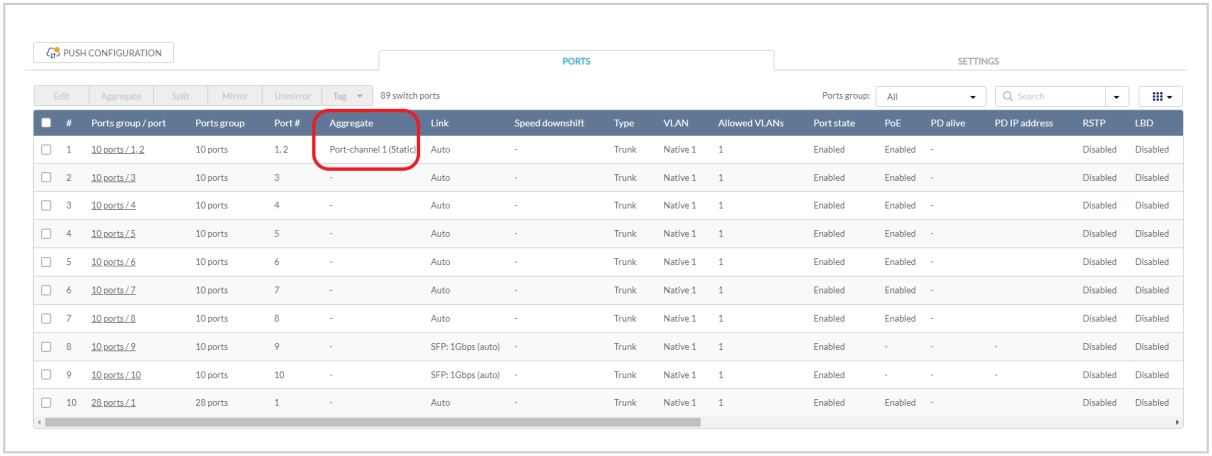
Note: Port aggregation is not supported if the port type is set to "Access". To configure the port type, refer to the above Configuring Profile Port Settings for One or More Switch Ports section for more information.

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 Aggregate

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.

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**.

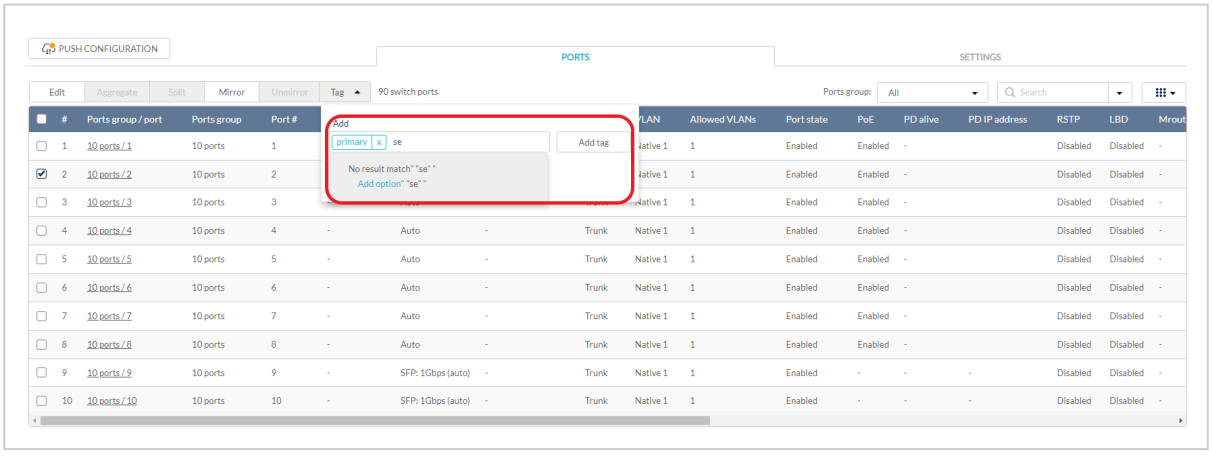
Undoing Port Traffic Mirroring

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.**
5. Click **Delete port mirror**.
6. Click **Push Configuration**.

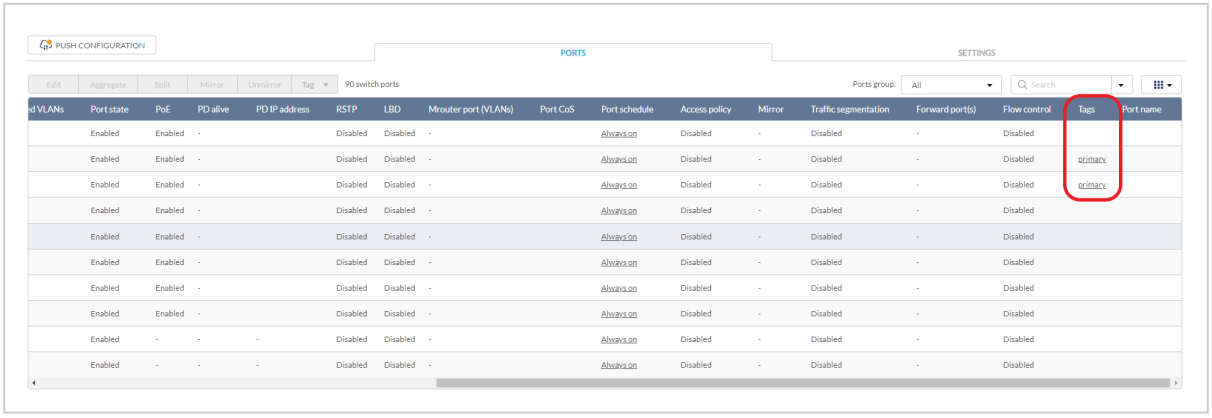
Adding a Tag to One or More Switch Profile Ports

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 tag**.
   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 > 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 tag**.

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.

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

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. You can enable/disable RSTP of individual ports under the Switch Ports page, or at **Configure > Switch > Profile > Ports**. **Note**: RSTP must be manually enabled under BOTH Switch Settings of a profile and Switch Ports.

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 RSTP Configuration section, select **Enable** next to RSTP.
5. Click **Add** to add an RSTP bridge priority.
6. 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.

7. [Optional] Click **Add** to add additional bridge priorities.
8. Click **Add**.
9. [Optional] To delete a bridge priority, check the checkbox next to the switch and click **Delete under** the Actions column.
10. Click **Save**.
11. 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: Up to 5 DHCP servers can be whitelisted.
6. Click **Save**.
7. Click **Push Configuration**.

Configuring Voice VLAN

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 in addition to the pre-configured OUIs.
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	
00:03:6B:00:00:00	FF:FF:FF:00:00:00	Cisco	
00:09:6E:00:00:00	FF:FF:FF:00:00:00	Avaya	
00:0F:E2:00:00:00	FF:FF:FF:00:00:00	Huawei&3COM	
00:60:B9:00:00:00	FF:FF:FF:00:00:00	NEC&Philips	
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**.

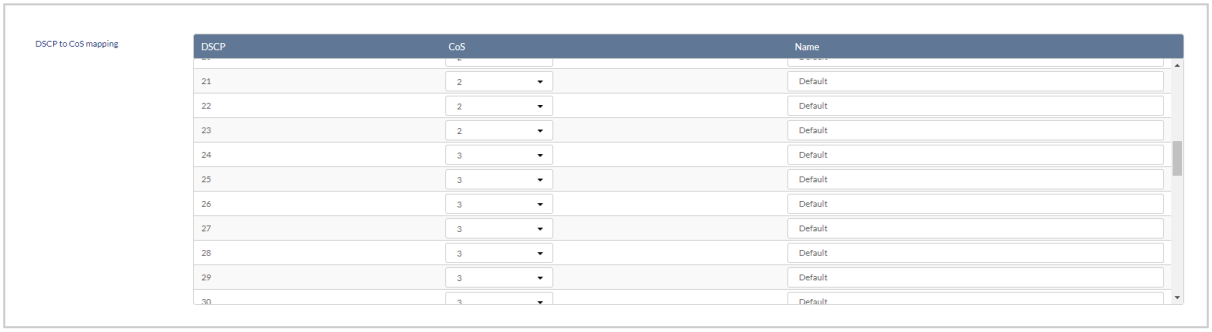
Configuring Quality of Service Settings

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, the overall network performance can be maintained and critical data can be transmitted smoothly.

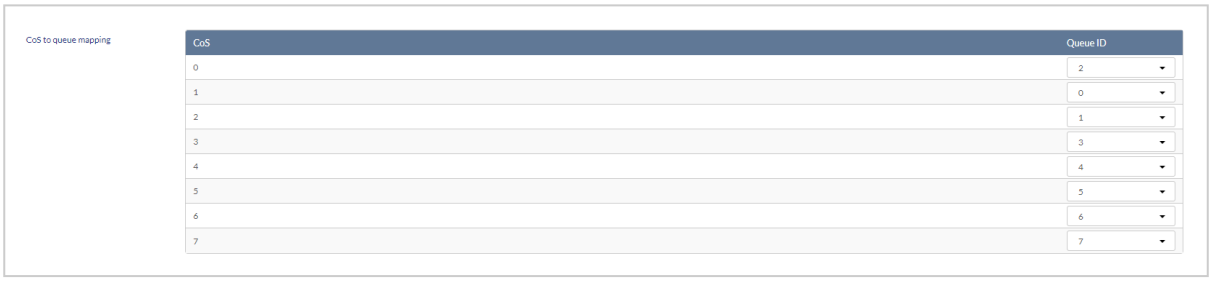
The Quality of Service windows displays the status of Quality of Service priority levels of each port, a higher priority means the traffic from this port will be first handled by the switch. For packets that are untagged, the switch will assign the priority depending on your configuration.

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, select the Trust State. The selection determines the CoS value assignment method. For CoS/802.1p, the CoS will be based on the packet's Queue ID. For DSCP, the CoS will be based on the DSCP value. Configure the mapping between Queue ID and CoS and between CoS and DSCP below for your selection.
5. Select the Scheduling method: SP (Strict Priority) and WRR (Weighted Round Robin. For SP, incoming traffic with the highest priority will be transmitted first. For WRR, the proportion of the incoming packets to be transmitted will be based on the weight of the queue.
6. In the DSCP to CoS Mapping section, 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. Depending on the Scheduling Method, Traffic from ports with assigned CoS values are processed differently.



7. In the CoS to Queue Mapping section, select the Queue ID to for each CoS value (0-7).



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

Configuring SNMP Settings

Simple Network Management Protocol (SNMP) can be enabled to support monitoring and management tasks on the network. Depending on the capabilities of the switch, versions v1, v2c and v3 are supported. Once it is enabled, the switch device can then reply to the SNMP commands and generate trap messages when there are alert events.

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 SNMP section, enable or disable the SNMP.
5. Enter the UDP port for SNMP communication. The default is 161.

6. Enter the SNMP community name. The default is public.
7. Enable or disable the trap state. If enabled, enter the trap receivers' IP addresses. Separate multiple addresses with a comma, space , or semicolon.
8. [Optional] Click Download MIBs to download MIB files. You can view them with a MIB browser.
9. Click **Save**.
10. Click **Push Configuration**.

Configuring 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 addresses.

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 **ACL** tab.
4. In the User Defined IPv4 Rules section, click **Add**.
5. In the Add an IPv4 rule window, specify the following information:

Sequence No.	Enter a sequence number for the ACL for proper positioning of the entry.
Policy	Select an access policy. Permit : 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 UDP header. TCP: The rule only applies to traffic with a 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 destination ports will be evaluated according to the conditions of the rule.
VLAN	Specify the VLAN ID of the traffic. If it is configured as Any, all VLANs will be evaluated according to the conditions of the rule.
Comment	Enter a description for the rule.

6. Click **Add**.
7. Click **Save**.
8. 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 **ACL** tab.
4. In the User Defined IPv4 Rules section, click **Edit** in the Actions column of the rule you wish to edit.
5. Specify the following information:

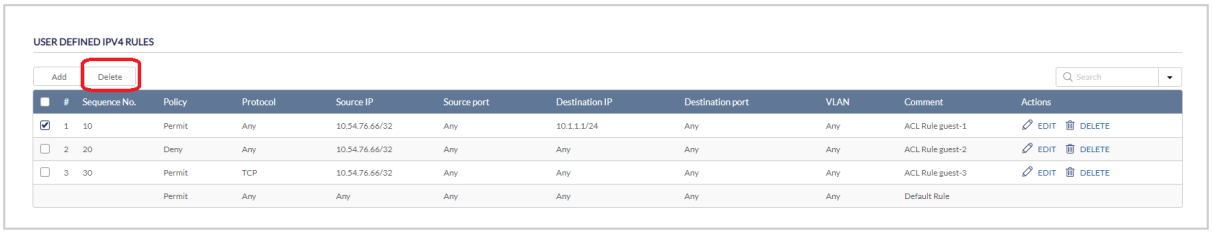
Sequence No.	Enter a sequence number for the ACL for proper positioning of the entry.

Policy	Select an access policy. Permit : 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 UDP header. TCP: The rule only applies to traffic with a 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 destination ports will be evaluated according to the conditions of the rule.
VLAN	Specify the VLAN ID of the traffic. If it is configured as Any, all VLANs will be evaluated according to the conditions of the rule.
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 **ACL** tab.
4. In the User Defined IPv4 Rules section, click the checkbox next to the rule(s) you wish to delete.
5. Click **Delete**.



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

Creating MAC Access Control Policy Rules

Besides ACL filtering according to IP addresses, MAC addresses can also be configured and applied to ACL.

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 **ACL** tab.
4. In the User Defined MAC Rules section, click **Add**.
5. In the Add a MAC ACL window, specify the following information:

Sequence No.	Enter a sequence number for the ACL for proper positioning of the entry.
Policy	Select an access policy. Permit : Traffic with matching parameters will be forwarded. Deny: Traffic with matching parameters will be denied.

Ethernet Type	Enter the Ethernet type using the hex value, for example, 0x0-0xffff. Enter Any for all Ethernet types.
Source MAC	Enter the source MAC address. If the source address is configured as Any, all source traffic will be evaluated according to the conditions of the rule.
Destination MAC	Enter the destination MAC address. If the destination address is configured as Any, all destination traffic will be evaluated according to the conditions of the rule.
CoS	Enter the Class of Service value (0-7). Enter Any if all CoS should be evaluated.
VLAN	Specify the VLAN ID of the traffic. If it is configured as Any, all VLANs will be evaluated according to the conditions of the rule.
Comment	Enter a description for the rule.

6. Click **Save**.
7. 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 Policy** tab.
4. Enter a name for the policy.

5. In the RADIUS servers field, select a pre-configured RADIUS server or click **Add a RADIUS server** to add a new RADIUS server.
6. In the Add RADIUS servers window, specify the following information:

Server Name	Enter a name for the RADIUS server.
IP address	Enter the IP address of the RADIUS server.
Port	Enter a port for the RADIUS server. The range is between 1 and 65535 and default is 1812.
Authentication method	Select an authentication method: Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP), MS-CHAPv2, or Extensible authentication protocol Message-digest algorithm (EAP-MD5) .
Secret	Enter a shared secret.
RADIUS Accounting	Enable or disable RADIUS accounting. Note that this feature depends on the features of the device model.

Note: RADIUS servers can be configured centrally in the Authentication menu. Refer to Authentication for more information.

7. [Optional] Click RADIUS server 2/RADIUS server 3 to add additional RADIUS servers.
8. Select an access policy type:

802.1x port-based	This method requires only one user to be authenticated per port by a remote RDIUS 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 512 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.

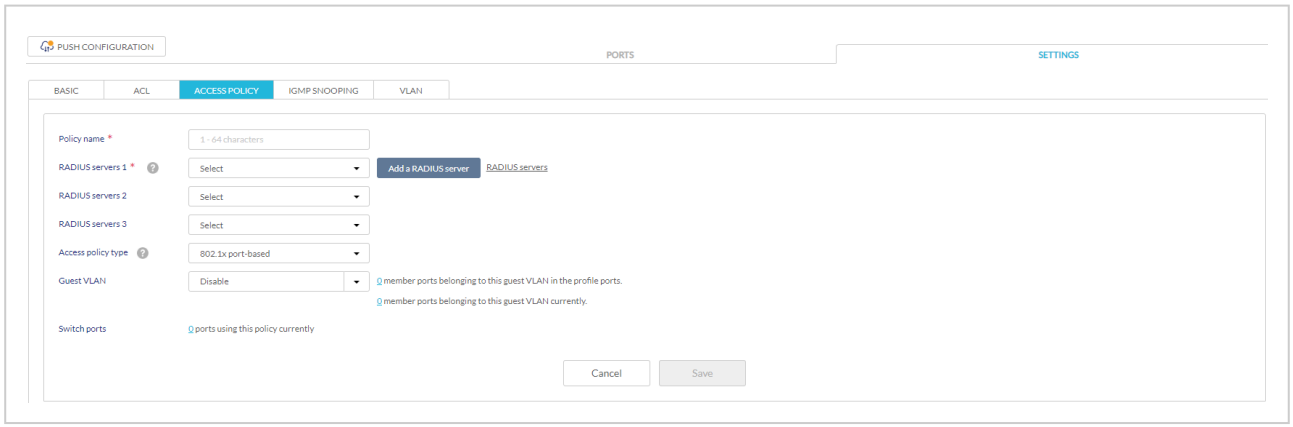
Note: DBS-2000 can support a total number of IPv4 and MAC rules of 512 (go to the ACL tab of the profile setting) and 256 for the total number of users for authentication.

9. [Optional] Select a VLAN ID for guest VLAN from the drop-down menu.
10. Click **Save**.
11. 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 Policy** tab.
4. Select a Guest VLAN from the list.
5. Click **Save**.
6. Click **Push Configuration**.



Configuring Internet Group Management Protocol (IGMP) Snooping

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.

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 **IGMP Snooping** tab.

4. Click **Add** to add a switch to the IGMP snooping list.
5. In the Add IGMP snooping 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	Select an IGMP policy. Enable: The switch will subscribe to and receive multicast traffic. Disable: The switch will not receive multicast traffic.

6. [Optional] Click **Add** to add switches to the IGMP list.
7. Click **Add**.
8. To configure IGMP snooping VLAN settings, click **Add.**

   Enter the following information:

VLAN ID	Assign a VLAN ID for the IGMP VLAN group.
IGMP Snooping	Select an IGMP policy. Enable: The VLAN will subscribe to and receive multicast traffic. Disable: The VLAN will not receive multicast traffic.
Querier state	Enable or disable the Querier state for sending query messages to discover members of a given multicast group.
Multicast filtering mode	Select the filtering mode for multicast: Forward unregistered or Filter unregistered.
Static Mrouter port settings	Select the member ports of the configured VLAN to set as a Static Multicast router (Mrouter) port which connects to a multicast router for forwarding multicast traffic.

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

Viewing Current VLANs on the Switch

The configured VLANs can be viewed in the Profile settings. To obtain the VLAN list, go to **Configure > Switch > Profiles**.

1. Navigate to **Configure > Switch > Profiles**.
2. From the Profile list, click **Settings** under the Actions column of the Profile you wish to view or edit.
3. Click the **VLAN** tab.

The following information is displayed:

VLAN ID	The VLAN ID.
VLAN Type	Shows the VLAN type: Management VLAN, Voice VLAN, or Guest VLAN. If it is not specified, it is regular VLAN.
Tagged member ports/ Untagged member ports	Shows the member ports' VLAN type.
IGMP Snooping Status	Shows the IGMP status for the VLAN. Enabled: The VLAN will subscribe to and receive multicast traffic. Disabled: The VLAN will not receive multicast traffic.

Pushing Configuration Changes

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

Note: Changes made to a Profile's ports 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 the checkbox next to the Profiles you wish to push the configuration to apply it to the associated devices of the configured model.
3. Click **Push Configuration** at the top of the table.

4. Select either Push Configuration Now or Schedule a Configuration Pushing Time to apply the configuration changes at a later time. The schedule will be reflected in the Scheduled Push column of the Profiles list.

   Note: A result window will appear providing a summary of the update status.

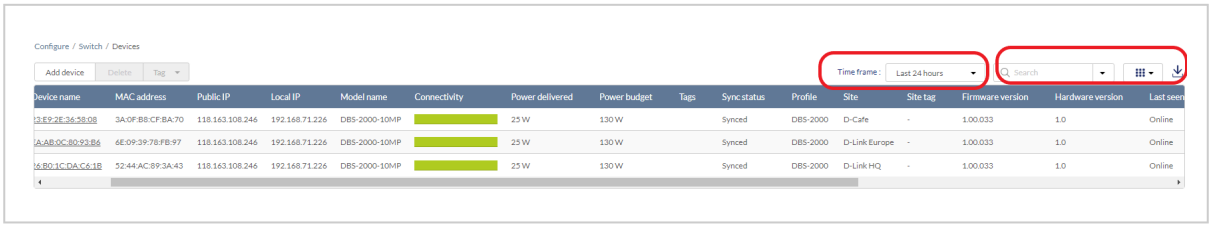
5. In the Push Configuration Result window, click the **X** icon in the top-right to close the window.

Devices

From the Devices page, you can add and register devices and configure individual devices. This page also provides a detailed overview of all currently registered devices with additional information including device status, resource utilization information, and general settings.

Filtering Device Information

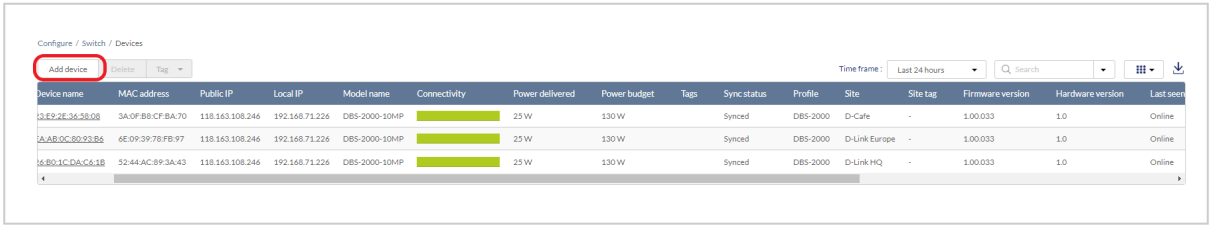
1. Navigate to **Configure > Switch > Devices.**
2. [Optional] Select a time frame from the drop-down menu.
3. Click the filter selection in the top-right.



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.

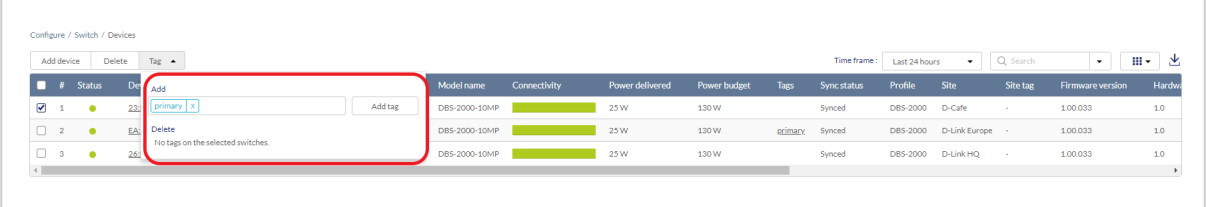
	The UID may be listed in the format **XXXX-XXXX-XXXX** or **XXXXXXXXXXXX**. When entering the UID, do not include dashes.
Device name	Enter a name for the device.
Site	Select a Site to link this device to.
Profile	Select a Profile for this device. The device will use the settings configured in that profile.
Add more Licenses	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**.

Adding a Tag to One or More Devices

You 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 > Devices**.
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 Tag**.

Editing a Device

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

Deleting Devices

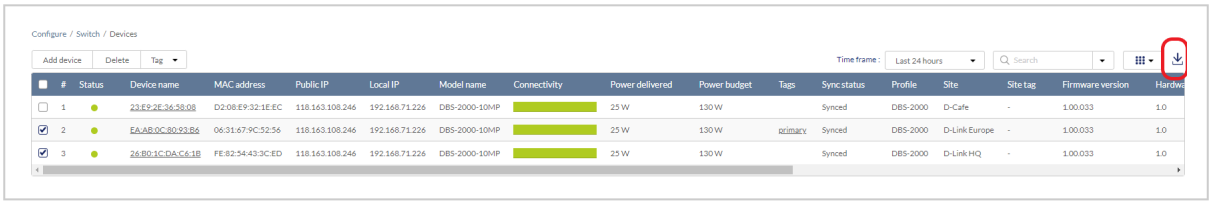
Assigned devices can be unassigned and remain in the device inventory so they can be reassigned at a later point.

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. You will be asked whether you would like to delete the device permanently or move it to the inventory.

Downloading 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
Delete
Tag
Time frame :
Last 24 hours
Search
Status Device name MAC address Public IP Local IP Model name Connectivity Power delivered Power budget Tags Sync status Profile Site Site tag Firmware version Hardwa
1 23:E9:2E:36:58:08 D2:08:E9:32:1E:EC 118.163.108.246 192.168.71.226 DBS-2000-10MP 25 W 130 W Synced DBS-2000 D-Cafe - 1.00.033 1.0
2 FA:AB:0C:80:93:B6 06:31:67:9C:52:56 118.163.108.246 192.168.71.226 DBS-2000-10MP 25 W 130 W primary Synced DBS-2000 D-Link Europe - 1.00.033 1.0
3 26:B0:1C:DA:C6:1B FE:82:54:43:3C:ED 118.163.108.246 192.168.71.226 DBS-2000-10MP 25 W 130 W Synced DBS-2000 D-Link HQ - 1.00.033 1.0

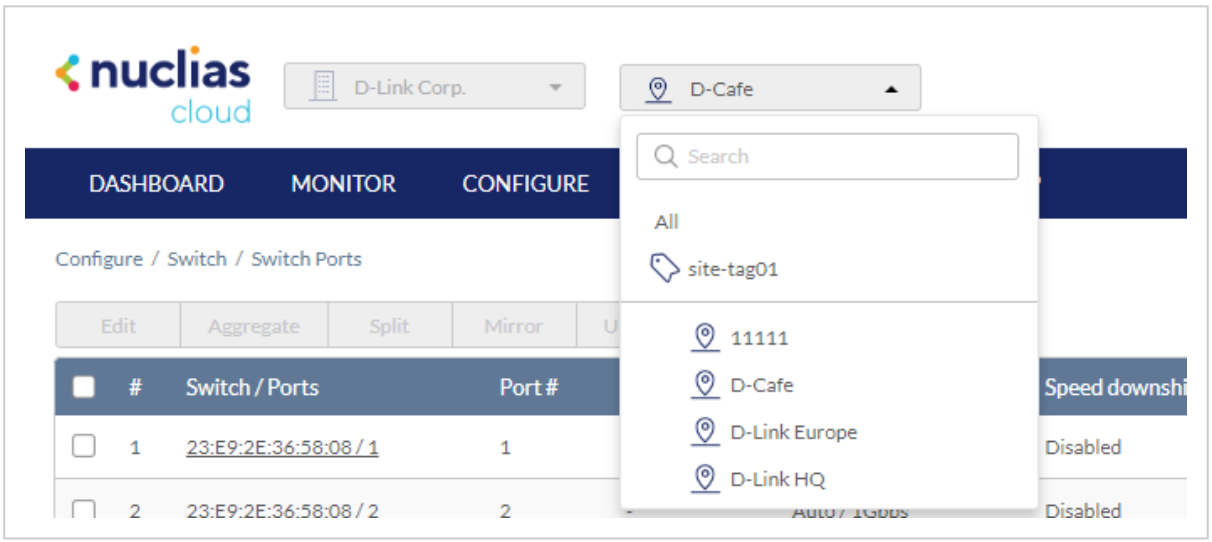
Switch Ports

From the Switch Ports section, you 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.

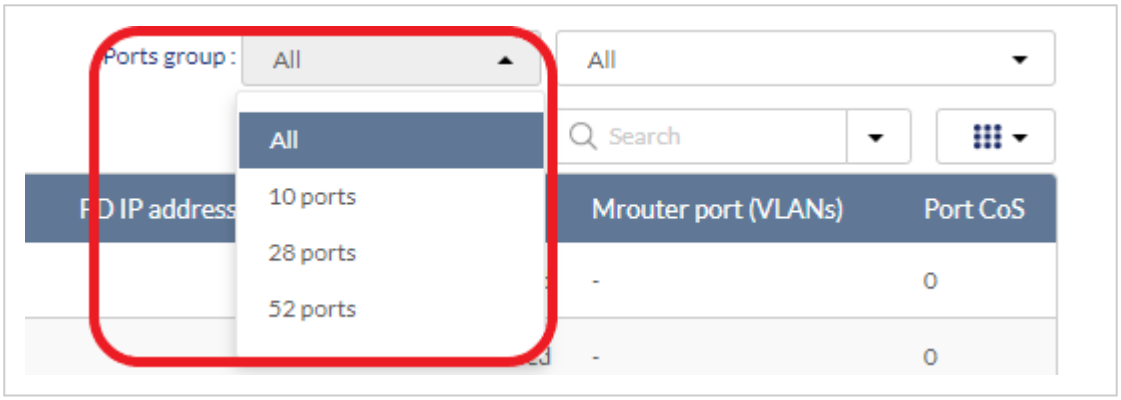
Local switch configurations may be useful in cases where one switch in a group of switches requires specialized settings that are not configured in the associated Profile to accommodate a specific application.

Customizing the Switch Ports Configuration Overview

1. Navigate to **Configure > Switch > Switch Ports**.s
2. Select the desired site from the site drop-down menu.



3. 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.



4. From the port list, check the box next to the ports you wish to edit.
5. Click **Edit**.
6. 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.

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 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. **Note**: RSTP cannot be used in conjunction with LBD.

	Note: 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. Note: LBD cannot be used in conjunction with RSTP.
Port CoS	Assign a Class of Service value for the port (0-7).
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 if the Trunk type is selected.
Allowed VLANs	Enter the IDs of the VLANs that can route traffic through this port if the Trunk type is selected. Enter **All** to allow all traffic from all VLANs to pass through this port.
Access VLAN	Enter the ID of the VLAN the port belongs to if the Access type is selected.
Access Policy	Select the Access Policy for this port if the Access type is selected. The options include Disabled, MAC Whitelist, Port

	Security Delete-on-Time Mode, and Port Security Permanent Mode.
Static Whitelisted MACs	Enter the MAC addresses that can access this port to restrict access to this port to devices with specific MAC addresses. If entering multiple MAC addresses, enter only one address per line.
Dynamic Whitelist Size Limit	Enter the maximum number of allowed MAC addresses that the device should learn dynamically for the Port Security Delete-on-time Mode or Port Security Permanent Mode.
Dynamic Whitelisted MACs	Display the learned MAC addresses for the Port Security Delete-on-time mode and Port Security Permanent Mode.
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.
Link (SFP)	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.
Speed downshift	Enables/disables automatic speed downshift on the supported interface when the designated maximum speed cannot be established.
PoE	Choose to enable or disable Power over Ethernet (PoE) functionality on this port.

	Note: The PoE setting will only apply to ports that support Power over Ethernet.
PD Alive	Enable or disable the automatic detection of the Powered Devices status.
PD IP address	Enter the IP address of the Powered Device.
Port Schedule	Choose a port schedule. Port schedules are separately configured. Refer to the Schedule Policies section.
Traffic segmentation	Enable or disable traffic segmentation on this port to further restrict traffic flow in your network. If enabled, select the forward ports.
Forward Ports	Select the forward ports if traffic segmentation is enabled.
Flow control	Enable or disable the flow control on the port to regulate the data transfer rate between two devices.

5. Click **Apply**. The **details** link next to the Switch/Ports will direct you to the Port Information page. You can view detailed information such as packets sent/received and configuration status.

Aggregating Switch Ports

Port aggregation allows you 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 you 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”.

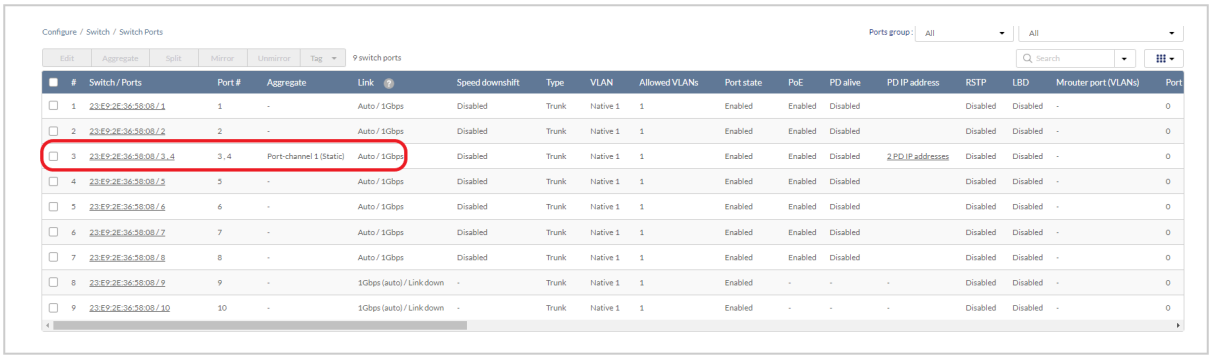
Note: These local settings will override any conflicting Profile settings associated with the device.

1. Navigate to **Configure > Switch > Switch Ports**.
2. From the port list, check the box next to the ports you wish to link together.
3. Click **Aggregate**.
4. In the Link Aggregation Setting window, select the aggregation type.

1. LACP
2. Static

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.

5. Click **Aggregate**.
   Note: Aggregated ports can be identified by the combined port number in the Port # and Aggregate column of the port list.



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. **Note**: The port number should be in numerical format, for example 28.

5. Click **Create port mirror**.

Undoing Port Traffic Mirroring

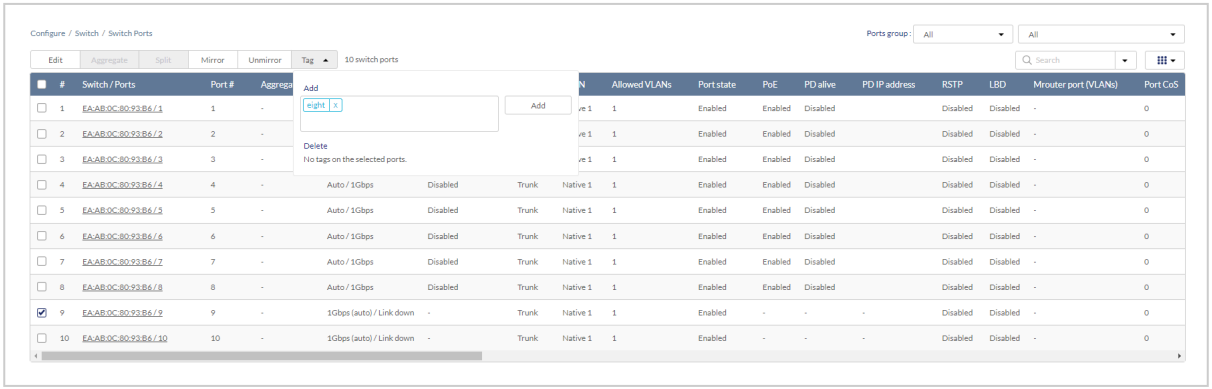
1. Navigate to **Configure > Switch > Switch Ports**.
2. From the port list, check the box next to the mirrored port(s) you wish to unmirror.
3. Click **Unmirror**.
   Note: This will immediately undo the selected mirrored ports.
4. Click **Delete port mirror**.

Adding a Tag to One or More Switch Ports

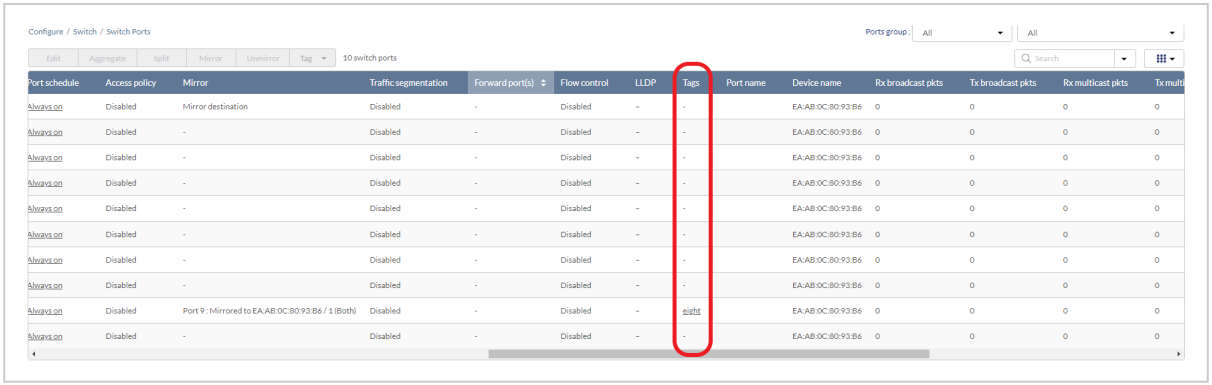
You can add descriptive tag to ports to identify and filter different ports or groups of ports. Tags are purely informational and do not affect the functionality of the port.

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**.

Configure - Gateway

Configure - Gateway

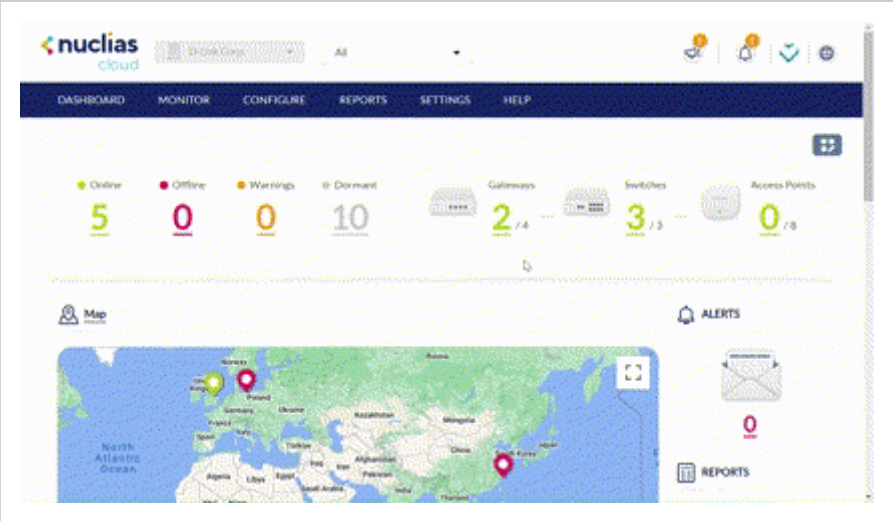
From the Configure section, you can manage profiles and devices for organizations. Profiles can be created to tailor configuration requirements to specific gateway models.

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

Profiles	From the Profiles section, you can create new and edit existing profiles and apply profile configuration settings to devices according to a schedule.
Devices	From the Devices section, you can add devices with Site and Profile information and configure individual devices.

Profiles

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.



Creating a Profile

After a profile is created, you can configure network routing rules and security features within each profile.

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

1. Navigate to **Configure > Gateway > 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. Select the Access Level for the accessibility level of the profile under the Organization, Site tag, or Site.
5. [Optional] Select **Clone from existing profile** and choose a Profile from the drop-down menu to clone an existing Profile. Or select **Use default configuration** to apply the default configurations. The page provides modification options to let you modify configurations later.
6. Click **Create Profile**.

Deleting Profiles

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

2. From the Profile list, click the checkbox next to the Profiles you wish to delete.
3. Click **Delete profile** at the top of the table.
4. When prompted to confirm, click **Yes**.

Pushing Configuration Changes

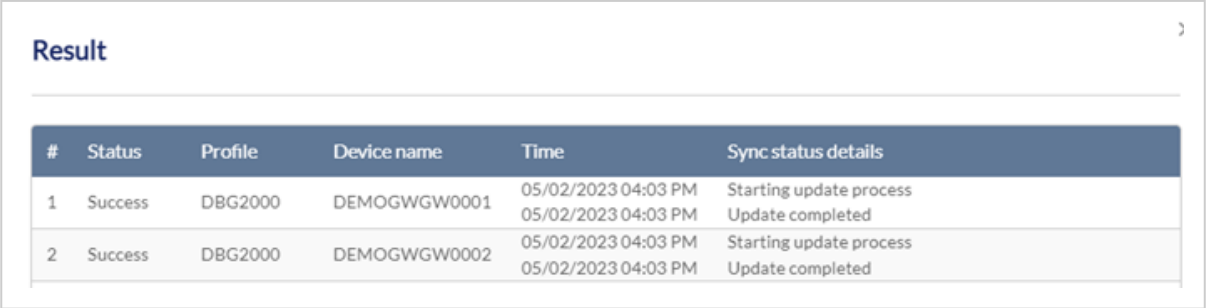
The Push Configuration function allows you to quickly apply Profile configuration changes to all devices using this Profile.

Note: Changes made to a Profile's settings will be pushed to all associated devices after the user selects Push Configuration.

1. Navigate to **Configure > Gateway > Profiles**.
2. From the Profile list, click the checkbox next to the Profiles you wish to push the configuration to apply it to the associated devices of the configured model.
3. Click **Push Configuration** at the top of the table.



4. Select either Push Configuration Now or Schedule a Configuration Pushing Time to apply the configuration changes at a later time. The schedule will be reflected in the Scheduled Push column of the Profiles list.
5. The **Result** windows appears to display the push configuration status, affected profiles and devices, time of the configuration change, and details about the update process.



Configuring Network Settings

From the Network window, you can configure basic port settings and advanced settings for routing and traffic management.

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

2. From the Profile list, click **Network** under the Actions column of the Profile you wish to edit.

   To configure a port's basic settings:

3. Select the **Network** tab at the top. The LAN ports of the device are displayed along with their information shown in the table below.
   Note: The Profile can only be used for the selected device model type.
4. Under **Port Configuration**, select a port and click **EDIT** under Actions.

   Specify the following information for the selected LAN port:

Interface Type	Select the connection type: LAN or DMZ.
Interface Name	Enter a name to identify this interface.
Bridge Network	Enable or disable bridging with another network. Configure the interface with more settings below if bridging is not enabled.
IP Address/Subnet Mask	Enter an IP address with subnet mask.
DHCP mode	Enable or disable DHCP service for IP address assignment.
DHCP server	Enter the following information if DHCP server is selected. Domain name: Assign a domain name for DHCP service. Starting IP address/Ending IP address: Enter the range of IP addresses that can be assigned dynamically. Default gateway: Assign a default gateway for DHCP service. DNS server: Configure DNS by specifying a static DNS server, DNS setting from the ISP, or using DNS proxy. For static DNS, enter the DNS servers or WIN server IP address. Lease Time: Enter a time value of 1 to 10080 minutes.

Allow ping from LAN/ DMZ	Enable or disable ping command executed from this port.
DHCP Relay	Enter the remote DHCP server address if DHCP relay is selected.
DNS proxy	Enable or disable DNS proxy.

For a WAN port (if the device supports this feature), configure the following:

Interface Type	Select the WAN interface for configuration.
Connection Type	Select the connection method: DHCP, Static IP, PPPoE, PPTP, L2TP, DS-Lite/IPIP, or MAP-E. For Static IP, enter the IP address/Subnet mask, Gateway IP address and Primary/ Secondary DNS servers, and specify whether to keep the original MAC address as well as the MTU size. For PPPoE, select the Address mode: Dynamic IP or Static IP. For static IP, enter the IP address/Subnet mask and PPPoE connection Username and Password. Then specify the Authentication type from one of the following: None, MS-CHAPv2, MS-CHAP, CHAP, PAP, or Auto-negotiate. For Dynamic IP, you don't need to enter the IP address/subnet information but configure all other settings as specified above. For both addressing modes, enter the Service name (optional) and select the Reconnect mode: Always on, or On demand (enter the Maximum idle time to wait before terminating the connection in minutes for this option). Then configure the DNS servers and specify whether to keep the original MAC address as well as the MTU size. For PPTP, if Static IP is selected, enter the following IP address information: IP address/Subnet mask, Gateway IP address, and Static DNS IP address. For both Address modes, enter the PPTP server name and connection Username and Password. For both modes, configure whether MPPE (Microsoft Point-to-Point Encryption (MPPE) will be used and the Reconnect mode: Always on or On demand (enter the Maximum idle time to wait before terminating the connection in minutes for this option). Then configure the DNS servers and specify

	whether to keep the original MAC address as well as the MTU size. For L2TP, if Static IP is selected, enter the following IP address information: IP address/Subnet mask, Gateway IP address, and Static DNS IP address. For both Address modes, enter the L2TP server name and connection Username and Password. For both modes, enter the Secret (optional) and configure the Reconnect mode: Always on or On demand (enter the Maximum idle time to wait before terminating the connection in minutes for this option). Then configure the DNS servers and specify whether to keep the original MAC address as well as the MTU size. For DS-Lite/IPIP, select the Service Provider and Address Family Transition Router (AFTR) Addressing method. For MAP-E, select the Service Provider. **Note:** Service providers are only available in specific countries.
Advanced Settings	Enable or disable the following passthroughs: **Internet Protocol Security (IPsec)** which is used for securing packets exchange at the IP layer. **Point-to-Point Tunneling Protocol (PPTP)** which is used for tunneling the Point-to-Point Protocol (PPP) communication in an IP network. **Layer 2 Tunneling Protocol (L2TP)** which is used for implementing Point-to-Point sessions utilizing multipoint tunneling technique.

5. Click **Push Configuration** at the top left to apply the settings to the affected devices immediately.

Configuring the Default WAN Configuration

Note: The availability of the WAN Mode Configuration depends on device model.

1. Navigate to **Configure > Gateway > Profiles**.
2. From the Profile list, click **Network** under the Actions column of the Profile you wish to edit.
3. Under **Default WAN Configuration**, select IPv4 and IPv6 default WAN port. Note that the settings or configurations here depend on the device model and firmware.
4. Under **WAN Mode,** select a WAN mode from the available options. For **Auto-rollover using WAN**, select both Primary and Secondary WAN ports as well as the **Health Check**

method. If DNS servers or Ping IP address method is selected, enter the respective server IP address as the destination to check the connectivity. Also enter the **Retry interval** (seconds) and **Failover after** (number of failed retries).

5. For Load balancing, select the method (either Round robin or Spillover mode). For **Round robin**, configure the Health check method (or none) and enter the **Retry interval** (seconds) and **Failover after** (number of failed retries). Hence, if a WAN interface disconnects, only the alternate WAN ports will transfer traffic flows in a round robin manner. For **Spillover**, enter the **Load tolerance** (%) and **Max bandwidth** (Mbps) as the threshold value. Once the threshold is exceeded for a WAN port, new traffic flows will be allocated to the alternate WAN interfaces. The precedence for selection is based on the configuration of Primary, Secondary, and Tertiary WAN interface.
6. Click **Push Configuration** at the top left to apply the settings to the affected devices immediately.

Configuring Wireless Settings

You can create multiple SSIDs under a single Profile and configure each SSID with unique settings to accommodate different wireless usage scenarios. Note that this feature is only available on supported models.
To create an SSID:

1. Navigate to **Configure > Gateway > Profiles**.
2. From the Profile list, click **Network** under the Actions column of the Profile you wish to edit.
3. Select **Wireless.**
4. Under **SSID**, click **Add** to add a new SSID profile setting. Enter the following information:

SSID Name	Enter a name for the SSID (1-32 characters).
Band Selection	Select the radio frequency to be used for the SSID configuration: 2.4GHz and/or 5GHz.

3. Click **Edit** under Actions to modify an SSID profile setting. Enter the following information:

SSID Name	Enter a name for the SSID (1-32 characters).
Security	Select the security mode: Open: Select this option for an unsecured network.

	Enhanced open: This method provides protection based on opportunistic wireless encryption (OWE) and open authentication. Enhanced Open+Open: This method provides transition from an open to Enhanced Open wireless environment. WPA2: The Wi-Fi Protected Access II (WPA2) security protocol requires users to enter an alphanumeric passphrase or the information of a RADIUS server. WPA/WPA2: This method allows both WPA and WPA2 clients to connect. WPA3: WPA3 is the strongest encryption method among WPA standards. WPA2/WPA3: This method allows both WPA2 and WPA3 clients to connect.
Authentication method	Select the respective authentication method for the security type selected above. If a RADIUS server is used in your network environment, enter the RADIUS server information (refer to Authentication Servers) as well as the Group key update interval and the encryption method.
MAC Filtering	Enable or disable MAC Filtering and select the desired filtering mechanism: MAC ACLs or RADIUS server. If MAC ACLs is selected, specify whether it is a Allow or Deny rule. For information on managing MAC ACLs, refer to MAC ACLs. If RADIUS server is selected, enter the RADIUS server information (refer to Authentication Servers).
Broadcast SSID	Enable or disable the visibility of the SSID.
Band Selection	Select the available radio frequencies that the device supports and enable or disable band steering which automatically connects newer devices to the higher frequency band available.
Guest Access Mode	Enable or disable guest access function.

Station Isolation	Enable or disable isolation of stations within the SSID so that wireless clients will not be able to communicate with each other.
NAS-IP-address (optional)	Enable the network access server IP address to let RADIUS server to choose an access policy for a connection request.
Bridge to Interface	Bridge this wireless network to a LAN/VLAN interface.
Schedule Policy	Select a pre-defined schedule policy to designate a time frame to make the configuration effective. To view all available schedule policies, go to **Configure > Schedule policies**. To add a new schedule policy, click **Add schedule policy** (refer to Schedule Policies for more information).

4. Click **Next** to configure more settings:

Max Client	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 Multicast 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	Limit the packet size for wireless packets transmitted in the network.
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.
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.
Weak RSSI Client Associations Attempts	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.

5. Under **Radio**, configure the following information for each available radio frequency:

Radio	Enable or disable this radio frequency.
Radio Mode	Select the 802.11 mode.
Channel Bandwidth	Select the channel bandwidth. The availability of channel width depends on the selected 802.11 mode.
Tx Power	Enter the transmission power.
Auto Channel	Enable or disable auto channel. If disabled, select the channel number.
Eligible Channels	Select channels to be operable under the Auto channel mode.
Force Auto Channel Scan	Enable or disable automatic channel scan.
Auto Channel Interval	Specify the time interval for auto channel scan.
Beacon Interval	Enter the interval between beacon transmissions in milliseconds (40-3500).
DTIM Interval	Specify the delivery traffic indication map interval (1-255). A larger interval sets a longer idle power time for the client devices.
Short Guard Interval	Enable Short guard interval to decrease the time between data characters to avoid propagation delays and reflections.
U-APSD	Unscheduled Automatic Power Save Delivery is a power-saving mechanism designed for latency sensitive traffic.
SSID Isolation	Enable or disable isolation among different SSIDs.

6. Click **Push Configuration** at the top-left to apply the settings to the affected devices immediately.

Configuring Addressing

Configuring VLANs

VLANs allow you to divide the network to different segments on your local network.

To configure a VLAN:

1. Navigate to **Configure > Gateway > Profiles**.
2. From the Profile list, click **Network** under the Actions column of the Profile you wish to edit.
3. Select **Addressing.**
4. Under **VLAN**, click **Add** to add a new VLAN. Enter the following information:

Name	Enter a name for this VLAN.
VLAN ID	Assign a VLAN ID (2-4094).
Untagged Ports	Select the member ports to be untagged.
Tagged Ports	Select the member ports to be tagged.
Bridge to Interface	Select a VLAN to create a network bridge to a VPN configuration. Note that since an SSID can be configured to bridge with a VLAN, the connectivity of a wireless network of an associated SSID will be affected once this setting has been changed.
InterVLAN	Enable or disable inter-VLAN routing.
VLAN Subnet	Enter the VLAN IP address and subnet mask to define the VLAN subnet.

DHCP Mode	Enable or disable DHCP service for IP address assignment and select the mode for DHCP.
DHCP Server	Enter the following information if DHCP server is selected. Domain name: Assign a domain name for DHCP service. Starting IP address/Ending IP address: Enter the range of IP addresses that can be assigned dynamically. Default gateway: Assign a default gateway for DHCP service. DNS server: For static DNS Server assignment, enter the IP address of a primary and (optional) secondary DNS server. WINs server: Enter the Windows Internet Naming Service (WINS) server if it is used. Lease Time: Enter a time value of 1 to 10080 minutes.
DHCP Relay Server	Enter the remote DHCP server address if DHCP relay is selected.
DNS Proxy	Enable or disable DNS proxy for this VLAN.
DHCPv6 Mode	Select the DHCPv6 mode: Disabled, Relay or Server (note not all models support IPv6 configuration). For server mode, specify the IPv6 assignment below.
RA Mode	Select the Router Advertisement mode for DHCPv6: Relay or Server. For server mode, specify the IPv6 assignment below.
IPv6 Assignment	If IPv6 assignment is enabled, enter the following: IPv6 assignment prefix length: enter a number between 1 and 128. IPv6 assignment hint: enter a hint message for the assignment. IPv6 suffix: select the suffix assignment method: EUI-64, Random, or Manual. For Manual, enter an IPv6 suffix to be assigned. If IPv6 assignment is disabled, enter an IPv6 address.

IPv6 Autoconfiguration Service	Select the IPv6 Autoconfiguration method: SLAAC (Stateless Address Autoconfiguration) +Stateless DHCPv6, DHCPv6 (Stateful), SLAAC+RDNSS (Recursive DNS Server), or Disable.
NDP-Proxy	Enable or disable Neighbor Discovery Protocol (NDP) proxy to enable the proxy function which will respond upon receiving NDP messages.
Captive Portal	Enable or disable Captive portal for connection control of this VLAN. Then assign a Captive portal page to it.
Allow Ping from LAN	Enable or disable the transmitting the ping command from this VLAN.

5. Click **Save**.
6. Click **Push Configuration** at the top left to apply the settings to the affected devices immediately.

IP Management List

The IP Management allows static DHCP assignment.

To configure IP management for DHCP clients:

1. Navigate to **Configure > Gateway > Profiles**.
2. From the Profile list, click **Network** under the Actions column of the Profile you wish to edit.
3. Select **Addressing.**
4. Under IP Management List, click **Add** to add a new IP assignment. Enter the following information:

Host Name	Enter the host name of the client device.
Interface	Select the interface associated with the DHCP IP assignment.
IP Address	Assign an IP address to the host.

MAC Address	The MAC address of the host.
IPv6 suffix	[optional] Assign an IPv6 suffix for IPv6 addressing for the last 8 hexadecimal characters.
IP / MAC Binding	Enable or disable the binding of the IP and MAC address so that the device with the specified MAC address cannot use any other IP address to access the network.
DHCP IP Reservation	Enable or disable the reservation of this DHCP IP lease for the client with the specified MAC address. It ensures that the same IP address is assigned to the designated client whenever the client connects to the network.

Note: You can add an entry to the static DHCP assignment without enabling either IP / MAC binding or DHCP IP reservation; in this case, it will only be a reference assignment.

5. Click **Push Configuration** at the top left to apply the settings to the affected devices immediately.

Configuring Routing

Routing determines the path for packet delivery in a network. The routing capabilities vary depending on the device model.

Configuring Static Route

Static Routing is a fixed pathway that packets will take when there is no automatic route updating mechanism in the current network topology.

To configure a static route:

1. Navigate to **Configure > Gateway > Profiles**.
2. From the Profile list, click **Network** under the Actions column of the Profile you wish to edit.
3. Select **Routing**. Under Static Route, click **Add** to add a new route. Enter the following information:

Name	Enter a name for this route

Destination	Enter the destination subnetwork IP address.
Subnet mask	Enter the subnet mask of the destination address.
Gateway	Enter the IP address of the gateway or next hop.
Interface	Select the interface through which the route is accessible.
Metric	Enter the number of hub count (range: 2-15).
Private	Enable the private option to disallow sharing of this route with other routers.

4. Click **Push Configuration** at the top left to apply the settings to the affected devices immediately.

Configuring Policy Route

Policy Route designates a specific type of traffic to a particular WAN link to meet the desired quality of service. It is only applicable when dual WAN mode is supported on the device. Note that the IPv6 Policy Route is only available for supported models.

To configure Policy Route:

1. Select a Profile for the desired Gateway model.
2. Select **Network > Routing**.
3. Under Policy Route, click **Add** to add a new route. Enter the following information:

Name	Enter a name for this route.
Local Gateway	Select the port of the device that the route should use for policy routing.

Protocol	Select the protocol that will use this route.
Source interface	Select the source interface.
Source Network	Enter a single IP address or a range of IP addresses using "-", for example, 192.168.200.101-192.168.200.188. Enter "any" for all source IP addresses. For IPv6, enter xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, where x is a hexadecimal digit. You can also use CIDR notation, for example, a.b.c.d/n for IPv4 and xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/n, where n represents the subnet prefix length.
Destination Interface	Select the destination interface.
Destination Network	Enter a single IP address or a range of IP addresses using "-", for example, 192.168.200.101-192.168.200.188. Enter "any" for all source IP addresses. For IPv6, enter xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, where x is a hexadecimal digit. You can also use CIDR notation, for example, a.b.c.d/n for IPv4 and xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/n, where n represents the subnet prefix length.
Source Port	Enter the port number used for this type of traffic (Range: 1-65535). Enter a single port or a range of ports using "," or "-", for example, 3000,3001 (do not include space) or 3000-3200. Enter "any" for all source ports for this service.
Destination Port	Enter the port number used for this type of traffic (Range: 1-65535). Enter a single port or a range of ports using "," or "-", for example, 3000,3001 (do not include space) or 3000-3200. Enter "any" for all destination ports for this service.

4. Click **Push Configuration** at the top left to apply the settings to the affected devices immediately.

Configuring RIP

Routing Information Protocol (RIP) utilizes distance vector as the metric for routing packets in local networks. It has two versions: RIP version 1 and RIP version 2. RIP version 1 is classful whereas RIP version 2 is classless. And only RIP version 2 uses authentication.

To configure RIP:

1. Select a Profile for the desired Gateway model.
2. Select **Network > Routing**.
3. Under RIP Configuration, click **Add** to add a new route. Enter the following information:

Interface	Select the port of the device to allow RIP information to be exchanged.
Direction	Select the either inbound, outbound, or traffic for both directions should use this route.
Version	Select the protocol version on which routing information should be exchanged.
Authentication	Enable or disable authentication of RIP packets. This is not available for RIP-1. If it is enabled, enter the following information: MD5 (challenge-response authentication) Key ID (1-255) and Authentication Key (16 characters maximum).

4. Click **Push Configuration** at the top left to apply the settings to the affected devices immediately.

Configuring OSPFv2

Open Shortest Path First (OSPF) is a link-state routing protocol that learns about neighbor routers specified by OSPF parameters through LSA.

To configure OSPFv2:

1. Select a Profile for the desired Gateway model.
2. Select **Network > Routing**.
3. Under OSPFv2 Configuration, click **Add** to add a new route. Enter the following information:

Interface	Select an interface to be assigned to the area defined below.
NSSA	Enable or disable the not-so-stubby area (NSSA) which can import external route information.
Area	Assign an OSPF area ID.
Priority	Assign a priority which helps determine the OSPF designated router.
Hello Interval	Specify the length of time between each hello packet (1-65535 seconds).
Dead Interval	Set the time (1-65535 seconds) the device must wait before it declares a neighbor OSPF router down when a hello packet has not been received.
Cost	The cost of the OSPF path (1-65535) which helps determine the best path.
Authentication	Enable or disable the authentication of OSPF packets. Authentication type: Simple or MD5. If MD5 is used, enter the Key ID (1-255) and Authentication Key (16 characters maximum).
LAN Route Exchange	Enable or disable the exchange of LAN routing table through OSPF.
Active	Enable or disable this OSPF configuration.

4. Click **Push Configuration** at the top left to apply the settings to the affected devices immediately.

Enabling Services

Supported services can be configured individually depending on the features of the gateway.

First, Select a Profile for the desired Gateway model.

Then, enable or disable the following features:

IGMP Snooping	Enable or disable IGMP Snooping. This allows the device to listen on IGMP conversations on the network and maintain the multicast forwarding table to ensure that traffic is sent only to member devices.
IGMP Proxy	IGMP proxy allows the device to receive IGMP membership requests from the hosts on the LAN and issue IGMP messages on behalf of these hosts.
Jumbo Frame	Jumbo Frame allows the device to process frames larger than the standard Ethernet frame and can maximize server-to-server performance.
RTSP	Allows applications that uses Real Time Streaming Protocol (RTSP) to receive streaming media from the Internet
UPnP	UPnP allows network devices such as PCs, gateways, and APs to discover each other and communicate.
SIP	Session Initiation Protocol (SIP) allows devices and applications using VoIP (Voice over IP) to communicate.
H.323	H.323 also allows IP telephony. However, it differs from SIP in many ways such as encoding, reliability, and extended support for file sharing and other applications.
TFTP	Trivial File Transfer Protocol (TFTP) is a simple protocol for file transfer without authentication mechanism.
SMTP	Simple Mail Transfer Protocol (SMTP) is a protocol for email transmission.

Managing Traffic Policies

The Traffic Management provides control over traffic of certain types by setting limits on bandwidth and session. Note that this function depends on the capability of the gateway.

To configure Traffic Shaping:

1. Select a Profile for the desired Gateway model.
2. Select **Network > Traffic Management**.

   Under Traffic Shaping, click **Add** to add a new rule. Enter the following:

Name	Enter a name for this policy.
Policy Type	Specify the traffic policy should be applied to inbound or outbound traffic.
WAN Interface	Select the WAN port that this policy should be applied to.
Management Type	Select the metric to define the policy: Rate or Priority. Configure the following if Priority is selected: Low, Medium, or High. Higher priority means the traffic will be allocated with more bandwidth. If Rate is selected, enter the maximum bandwidth and minimum bandwidth.
Service	Select the type of traffic based on the protocol or application service.
Traffic Selector Match Type	Select the criteria to which the policy should be applied: IP address, MAC address, or Interface and enter an IP address or a MAC address or select a LAN interface respectively. Only the IP address match type can be used for managing inbound traffic.
Schedule Policy	Select the schedule policy to make the policy effective during the designated time frame. Go to **Configure > Schedule** policies for information about configured schedules.

3. Click **Save**to save the settings.

To configure Session Limiting:

1. Under Session Limiting, click **Add** to add a new rule. Enter the following:

Name	Enter a name for this policy.
Source Type	Select the criteria to which the policy should be applied: IP address, IP range, or Interface. Enter an IP address or a range of IP addresses or select a LAN interface respectively.
Maximum Sessions	The maximum number of concurrent sessions for the specified traffic flow (1-999).
Schedule Policy	Select the schedule policy to make the policy effective during the designated time frame. Go to **Configure > Schedule** policies for information about configured schedules.

2. Click **Save**

You can also configure a warning page to display related messages when the maximum session has been reached.

To configure a warning page:

1. Under Custom Warning Page, click **Add** to add a new warning page. Enter the following:

Name	Enter a name for this configuration.
Warning page	Select one of the pre-defined warning page to be displayed. Go to **Configure > Splash pages** for information about configured splash pages.

2. Click **Push Configuration**at the top left to apply the settings to the affected devices immediately.

Configuring SSID Captive Portal Settings

The captive portal displays a splash page to wireless users which requires them to agree to terms and conditions to use Internet services.

To configure Captive Portal:

1. Select a Profile for the desired Gateway model.
2. Select **Network > Captive Portal**.
3. Under Captive Portal, click **Add**. Enter the following:

Name	Enter a name for this profile.
User Authentication	Specify the authentication method for the users: None: No signing-on method required. Click-through: Sign on by simply clicking to agree the terms. Sign-on with basic login page: Sign on using a login page Sign-on with third-party credentials: Sign on using account access from a third-party app or service. Sign-on with basic login and third-party credentials: Sign on using a login page or account access from a third-party app or service Sign on with e-mail authentication, SMS authentication and third-party credentials: Sign on with email account verification, short message authentication or third-party credentials. Sign-on with external captive portal: Sign on using an external captive portal. Sign-on with Facebook Wi-Fi: Sign on through a designated Facebook page that requires users to check in. After an authentication is selected, configure the Splash page accordingly by clicking Splash page editor. On the Splash page editor screen, you can configure the header, footer, terms of use text, etc. Alternatively, select a pre-defined Splash page from the drop-down list that is customized for the selected authentication type.
Splash Page	Enter the splash page which a wireless user must visit prior to using Internet services. The design of the page depends on the use case.
Splash Page URL	Enter the URL of a splash page if using an external captive portal.

Email Authentication	For email authentication, enter the following: Grace period: The time period in minutes for email verification. Authentication times: The number of email authentication that a user can request in one day. Denial period limit: The time period to wait for another request of email authentication if the previous verification fails. SMS configuration: SMS text messages for authentication requires Twilio SMS account settings. Click Add Twilio SMS settings to add your account information or select one pre-defined SMS configuration from the drop-down menu.
SMS configuration	SMS text messages for authentication requires Twilio SMS account settings. Click Add Twilio SMS settings to add your account information or select one pre-defined SMS configuration from the drop-down menu. Refer to SMS_Configuration in Advanced Settings.
Local Authentication	For basic login page, select a local authentication database or click Add authentication users to create a new Local Authentication database.
3rd party Credentials	Select the third-party credential to be used for login.
Authentication Server	For basic login page, select a pre-configured server in accordance with the existing authentication system or click Add a RADIUS/LDAP/AD/NT Domain server to configure a new server. You can select the primary and backup servers. Refer to Authentication for more information.
RADIUS Server	For external captive portal, select a pre-configured RADIUS server in accordance with the existing authentication system or click Add a RADIUS server to configure a new server. You can select the primary and backup servers. Refer to Authentication for more information.

MAC Authentication	Enable or disable MAC authentication if an external captive portal is selected.
Simultaneous Login	Allow or disallow users to login simultaneously from different sessions with the same user.
Session Limited	Select the session number to be limited.
Session Timeout	Select the timeout value for connection in minutes (2-1440).
Idle Timeout	Select the timeout value for authentication in minutes (1-1439).
URL Redirection	Enter the URL redirection which users will visit after successful login.
Redirection Interval	Enter the URL redirection time length after which users will visit periodically.
Walled Garden	[Optional] Select a pre-configured Walled Garden which permits access to certain websites before a user has been authorized. Go to **Configure > Walled Garden** for a list of pre-defined walled garden.
SSID/VLAN	Assign a pre-configured VLAN to this captive portal profile.

4. Click **Save.**
5. Click **Push Configuration** at the top left to apply the settings to the affected devices immediately.

Configuring High Availability for VRRP

Virtual Router Redundancy Protocol (VRRP) can be utilized to implement fault tolerance and load balancing on a LAN by designating primary and backup roles among the virtual routers. The primary router is responsible for processing packets send to a virtual IP address and the backup router takes up the primary role when the primary becomes unavailable. This availability of this feature depends on device model.

To configure VRRP:

1. Select a Profile for the desired Gateway model.
2. Select **Network > High Availability.**
3. Enter the following:

VRRP ID	Enter a unique identifier for the VRRP group.
Interface	Select the interface to which the VRRP configuration would be applied.
IP Address	Enter the virtual IP address.
Node Type	Select the designated role of the virtual router.
Priority	Priority determines the order of selection for a primary virtual router among the backup virtual routers (1-255). Higher number means high priority.

Configuring Security Settings

Security features consist of firewall, intrusion prevention, web content filtering, and application control.

1. Navigate to **Configure > Gateway > Profiles.**
2. From the Profile list, click **Security** under the Actions column of the Profile you wish to edit.

Configuring Firewall Settings

IPV4/IPv6 FIREWALL RULES

To Configure IPv4/IPv6 Firewall rules:

1. Select **Security > Firewall.**
2. Under IPv4 or IPv6 Firewall Rules, click **Add** to add a new rule.

   Enter the following:

Priority	Assign a priority number (1-998). Lower number means higher priority.

Name	Enter a name for the new rule (1-64 characters).
Policy	Select the option to allow or deny the specified traffic.
Protocol	Select the protocol to which the rule should be applied: Any, TCP, UDP, TCP/UDP, or ICMP.
Source Interface	Select the interface that the traffic is sent from.
Source	Enter a single IP address or a range of IP addresses using "," or "-", for example, 192.168.200.100,192.168.200.101 (do not include space), or 192.168.200.105-192.168.200.188. Enter "any" for traffic from all IP addresses. For IPv6, enter xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, where x is a hexadecimal digit. You can also use CIDR notation, for example, a.b.c.d/n for IPv4 and xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/n for IPv6, where n represents the subnet prefix length.
Source Port	Enter the port number used for this type of traffic (1-65535). Enter a single port or a range of ports using "," or "-", for example, 3000,3001 (do not include space), or 3000-3200. Enter "any" for all ports for this service.
Destination	Enter a single IP address or a range of IP addresses using "," or "-", for example, 192.168.200.100,192.168.200.101 (do not include space), or 192.168.200.105-192.168.200.188. Enter "any" for traffic to all IP addresses. For IPv6, enter xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, where x is a hexadecimal digit. You can also use CIDR notation, for example, a.b.c.d/n for IPv4 and xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/n for IPv6, where n represents the subnet prefix length.
Destination Port	Enter the port number used for this type of traffic (1-65535). Enter a single port or a range of ports using "," or "-", for example, 3000,3001 (do not include space), or 3000-3200. Enter "any" for all ports for this service.

Schedule	Select a pre-configured Schedule to make the policy effective during the designated time frame. Go to **Configure > Schedule** policies for information about configured schedules.

3. Click **Save**.
4. Click **Push Configuration** at the top left to apply the settings to the affected devices immediately.

Note: The availability of IPv6 Firewall Settings depends on the features of the device.

Port Forwarding

Port Forwarding redirects traffic entering the WAN to another port on the LAN. This is useful when a certain service is hosted on an interval server on the LAN.

To configure Port Forwarding rules:

1. Select **Security > Firewall**.
2. Under Port Forwarding, click **Add** to add a new rule. Enter the following:

Name	Enter a name for the rule (1-64 characters).
Mode	Select whether the rule is for traffic forwarding with or without port translation. If port translation is used, enter the Local Port below.
Interface	Select the WAN interface to which this rule should be applied.
Protocol	Select the protocol to which the rule should be applied: TCP, UDP, or TCP/UDP.
Public Port	Enter the external port associated with this type of traffic or service (1-65535). Enter a single port or a range of ports with "-", e.g. 3000-3002.
Local IP	Enter the IP address of the local server.
Local Port	Enter the local port used for this service if translation mode is selected. Note that the length of the port range must be the same as for the public port specified above.

Allowed Remote IPs	Enter the IP addresses of the remote hosts that are allowed to make connections on the ports specified above . Any means to allow all remote hosts. Multiple IP address can be entered using "," or "-" for an IP address range, for example, 192.168.1.5,192.168.1.6 or 192.168.1.5-192.168.1.6. You can also use the CIDR notation, for example, 192.168.1.0/24.

3. Click **Save.**
4. Click **Push Configuration** at the top left to apply the settings to the affected devices immediately.

Port Triggering

Port Triggering dynamically opens public ports for inbound traffic after certain ports are triggered by a service request.

To configure Port Triggering rules:

1. Select **Security > Firewall**.
2. Under Port Triggering, click **Add** to add a new rule. Enter the following:

Name	Enter a name for the rule (1-64 characters).
Protocol	Select the protocol to which the rule should be applied: TCP, UDP, or TCP/UDP.
Outgoing Trigger Port	Enter the outgoing port used for this service. Enter a single port or a range of ports using “-“, for example, 3000 or 3000-3200.
Incoming Trigger Port	Enter the incoming port used for this service. Enter a single port or a range of ports using “-“, for example, 3000 or 3000-3200.

3. Click **Save.**
4. Click **Push Configuration** at the top left to apply the settings to the affected devices immediately.

1:1 NAT

One-to-one NAT allows a static mapping between an internal IP address and an external IP address.

To configure 1:1 NAT rules:

1. Select **Security > Firewall**.
2. Under 1:1 NAT, click **Add** to add a new rule. Enter the following:

Name	Enter a name for the rule (1-64 characters).
Protocol	Select the protocol to which the rule should be applied: TCP, UDP, or TCP/UDP.
Interface	Select the WAN interface that this rule should be applied to.
WAN IP	Enter the WAN IP address as the external IP address for translation.
Local IP	Enter the local IP address as the internal IP address for translation. It is usually an internal server or device that hosts services for the designated WAN connection to access.
Port	The port used for this traffic type. Enter a single port or a range of ports using “-“, for example, 3000 or 3000-3200.
Allowed Remote IPs	The IP addresses of the remote hosts that this rule will be applied to when the device receives incoming packets for connections on the specified ports. Any means this rule apply to all remote hosts. Multiple IP address can be entered using "," or "-" for an IP address range, for example, 192.168.1.5,192.168.1.6 or 192.168.1.5-192.168.1.6. You can also use the CIDR notation, for example, 192.168.1.0/24.

3. Click **Save** to save the settings.
4. Click **Push Configuration** at the top left to apply the settings to the affected devices immediately.

Configuring IPS Settings

IPS

To Configure Intrusion detection and prevention:

1. Select **Security > IPS.**
2. If the device is equipped of intrusion detection functions, you can enable or disable the following services:

Intrusion Detection	Enable intrusion detection. And select the interface that the IPS and IDS should be implemented.
Intrusion Prevention	Enable intrusion prevention. And select the interface that the IPS and IDS should be implemented.
Stealth Mode	This mode protects your device from Internet intrusion by not responding to unauthorized requests.
Block TCP Flood	Enable this to block TCP flooding to WAN.
Bock UDP Flood	Enable this to block UDP flooding to LAN.
Filter Check Mode	Enable the TCP filtering check mode.
Allow ICMP Traffic	Enable this to allow packets of Internet Control Message Protocol to pass through.
DoS Attacks	Denial-of-Service (DoS) attacks encompass SYN Flood, ICMP Flood, and Echo storm. Configure the flood rate of each attack in packets/second for detection.

3. Click **Push Configuration** at the top left to apply the settings to the affected devices immediately.

Configuring Web Content Filter

The Web Content Filter is used to prevent access to unwanted websites. It allows you to create profiles that can take effect during the designated time frame and block websites belonging to a certain category.

Web Content Filter List

To add a web content filtering rule:

1. Select **Security > Web Content Filter.**
2. Under Web Content Filter List, click **Add** to add a new rule. Enter the following:

Name	Enter a name for the filtering rule.

Policy	Select whether this is a allow or block policy. Go to **Configure > Schedule policies** for information about configured schedules.
Scope	The specified hosts or the whole network that this rule will be applied to.
Non-managed Action	If Block policy is selected, select Allow or Block to allow or block unmanaged sites (i.e. sites not being in the filter). And select Enable for Allow override if you would like to allow the site temporarily. Then enter the Override timeout in seconds to specify the length of time that a blocked site will be allowed before being blocked. The Update on access can also be enabled to restart the timer for each access attempt to the blocked sites.
Policy Scope	Select either Global or By feature to define the scope of the policy. If By feature is selected, enter a single IP address or a range of IP addresses or select an interface to apply the policy with the respective options from Network. Select None for Network if you do not want to apply this rule using IP addresses.
Content Filtering	Define filtering rules using URL or default category alone, both default category and URL, or custom groups. If category or custom group is selected, select the default category or a pre-configured group of categories encompassing a wider variety of website themes. If URL is selected,enter the name or keyword for the website.

You can also configure a warning page to display related messages to prompt the user when a restricted website has been visited.

To configure a warning page:

Under Custom Warning Page, click **Add** to add a new warning page. Enter the following:

Name	Enter a name for this configuration.
Warning Page	Select one of the pre-defined warning page to be displayed. Refer to Splash Pages.

Configure a **Custom Group** if Custom group will be used to define the content filtering above:

Group Name	Enter a name for the custom group.
Custom Filtering Type	Select the filtering type to filter by URL, Category, or URL and Category.
URL Filtering	If URL is selected, enter the name and keyword for the website. This blocks access to websites based on a website's domain name (e.g. google.com) and keywords with matching URLs. For example, use keyword "ABC" to block "www.ABC.com" and "xxx.ABC.com" as well as other URLs containing ABC.
Category Filtering	Select one of the pre-defined categories to block access to.
Bulk Import	Use this method to import a list of websites to the filtering list. It must be a CSV-formatted file containing URLs. Click here to download a sample file.

3. Click **Save** to save the settings.
4. Click **Push Configuration** at the top left to apply the settings to the affected devices immediately.

Configuring Application Control

The Application Control is used to restrict certain communication of applications. It allows you to create profiles that can take effect during the designated time frame and prevent traffic of certain applications from being transferred.

Auto Upgrade

Enable automatic upgrade of application signature database and enter the upgrade frequency in minutes. You may also select a day of week and specify the time in 12-hour clock format for the automatic upgrade.

To add an application control rule:

1. Select **Security > Application Control.**
2. Under Application Control List, click **Add** to add a new rule. Enter the following:

Policy Name	Enter a name for the policy.
Policy	Select whether this is a allow or block policy.

Schedule	Select a pre-configured schedule policy. Refer to Schedule Policies for more information about creating schedules.
Scope	The specified hosts or the whole network that this rule will be applied to.
Policy Scope	Select either Global or By feature to define the scope of the policy. If By feature is selected, enter a single IP address or a range of IP addresses or select an interface to apply the policy with the respective options from Network.
Application Type	Define filtering rules based on a single application, a default group or custom group encompassing a variety of applications from different categories. If default or custom group is selected, select the group from the list.

Configure a **Custom Group** if Custom group will be used to define the application type above:

Group Name	Enter a name for the custom group.
Application List	Select the applications from the list organized by different categories for the custom group.

3. Click **Save** to save the settings.
4. Click **Push Configuration** at the top left to apply the settings to the affected devices immediately.

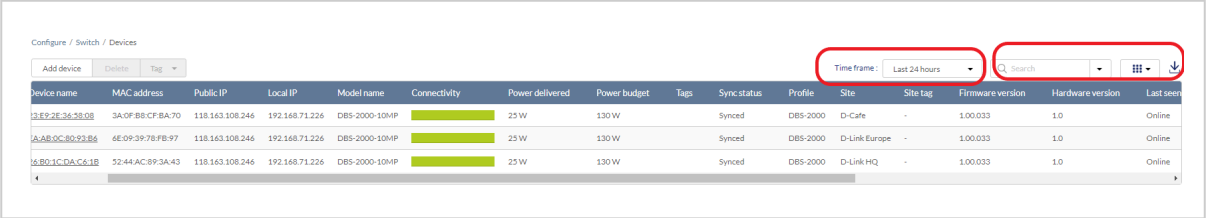
Note: For each of the above configuration page, you can opt to use Push Configuration at the top left of the page to apply the settings to the associated devices of the profile immediately. Or you can use the Push Configuration on the Profiles page to apply the settings of the profile after you are done with all configuration immediately or at a scheduled date and time. We recommend the later method.

Devices

From the Devices page, you can add a single device and register it to a site with a profile, and configure individual devices. This page also provides a detailed overview of all currently registered devices with additional information, including connectivity and operation status, and general settings such as firmware version and license status.

Device Overview

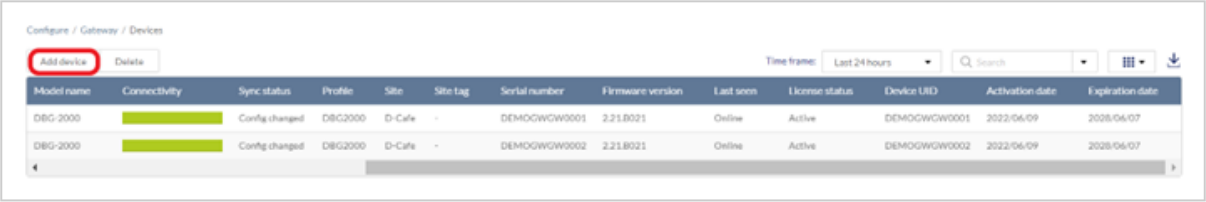
1. Navigate to **Configure > Gateway > Devices.**
2. From the device list, enter a keyword in the search field or click the Search field drop-down menu and specify the criteria to search for a device: Device name, Status, and Site tag. Select the time frame to further define the connectivity period for display.



3. To customize the properties of the table listing, click  .
4. The results will reflect in the refined table listing. You can download the table listing as a single file in CSV format by clicking the download button. In the connectivity bar, red means disconnection to the Internet while green means connected status to the Internet.

Adding Devices

1. Navigate to **Configure > Gateway > 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 **XXXXXXXXXXXX**. When entering the UID, do not include dashes.
Device Name	Enter a name for the device.
Site	Select a Site to link this device to.
Profile	Select a Profile for this device. The device will use the settings configured in that profile.
Add More Licenses	Enter the device license key. Note: Every new device should have a valid license key. Once expired, an additional license must be purchased to continue using the device.

4. Click **Save**.

Editing a Device

Editing the Device Name

1. Navigate to **Configure > Gateway > Devices**.
2. From the device list, click the device name link.
3. In the Device Information section, click the device name in the Device Name field. You will be navigated to the **Monitor > Gateway > Device** page when you select a device from this list.
4. Enter a new name and press **Enter** or click outside of the field.
5. Click **Save**.

Changing the Device Site and Profile

1. Navigate to **Configure > Gateway > Devices**.
2. From the device list, click the device name link.
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 **Save**.

Configuring the Local Device Network Settings

Under normal circumstances, devices will use the network settings of the Profile they are assigned to. If necessary, you 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 > Gateway > Devices**.
2. From the device list, click the device name link.
3. Click the Network tab.
4. In the Use profile configuration field, select disable.

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section. After you have finished all configuration , click **Apply** at the left top to apply the changes immediately to the affected device.

Configuring the Local Device Security Settings

Under normal circumstances, devices will use the firewall and other related security settings of the Profile they are assigned to. If necessary, you 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.

Note: Changing the Routing mode from Network Address Translation (NAT) to Router (go to **Network > Addressing**), the Use Profile configuration option for Security's Firewall settings would be disabled. Moreover, the configured rules of Port forwarding, Port triggering, and 1:1 NAT would be erased.

1. Navigate to **Configure > Gateway > Devices**.
2. From the device list, click the device name link.
3. Click the Security tab.
4. In the Use profile configuration field, select disable.

Note: Local settings are configured identically to Profile settings. Refer to Profiles of Configure - Gateway for more information on how to configure each section. After you have finished all configuration , click **Apply** at the left top to apply the changes immediately to the affected device.

Configuring the Local Device VPN Connections

A Virtual Private Network (VPN) builds an encrypted connection between endpoints over a public network utilizing tunneling techniques. VPN can be configured only if your device supports this feature.

1. Navigate to **Configure > Gateway > Devices**.
2. From the device list, click the device name link.

3. Click the VPN tab in the top-right of the screen.

For more details about the configuration settings, refer to VPN Settings in Monitor-Gateway. After you have finished all configuration , click **Apply** at the left top to apply the changes immediately to the affected device.

Troubleshooting Connectivity of a Device

You can perform Ping test, Traceroute test, obtain WAN throughput and Reboot device. You can also blink the LEDs on the device for diagnostic purposes remotely.

1. Navigate to **Configure > Gateway > Devices**.
2. From the device list, click the device name link.
3. Select the **Tools** tab in the top-right of the screen.

For more details, refer to: Performing a Device Ping Test, Performing a Traceroute Test, Performing LED Blinking and Device Reboot, Performing WAN Throughput Test in Monitor-Gateway.

Adding a License Key to a Device

1. Navigate to **Configure > Gateway > Devices**.
2. From the device list, click the device name link.
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 > Gateway > Devices**.
2. From the device list, click the device name link.
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: Removing a license key from a device will reclassify it as Unused in the license management inventory.

Deleting Devices

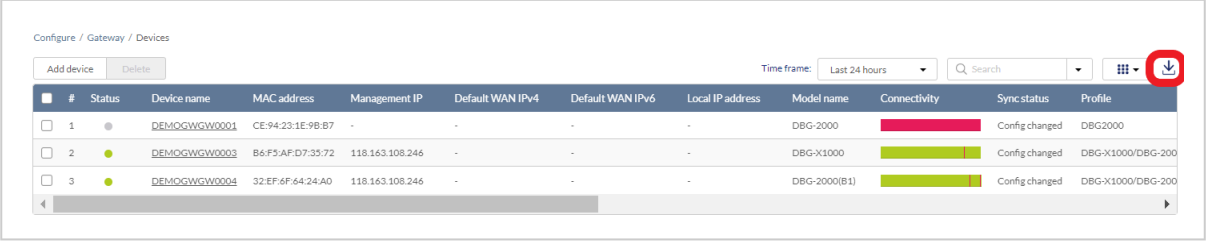
Assigned devices can be unassigned so they can be reassigned at a later point in the device inventory.

1. Navigate to **Configure > Gateway > Devices**.
2. From the device list, click the checkbox next to the device you wish to delete.
3. Click **Delete**.
4. You will be asked whether you would like to delete the device permanently or move it to the Inventory.

Downloading the Device List

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

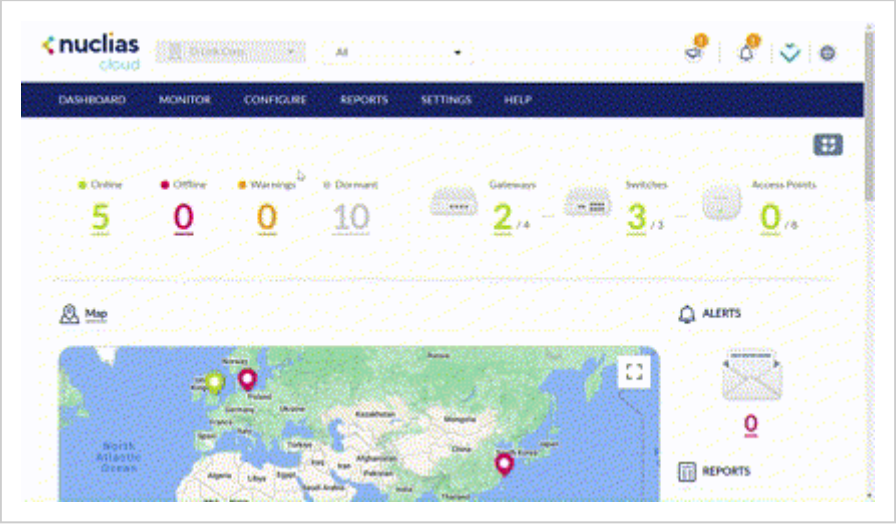
1. Navigate to **Configure > Gateway > Devices**.
2. From the device list, click the Download icon in the top-right.



Authentication

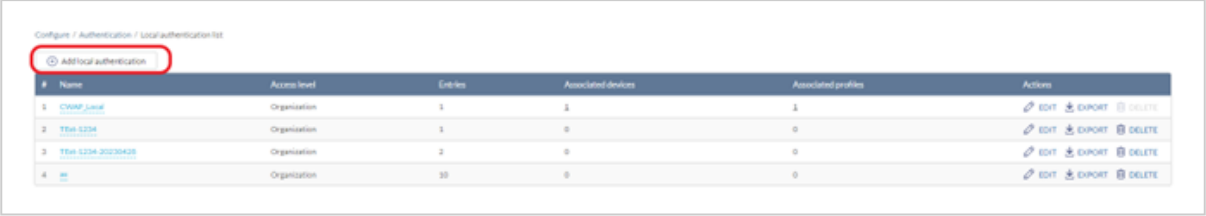
Local Authentication

Local Authentication is used as a local database for user authentication for connection request in many applications such as VPN and SSID connection request with Captive Portal,



Creating a Local Authentication Database

1. Navigate to **Configure > Authentication > Local authentication list**.
2. Click **Add local authentication**.



3. In the Add local authentication window, enter a name for the local authentication list.
4. Select the Access level for the accessibility level of the Local authentication list.
5. Enter a Username and Password for the authentication profile.
6. Add more users by entering more pairs of usernames and passwords or Bulk Import to import a list of user accounts.
7. For Bulk Import, you can download the reference sample template by clicking the **Here** link. The CSV-formatted file contains the local usernames and passwords using this format: [Username] [Password]
8. Click **Browse** to locate the file for bulk import.

9. Click **Save**.

After a new entry is created, the following information will be displayed in the Local Authentication List:

Name	The local authentication database name.
Access Level	The authorized level of access to this authentication profile.
Entries	The number of entries of the authentication profile
Associated Devices	The number of devices that have used this authentication profile for SSID or VPN connection. Click on the number to display the devices' information.
Associated Profiles	The number of configuration profiles that have used this authentication profile for SSID's captive portal setting. Click on the number to display the profiles' information.
Actions	Click Edit, Export, or Delete to edit this profile, export the profile as a single file in CSV format, or delete this profile respectively.

Editing an Existing Local Authentication Database

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

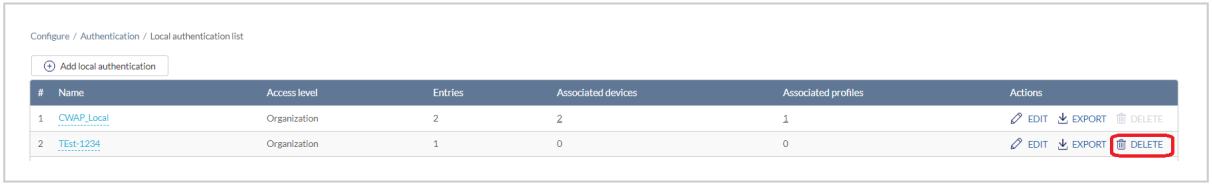


3. In the Edit local authentication window, you can modify the username and password for a user. Click **Delete** to delete a user/password entry. Or click **Add** below the table to add a new username/password entry.
4. Click **Save**.

Deleting a Local Authentication Database

Note: You cannot delete a Local authentication database if there are devices or profiles associated with it.

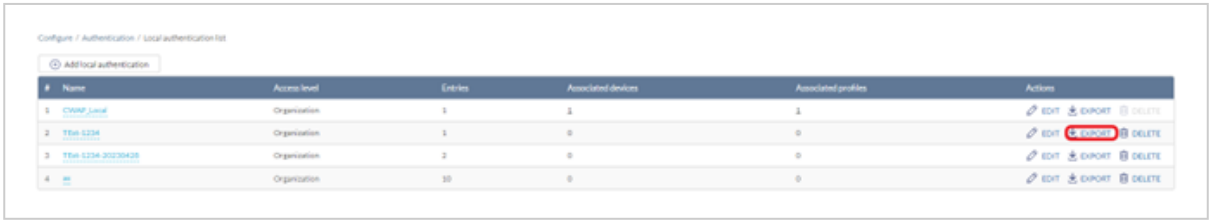
1. Navigate to **Configure > Authentication > Local authentication list**.
2. From the local authentication database list, click the Delete icon under the Actions column of the database you wish to delete.



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

Exporting a Local Authentication Database

1. Navigate to **Configure > Authentication > Local authentication list**.
2. From the local authentication database list, click the Export icon under the Actions column of the database you wish to export.



3. The CSV file will be downloaded in your browser's default download directory.

Authentication Servers

From the Authentication Servers page, you can configure servers that you have installed in your environment to manage network resources and control access to the resources. For example, the Sign-on with basic login for Captive Portal may use an authentication system with an LDAP or a RADIUS server to grant access to a network by authenticating users when a connection request has been issued. And for MAC filtering as an access control for a wireless network, a RADIUS server can be used to permit only authorized devices.

LDAP Server

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

Add an LDAP Server

1. Navigate to **Configure > Authentication > Authentication Servers**.
2. Select LDAP from the Authentication server list, then click **Add**.
3. In the Add an LDAP server window, enter the information below:

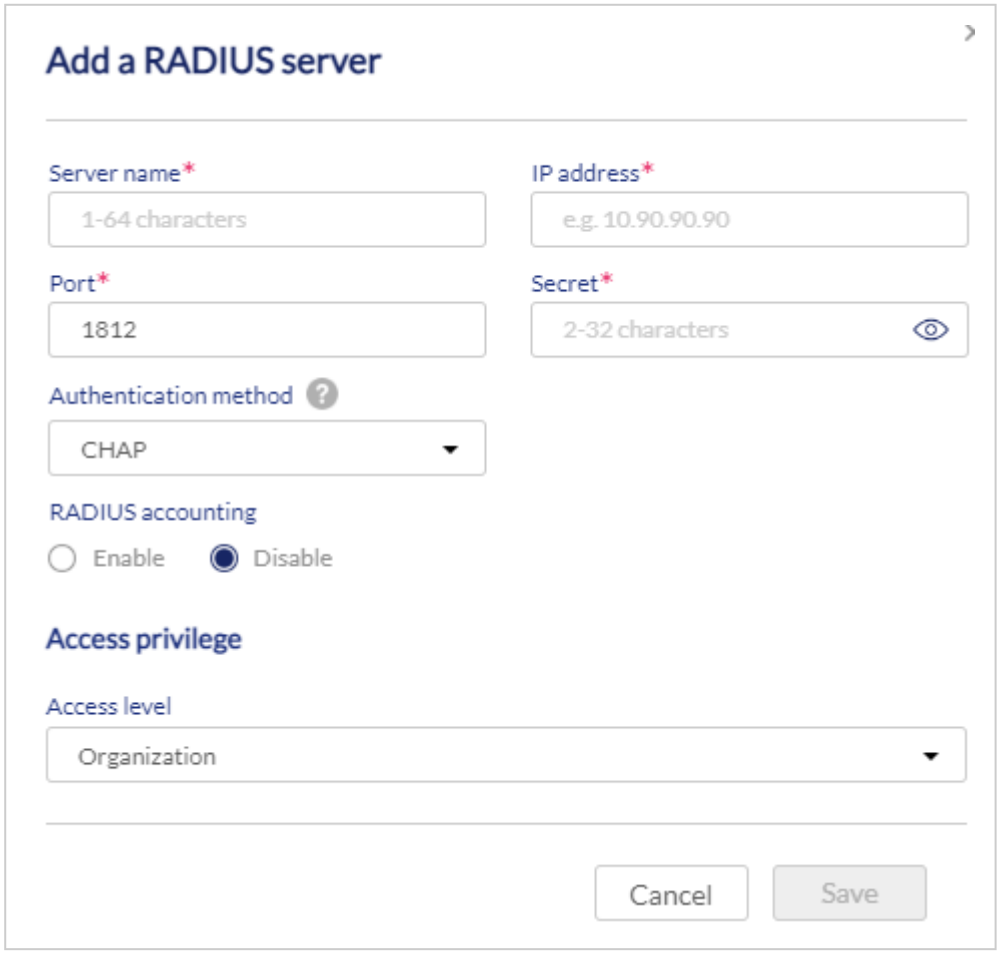
Server Name	Enter a name for the server.
IP Address	Enter a valid IP address.
Port	Enter the port used for LDAP communication.
Base DN	Enter the Base DN, which is the point where the server will search for users.
Encryption	Select the encryption used for the LDAP server from the drop-down menu. You can also choose to disable encryption.
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 setting.

4. Click **Save.** You can click Edit or Delete to edit or delete an entry from the list after the server configuration has been created successfully.

RADIUS Server

Remote Authentication Dial-In User Service (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 > Authentication > Authentication Servers**.
2. Select RADIUS from the Authentication server list, then click **Add**.
3. In the Add a RADIUS server window, enter the information below:

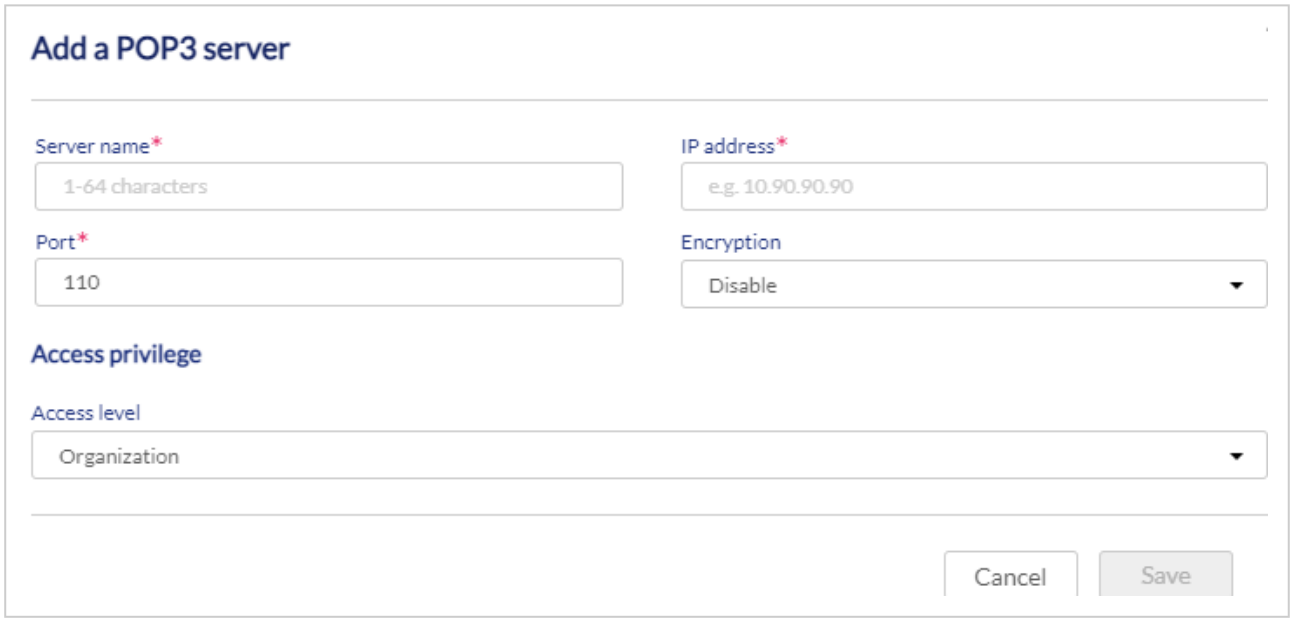
Server Name	Enter a name for the server.
IP Address	Enter a valid IP address.
Port	Enter the RADIUS port number.
Secret	Enter the secret text string that serves as a password between hosts (2-32 characters).
RADIUS Accounting	Enable or disable accounting service for RADIUs. It collects traffic data for monitoring and billing. If this is enabled, enter the

	IP address, Port, Secret and Accounting interim interval of the accounting server.
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 setting.

4. Click **Save.** You can click Edit or Delete to edit or delete an entry from the list after the server configuration has been created successfully.

POP3 Server

POP3 (Post Office Protocol Version 3) is a mail service protocol that allows emails to be downloaded from a mail server. POP3 mail servers can be configured for authentication process to check the username and password supplied by the client.



Add a POP3 Server

1. Navigate to **Configure > Authentication > Authentication Servers.**
2. Select POP3 from the Authentication server list, then click **Add.**
3. In the Add a POP3 server window, enter the information below:

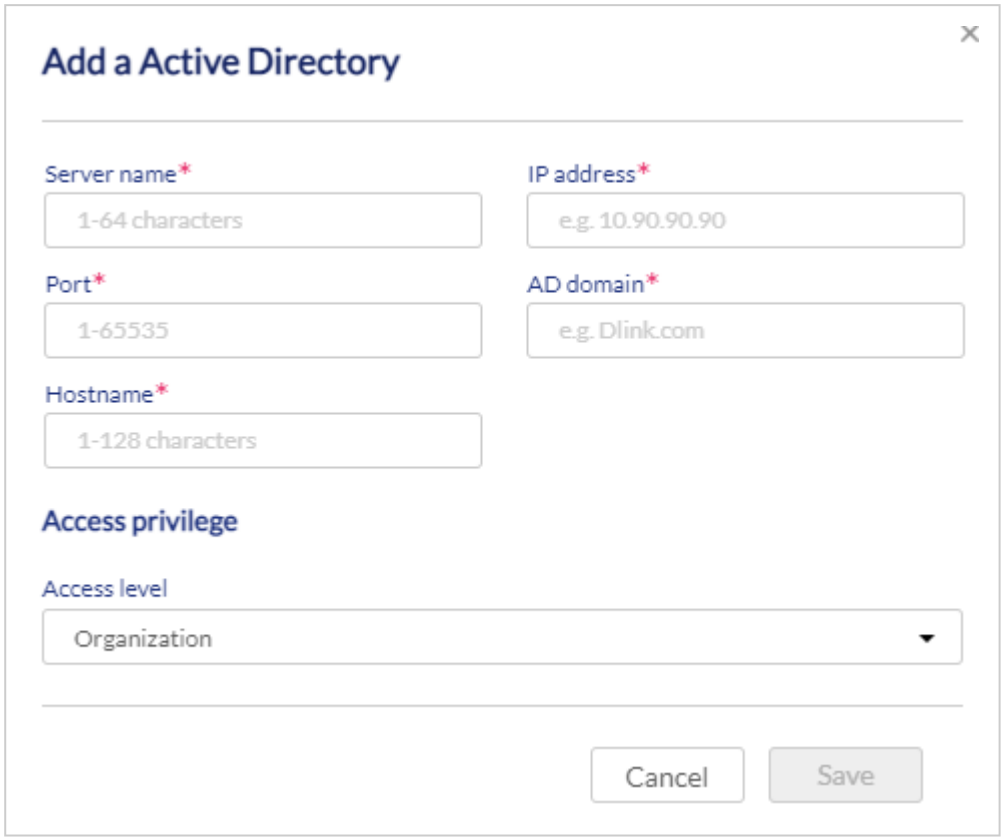
Server Name	Enter a name for the server.
IP Address	Enter the IP address of the POP3 server.

Port	Enter the port used to connect to the server.
Encryption	Select the encryption used for the POP3 server from the drop-down menu. You can also choose to disable encryption.
Certificate	Select the certificate if encryption is used. Refer to Certificate Management for more information.
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 setting.

4. Click **Save**. You can click Edit or Delete to edit or delete an entry from the list after the server configuration has been created successfully.

Active Directory Server

Active Directory (AD) is a service that uses hierarchical structure for managing user account information and network resources and sharing the information to authorized users on the network.



Add a Directory Server

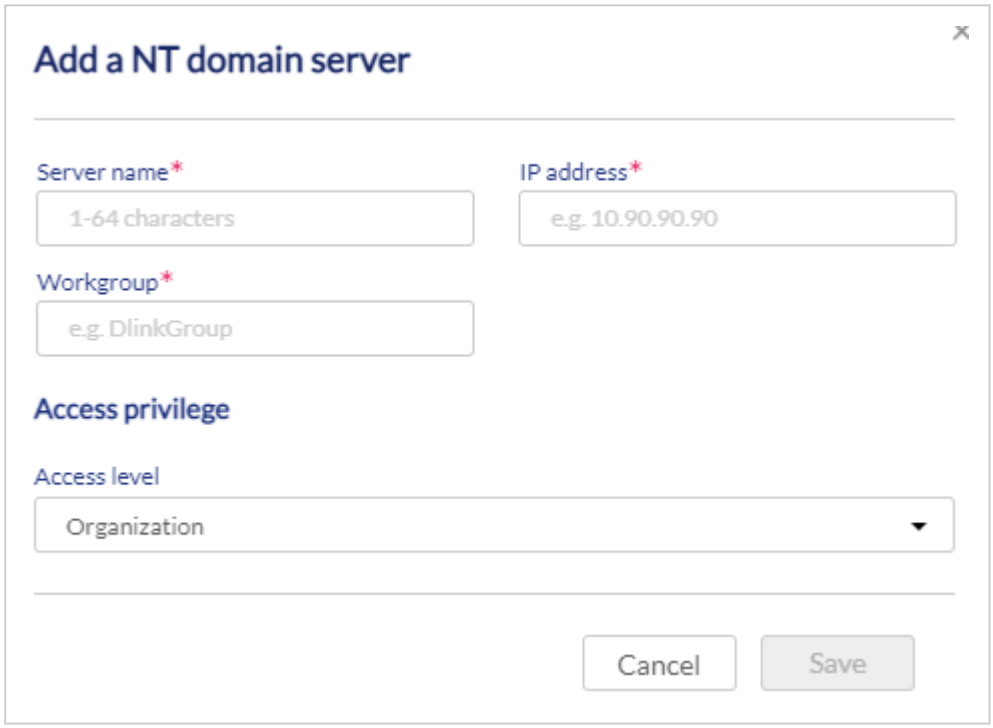
1. Navigate to **Configure > Authentication > Authentication Servers.**
2. Select **Active Directory** from the Authentication server list, then click **Add.**
3. In the Add a Active Directory window, enter the information below:

Server Name	Enter a name for the server.
> IP Address	Enter the IP address of the AD server.
Port	Enter the port used to connect to the server.
AD Domain	Enter the defined domain name.
Hostname	Enter the hostname of the AD server.
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 setting.

4. Click **Save**. You can click Edit or Delete to edit or delete an entry from the list after the server configuration has been created successfully.

NT Domain Server

NT Domain is also a directory service as the above introduced AD service for managing user account information and network resources and sharing the information to authorized users on the network. However, Windows NT uses NetBIOS and WINS instead of DNS for naming resolution. They also differ in many other areas such as administration scope and replication method.



Add an NT Domain Server

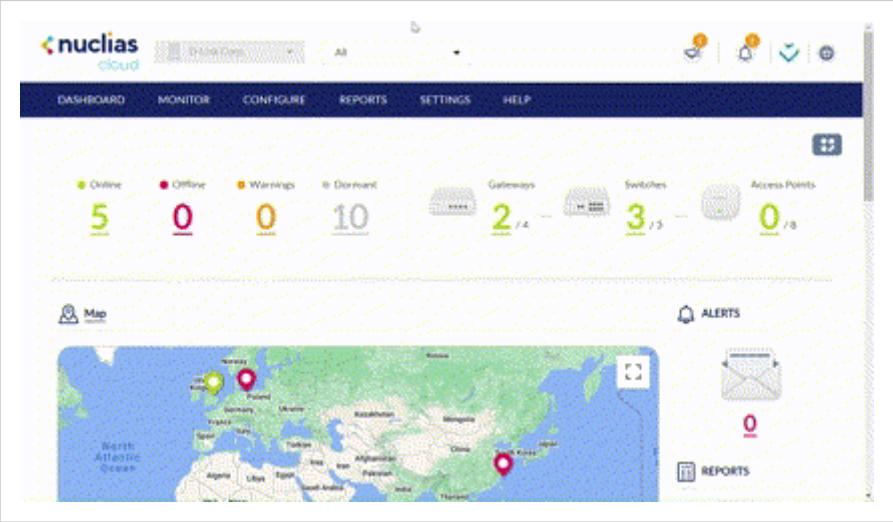
1. Navigate to **Configure > Authentication > Authentication Servers.**
2. Select **NT Domain** from the Authentication server list, then click **Add.**
3. In the Add an NT Domain server window, enter the information below:

Server Name	Enter a name for the server.
IP Address	Enter the IP address of the NT Domain server.
Workgroup	Enter the Windows NT workgroup name.
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 setting.

4. Click **Save**. You can click Edit or Delete to edit or delete an entry from the list after the server configuration has been created successfully.

MAC ACLs

From the MAC ACL section, you can create, manage, and delete MAC access control lists used to manage users' network access using their device's MAC addresses (go to the Access Control page of an SSID of an Access Point or Wireless page of the Network configuration of a supported gateway.)



Creating a MAC ACL Using Single Entries

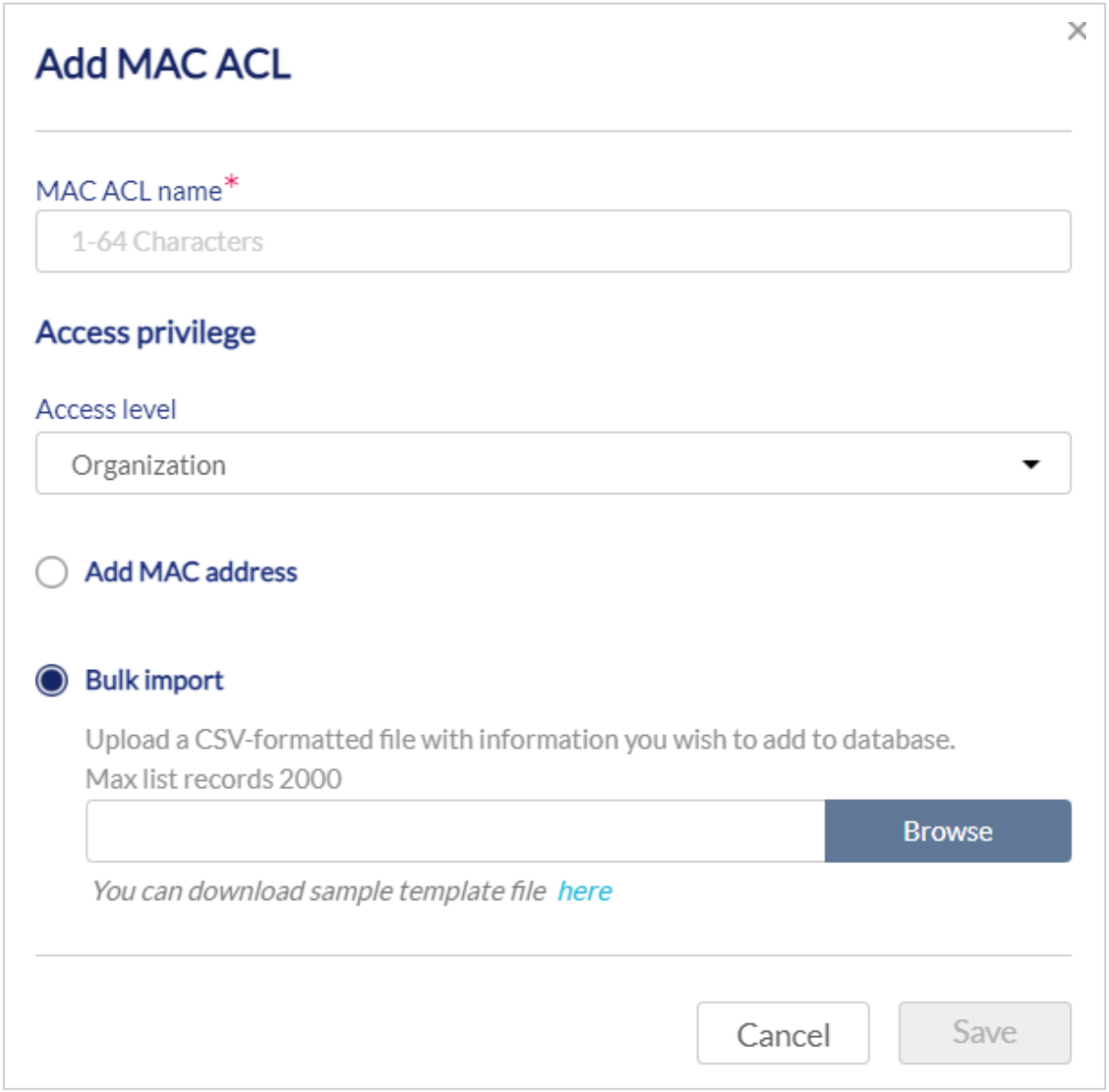
1. Navigate to **Configure >MAC ACLs**.
2. Click **Add MAC ACLs.**
3. In the Add MAC ACL window, enter a name for the MAC ACL.
4. Select the **Access Level** for the accessibility level of the MAC ACL entry.
5. Select **Add MAC address**.
6. Specify the following information:

MAC Address [#]	Enter a valid MAC address.

6. [Optional] Click **Add** to add additional MAC entries. Repeat step 2 to 5 for each new entry.
7. Click **Save**.

Creating a MAC ACL Using Bulk Import

1. Navigate to **Configure > MAC ACLs**.
2. Click **Add MAC ACLs.**
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.



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 > MAC ACLs**.
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**.
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 > MAC ACLs**.
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, edit the following information for the desired MAC entry:

MAC Address [#]	Enter a valid MAC address.

5. Click **Save**.

Deleting a MAC Address From an Existing MAC ACL

1. Navigate to **Configure > MAC ACLs**.
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 MAC entry you wish to delete.
4. Click **Save**.

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

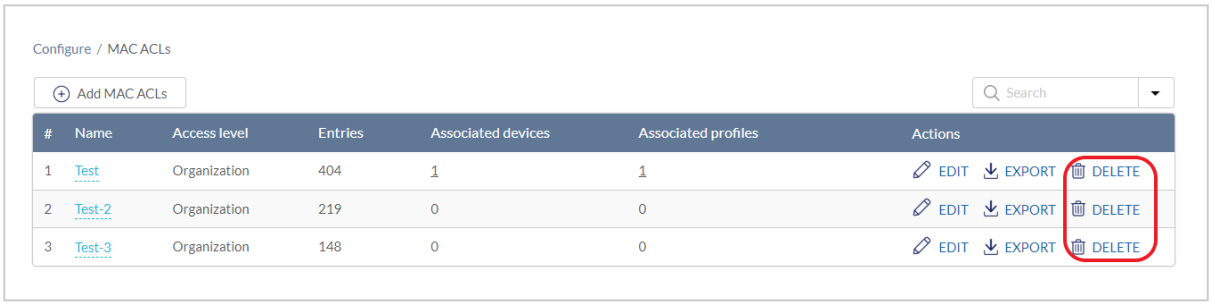
Exporting a MAC ACL

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

1. Navigate to **Configure > MAC ACLs**.
2. From the MAC ACL list, click **Export** to export the desired MAC ACL.

Deleting a MAC ACL

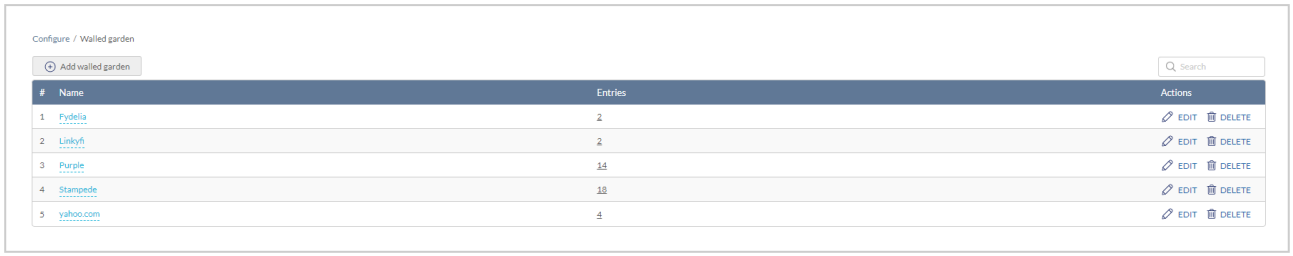
1. Navigate to **Configure > MAC ACLs**.
2. From the MAC ACL list, click the trash can icon under the Actions column of the MAC ACL you wish to delete.



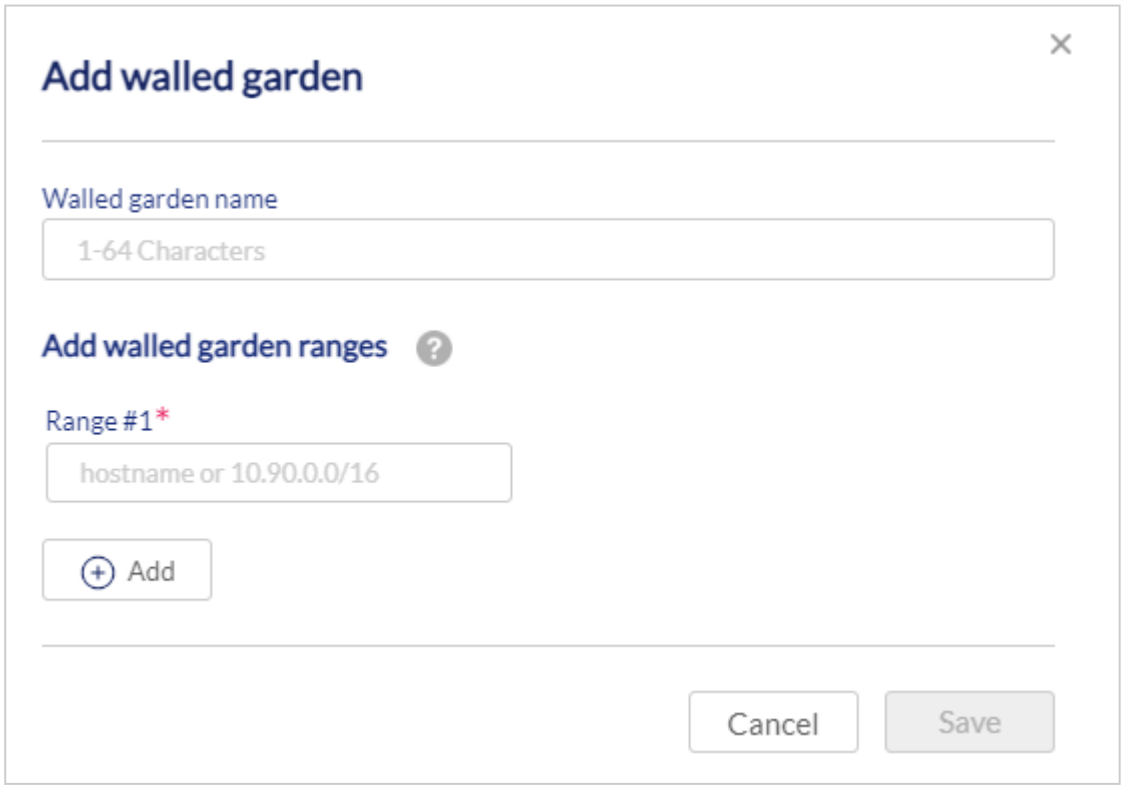
3. When prompted to confirm, click **Yes**.

Walled Garden

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



Adding a Walled Garden



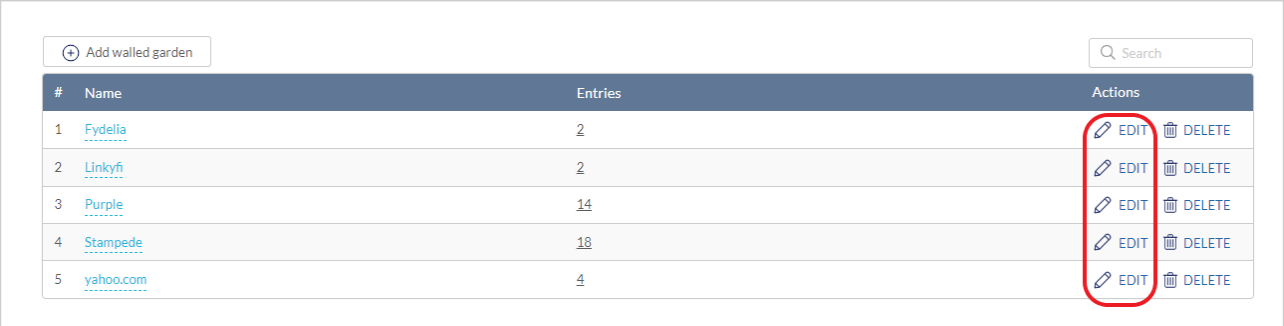
1. Navigate to **Configure > Walled Garden**.
2. Click **Add Walled Garden** in the top left.
3. In the Add Walled Garden window, enter the information below:

Walled Garden Name	Enter a name for your walled garden (1-64 characters).

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

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

Editing an Existing Walled Garden



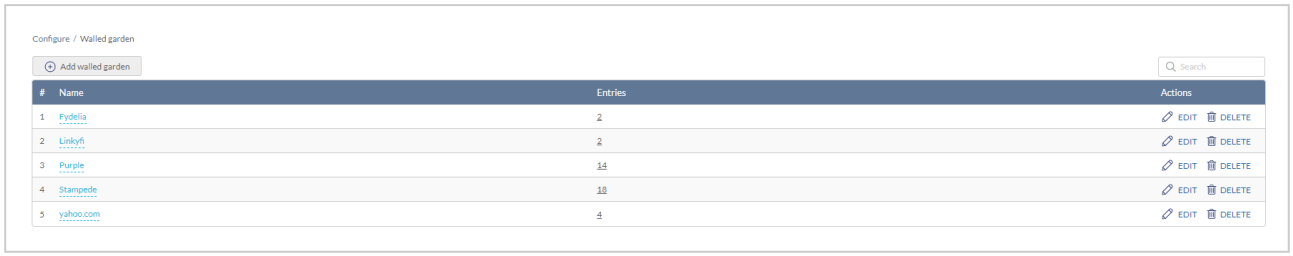
1. Navigate to **Configure > Walled Garden.**
2. From the Walled Garden list, click **Edit** under the Actions column of the Walled Garden you wish to edit.
3. From there, delete existing addresses or add addresses to the list of permitted websites.
4. [Optional] Delete multiple entries by clicking the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

Deleting a Walled Garden

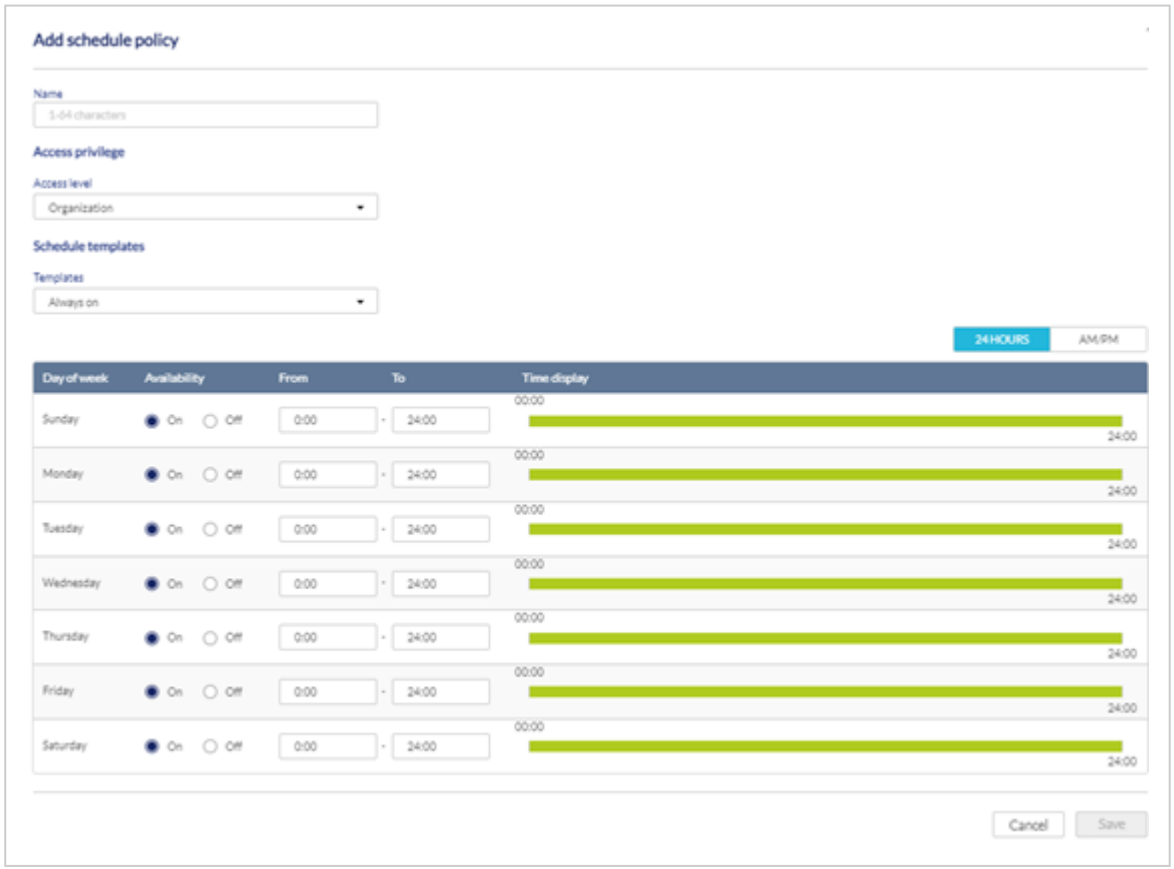
1. Navigate to **Configure > Walled Garden.**
2. From the Walled Garden list, click **Delete** under the Actions column of the Walled Garden you wish to delete.
3. When prompted to confirm, click **Yes**.

Schedule Policies

Schedule policies are used for performing automatic functions periodically according to a defined recurrent frequency. You can create schedule policies to apply configuration changes for functions such as firewall rules and traffic management policies on specific days or time of day.



Adding a Schedule Policy

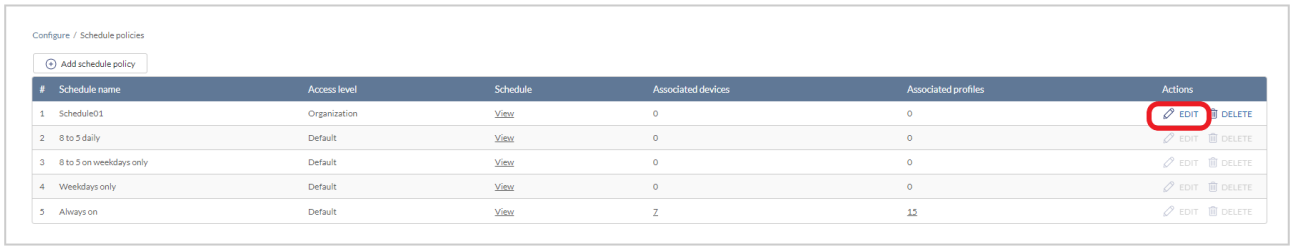


1. Navigate to **Configure > Schedule policies.**
2. Click **Add Schedule Policy** in the top left.
3. In the Add Schedule Policy window, enter the information below:

Name	Enter a name for the schedule policy (1-64 characters).
Access Level	Select among Organization, Site Tag or Site for the access level from the drop-down menu to define the accessibility level.
Template	Select a pre-defined template to start configuring the schedule: 8 to 5 daily, 8 to 5 on weekdays only, Weekday only, or Always on.
Availability	Select the on/off button for the availability of each weekday and enter the start and end time for the days. Optionally, Click the 24 HOURS or AM/PM button in the top-right to change the time display format.

4. Click **Save**.

Editing an Existing Schedule Policy



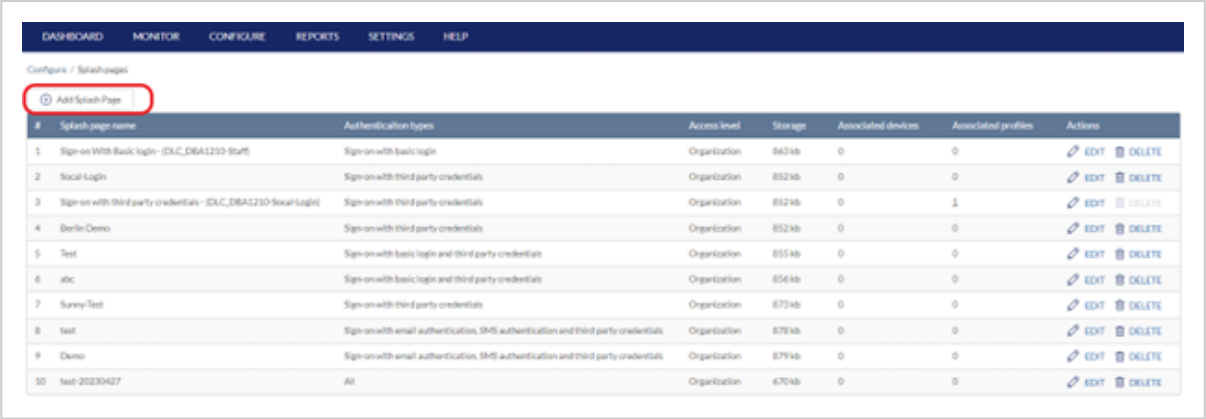
1. Navigate to **Configure > Schedule Policies.**
2. From the Schedule Policies list, click **Edit** under the Actions column of the Schedule Policy you wish to edit.
3. From there, edit the name for the schedule or modify the days of the week and the time span for each day .
4. Click **Save**.

Splash Pages

From the Splash Page Editor window, you can configure and customize splash pages to use with the SSID or gateway. This can be configured to have users click through or enter credentials for a variety of purposes such as Captive Portal authentication page and OpenVPN profile download page or to display warning messages for Web Content Filtering. You can either customize any of the default splash pages or create your own unique splash pages.

Creating a Custom Splash Page

1. Navigate to **Configure > Splash Pages.**
2. Click **Add Splash Page** at the top left.



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

Splash Name	Enter a name for the splash page.
Style	Select the Template option to save it as a template.
Access Level	Select the level of access: Organization, Site tag, or Site to make the template available under the defined level.
Clone from	Select a template to use with the design from available templates under the designated access level.
Click **Next** to continue configuring the items on the Splash Page.	
Preview and Edit in Use Case	Select the use case of the splash page. The following 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 local user account or third-party account credentials. Sign-on with email authentication, SMS authentication and third party credentials: Requires users to log in using their emails, verification code through SMS, or third-party account credentials. Sign-on with SMS authentication: Requires users to log in using verification code through SMS. Sign-on OmniSSL VPN: Used for signing to download OpenVPN clients and connection profile. Session limit warning page: Used to display warning of maximum session reached. Web content filter warning page: Used to display a warning about restricted web content.
Login	Select the Login tab at the top to edit the login page for signing on. You can click on an element to modify the background image or the displayed words with the desired fonts and colors.
Messages	Select the Messages tab to edit message pages for different circumstances depending on the use case selected. You can click on an element to modify the background image or the displayed words with the desired fonts and colors.
Terms	Click this tab at the top to modify the content of Terms.

You can then use the Preview function at the top right to preview the page design under different devices. Just click Edit to switch back to the Edit mode.

4. Click **Save**.

Editing a Splash Page

1. Navigate to **Configure > Splash Pages.**
2. In the Actions column, click Edit for 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.
Login	Edit the login page content.
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	Edit the Terms of Use content.

4. Click **Save**.

Deleting a Custom Splash Page

1. Navigate to **Configure > Splash Pages.**

2. From the list, click **Delete** under the Actions column for the splash page you wish to delete.
3. When prompted to confirm, click **Yes**.

Reports

Reports

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

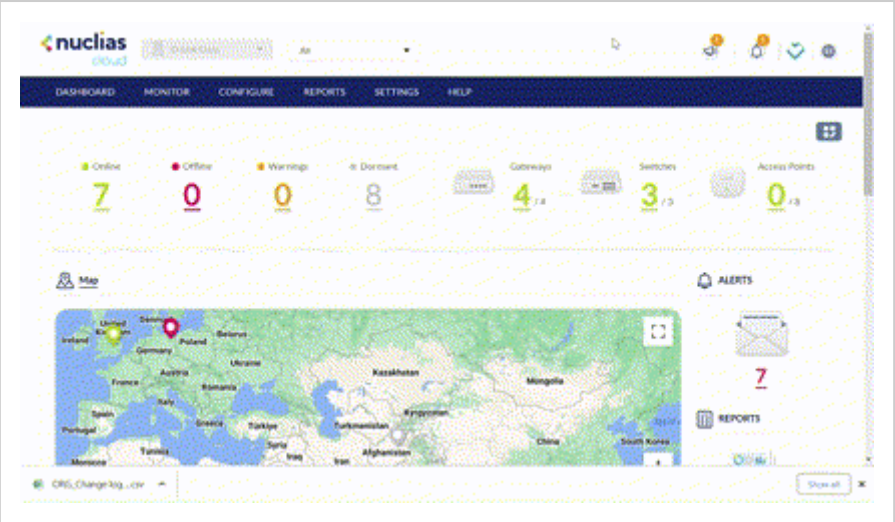
Note: The availability of the pages of the Reports menu depends depends on the account role and privilege level of the managing user.

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

Change Log	From the Change Log section, you can consult a detailed log of changes occurring on the network.
Summary Report	The Summary report provides detailed reports about AP, switch or gateway activities on the managed network. The available types of statistics for reporting depend on the product category.
Alerts	From the Alerts section, you can view a detailed log of all alerts occurring on the network.
Licenses	From the Licenses section, you can consult a list of detailed information about licenses assigned to the selected organization.

Change Log

From the Change Log window, you can consult a detailed log of changes to user accounts, profiles, SSIDs, device configurations as well as other related settings such as schedule policies and MAC ACLs, and firmware upgrades.



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 a keyword to search in all displayed fields,
5. [Optional] Click the filter drop-down menu and enter the following information:

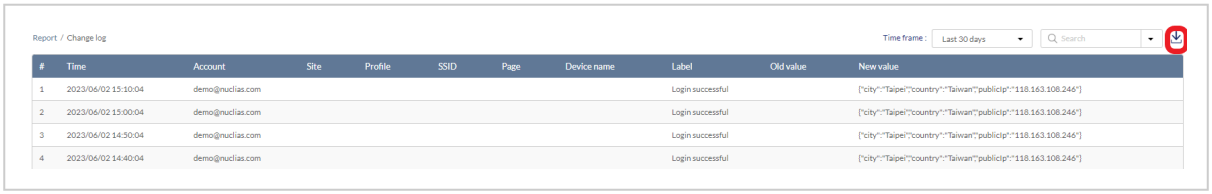
   Note:Multiple filters can be populated to narrow down the search result.

Account	Enter the Account name that the event is linked to.
Site	Enter the name of the Site the event is linked to.
SSID	Select the SSID the event is linked to.
Page	Select the menu page related to the event.

Label	Select the label which briefly explains the event.

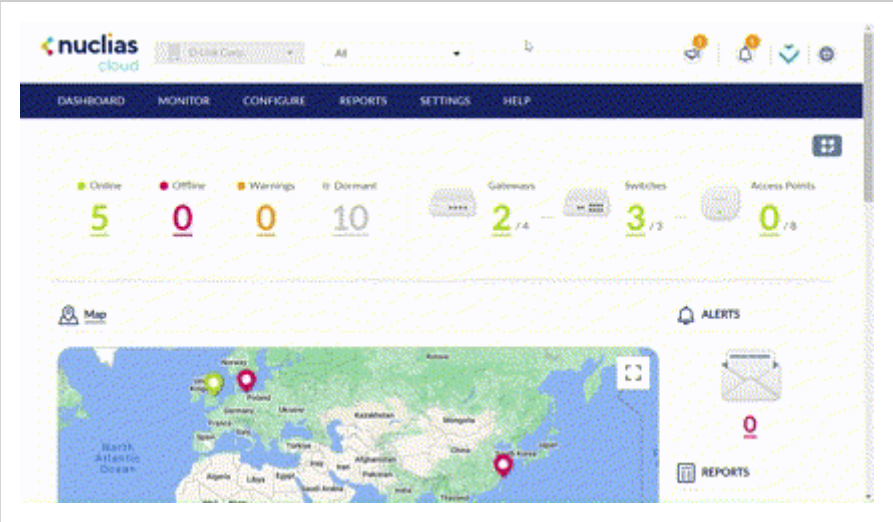
Downloading Change Logs

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



Summary Report

The summary reports provide statistic reports (e.g. Highest CPU utilization and top service ports), which is similar to the Last 24 Hours Summary in the Dashboard; however, it allows you to select the desired time frame and specific statistics for reporting.



Filtering the Reports

1. Navigate to **Reports > Summary report**.
2. Select the desired **Site** to filter the report.
3. Select the **Product category** to filter the report by device type.
4. Select the types of statistics from **Customize report** to display statistic information in the report. Select **All** to show all report types.
5. Select the maximum number of entries for each information category to display from the Show top results drop-down menu.
6. Select a time frame from the drop-down menu.
7. Click **Preview**.
8. You can download the current report by clicking **Download > Download report**.

Sending Reports by Email

1. Navigate to **Reports > Summary report**.
2. Refer to the above section on report filtering to customize the report.
3. Click **Email**. Fill in email addresses then click **Send email**. For multiple recipients, please add separator ";" between email addresses, for example, 123@gmail.com;456@hotmail.com.

Downloading Archived Reports

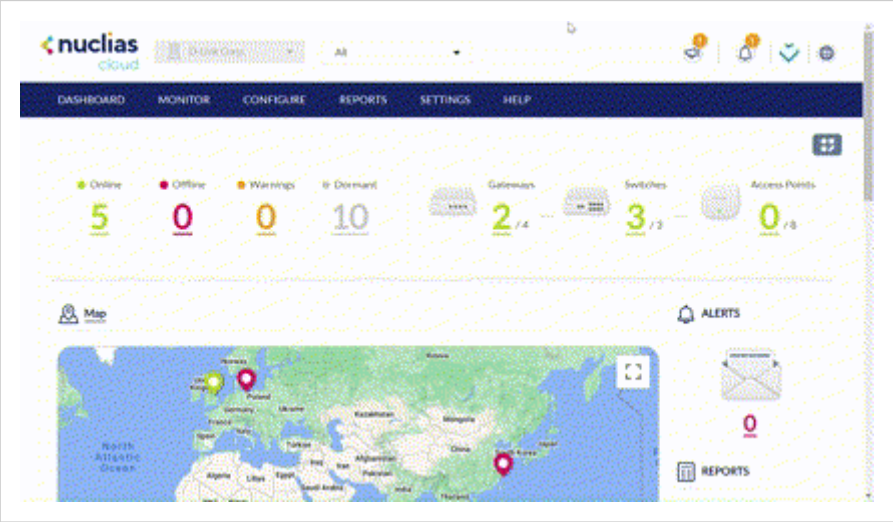
Monthly reports are automatically archived in Nuclias Cloud and can be downloaded for reference.

1. Navigate to **Reports > Summary report**.
2. Click **Download > Download archives** in the top-right.
3. Select a month from the drop-down menu.
4. Click **Download**.

   Note: The system archives reports older than 60 days and store them for up to 2 years.

Alerts

From the Alerts window, you 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.



Note: Users of the Viewer role type will not receive alert notifications.

The types of alerts shown in the alert report 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 organization can see the same alerts depending on their Alert Settings. 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/Processed Alerts

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** or **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

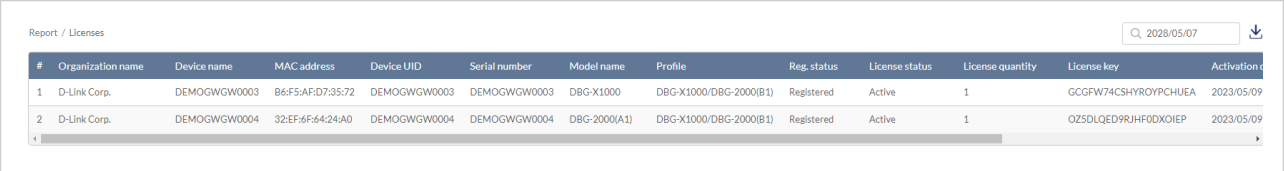
1. Navigate to **Reports > Alerts**.
2. Click the **Not Processed** or **Processed** tab to filter the shown alerts.
3. [Optional] Select a time frame from the drop-down menu.
4. From the alert list, click the Search field.
5. [Optional] Click the filter drop-down menu and enter the following information:

   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

The license report page lists registered devices and their active license information; to obtain information about unregistered devices (i.e. devices without Site and Profile assignment) or devices with expired licenses, go to **Settings > Inventory** and select the **Devices** tab. Furthermore, you can perform license assignment on the Inventory page.



Note: The Licenses Report page is only available to users with the organization-level access privilege.

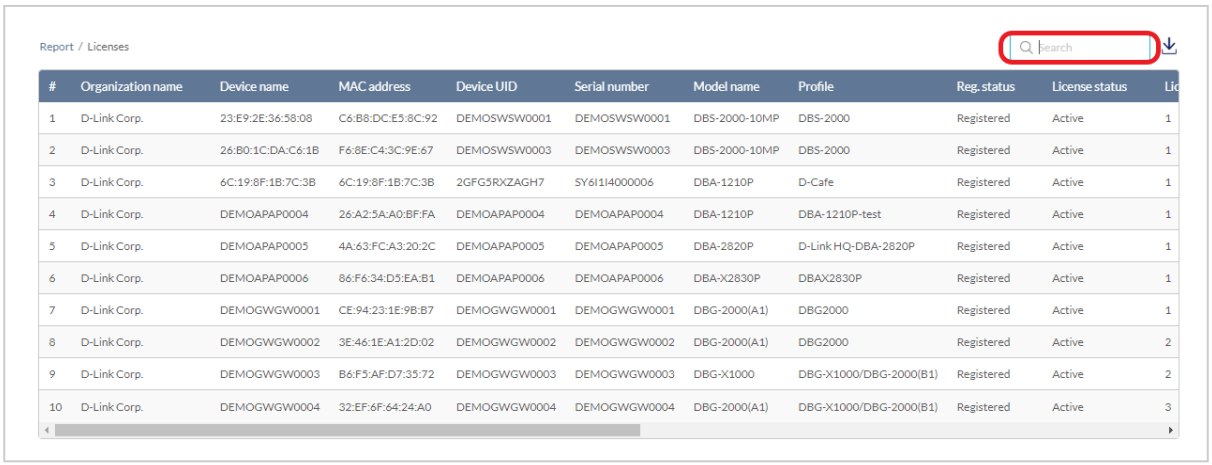
The Licenses page displays the following:

Organization Name	The organization name to which the license belongs.
Device Name	The device name that the license has been registered to.
MAC Address	The MAC address of the device.
Device UID	The device's UID.
Serial Number	The device's serial number.
Model Name	The model name of the device.
Profile	The profile that has been assigned to the device.
Reg. Status	The registration status of the device.
License Status	The status of the device's license. It will display active as long as the device has one active license.
License Quantity	The number of licenses that have been assigned to the device.
License Keys	The keys of the licenses.

Activation Date	The date that the license activates or the license period starts.
Expiration Date	The date that the license expires (after adding up all the license terms).
Last Online on	The last time that the device was detected online.
Firmware	The firmware version of the device.

Filtering License Logs

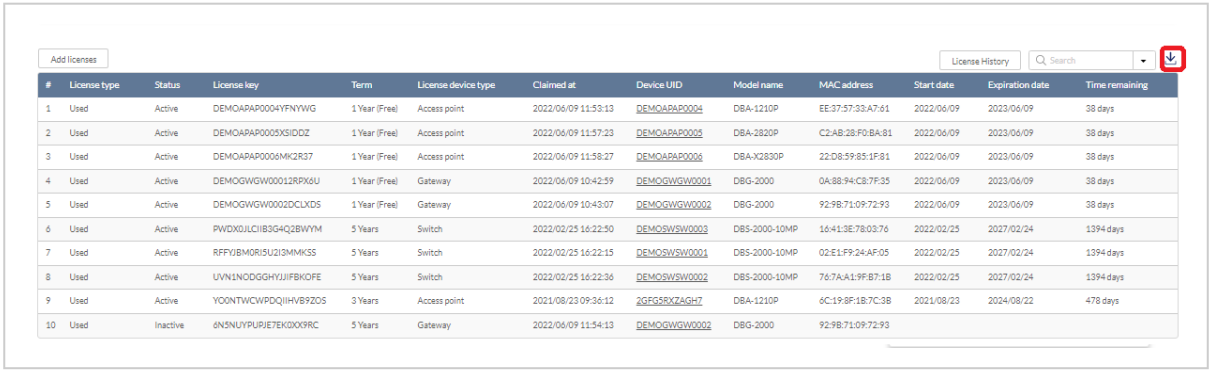
1. Navigate to **Reports > Licenses**.
2. Use the search bar in the top-right to enter a keyword to filter all the fields.



#	Organization name	Device name	MAC address	Device UID	Serial number	Model name	Profile	Reg. status	License status	Lic
1	D-Link Corp.	23:E9:2E:36:58:08	C6:B8:DC:E5:8C:92	DEMOSWSW0001	DEMOSWSW0001	DBS-2000-10MP	DBS-2000	Registered	Active	1
2	D-Link Corp.	26:B0:1C:DA:C6:1B	F6:8E:C4:3C:9E:67	DEMOSWSW0003	DEMOSWSW0003	DBS-2000-10MP	DBS-2000	Registered	Active	1
3	D-Link Corp.	6C:19:8F:1B:7C:3B	6C:19:8F:1B:7C:3B	2GFG5RXZAGH7	SY6I1I4000006	DBA-1210P	D-Cafe	Registered	Active	1
4	D-Link Corp.	DEMOAPAP0004	26:A2:5A:A0:BF:FA	DEMOAPAP0004	DEMOAPAP0004	DBA-1210P	DBA-1210P-test	Registered	Active	1
5	D-Link Corp.	DEMOAPAP0005	4A:63:FC:A3:20:2C	DEMOAPAP0005	DEMOAPAP0005	DBA-2820P	D-Link HQ-DBA-2820P	Registered	Active	1
6	D-Link Corp.	DEMOAPAP0006	86:F6:34:D5:EA:B1	DEMOAPAP0006	DEMOAPAP0006	DBA-X2830P	DBAX2830P	Registered	Active	1
7	D-Link Corp.	DEMOGWGW0001	CE:94:23:1E:9B:B7	DEMOGWGW0001	DEMOGWGW0001	DBG-2000(A1)	DBG2000	Registered	Active	1
8	D-Link Corp.	DEMOGWGW0002	3E:46:1E:A1:2D:02	DEMOGWGW0002	DEMOGWGW0002	DBG-2000(A1)	DBG2000	Registered	Active	2
9	D-Link Corp.	DEMOGWGW0003	B6:F5:AF:D7:35:72	DEMOGWGW0003	DEMOGWGW0003	DBG-X1000	DBG-X1000/DBG-2000(B1)	Registered	Active	2
10	D-Link Corp.	DEMOGWGW0004	32:EF:6F:64:24:A0	DEMOGWGW0004	DEMOGWGW0004	DBG-2000(A1)	DBG-X1000/DBG-2000(B1)	Registered	Active	3

Downloading License Logs

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



#	License type	Status	License key	Term	License device type	Claimed at	Device UID	Model name	MAC address	Start date	Expiration date	Time remaining
1	Used	Active	DEMOAPAP0004YFNYWG	1 Year (Free)	Access point	2022/06/09 11:53:13	DEMOAPAP0004	DBA-1210P	EE:37:57:33:A7:61	2022/06/09	2023/06/09	38 days
2	Used	Active	DEMOAPAP0005XSIDDZ	1 Year (Free)	Access point	2022/06/09 11:57:23	DEMOAPAP0005	DBA-2820P	C2:AB:28:F0:BA:81	2022/06/09	2023/06/09	38 days
3	Used	Active	DEMOAPAP0006MK2R37	1 Year (Free)	Access point	2022/06/09 11:58:27	DEMOAPAP0006	DBA-X2830P	22:D8:59:85:1F:81	2022/06/09	2023/06/09	38 days
4	Used	Active	DEMOGWGW00012RPX6U	1 Year (Free)	Gateway	2022/06/09 10:42:59	DEMOGWGW0001	DBG-2000	0A:88:94:C8:7F:35	2022/06/09	2023/06/09	38 days
5	Used	Active	DEMOGWGW0002DCLXDS	1 Year (Free)	Gateway	2022/06/09 10:43:07	DEMOGWGW0002	DBG-2000	92:9B:71:09:72:93	2022/06/09	2023/06/09	38 days
6	Used	Active	PWDX0JLCIIB3G4Q2BWYM	5 Years	Switch	2022/02/25 16:22:50	DEMOSWSW0003	DBS-2000-10MP	16:41:3E:78:03:76	2022/02/25	2027/02/24	1394 days
7	Used	Active	RFFYJBM0RI5U2I3MMKSS	5 Years	Switch	2022/02/25 16:22:15	DEMOSWSW0001	DBS-2000-10MP	02:E1:F9:24:AF:05	2022/02/25	2027/02/24	1394 days
8	Used	Active	UVN1NODGGHYJJFBKOFE	5 Years	Switch	2022/02/25 16:22:36	DEMOSWSW0002	DBS-2000-10MP	76:7A:A1:9F:B7:1B	2022/02/25	2027/02/24	1394 days
9	Used	Active	YOONTWCWPDQIIHVB9ZOS	3 Years	Access point	2021/08/23 09:36:12	2GFG5RXZAGH7	DBA-1210P	6C:19:8F:1B:7C:3B	2021/08/23	2024/08/22	478 days
10	Used	Inactive	6N5NUYPUPJE7EKOXX9RC	5 Years	Gateway	2022/06/09 11:54:13	DEMOGWGW0002	DBG-2000	92:9B:71:09:72:93			

Settings

Settings

The Settings page provides management functions encompassing portal accessibility and site security control, alert settings, and license as well as inventory maintenance for administrators.

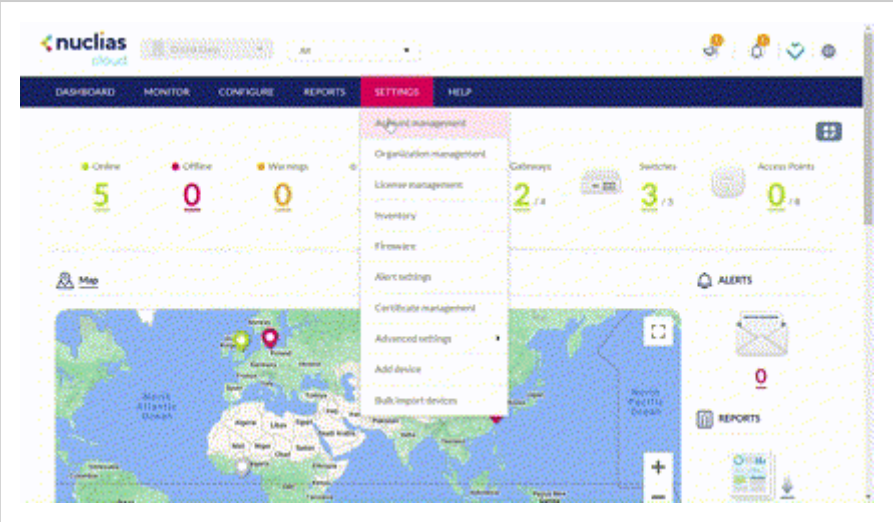
Note: The availability of the pages of the Settings menu depends on the account role and privilege level of the managing user.

Account Management	From the Account Management section, you can view a full overview that includes detailed information of all managed user accounts, invite new users, and edit existing users. Refer to the Account Management page for more information.
Organization Management	From the Organization Management page, you can create and edit Sites and Site Tags, as well as invite users to the organization. Refer to the Organization Management page for more information.
License Management	From the License Management section, you can consult more detailed information of all licenses assigned to the organization including status, activation and expiration dates, and use license co-termination to align licenses with different termination dates . Refer to the License Management page for more information.
Inventory	From the Inventory section, you can consult comprehensive information about all devices currently assigned to the selected organization, including status, hardware information, and which Site (Tag) it is associated with. New devices can also be added from this window. Refer to the Inventory page for more information.

Firmware	From the Firmware page, you can set device upgrade schedules, or manually upgrade a device's firmware. Refer to the Firmware page for more information.
Alert Settings	From the Alert Settings page, you can choose the type of network events that will trigger alert notifications. Refer to the Alert Settings page for more information.
Certificate Management	From the Certificate Management page, you can maintain digital certificates and keys in a central place. It allows you to store certificates issued directly from Nuclias server or from third-party Certificate Authorities. Refer to the Certificate Management page for more information.
Advanced Settings	From the Advanced Settings page, you can change SAML and SMS configurations. Refer to the Advanced Settings page for more information.
Add Device	From the Add Device page, you can quickly add a new device to the organization. Refer to the Add Device page for more information.
Bulk Import Devices	From the Bulk Import page, you can import devices and config them with basic registration information at the same time. Refer to the Bulk Import Devices page for more information.

Account Management

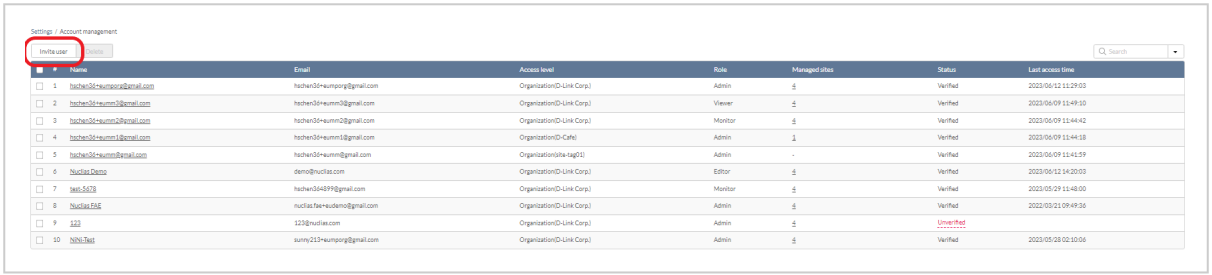
From the Account Management window, you can consult an overview of all managed user accounts. It provides additional information about users, including the organization, Site Tag, and Site(s) the user is assigned to, and the user status.



Note: Access to user accounts depends on the account role and privilege level of the managing user. Only administrators can modify account information of the managed sites.

Inviting a New User

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



3. Specify the following information:

Username	Enter the user's name.

Email Address	Enter the user's email address. This is also the user account to log in to 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: Full 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**.

Note: The invited users will receive an email and be required to set their own password to login. Once logged in, the invited user will be able to manage the sites with the corresponding rights.

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 the user's name.

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: Full viewing rights. Viewer: Limited viewing rights.
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 **Save change**.

Searching for a User

1. Navigate to **Settings > Account Management**.
2. From the user list, click the Search field.
3. Enter a keyword in the search field.
   Note: All fields matching the value entered 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.

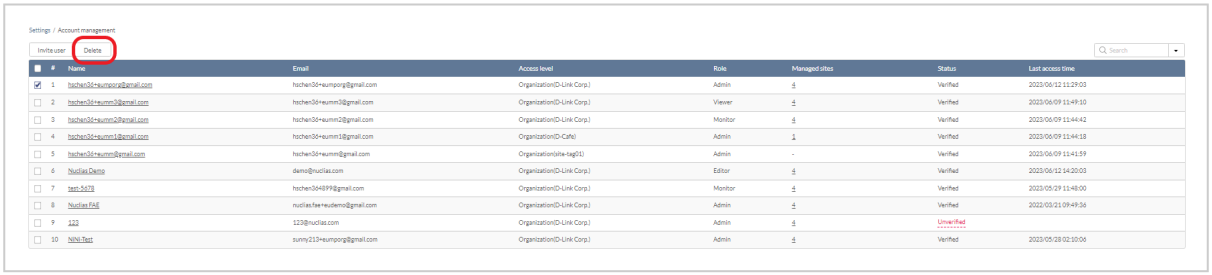
Name	Enter the user's name.
Email	Enter the user’s email address.
Role	Enter the role assigned to the user.

Deleting a User

User accounts 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.

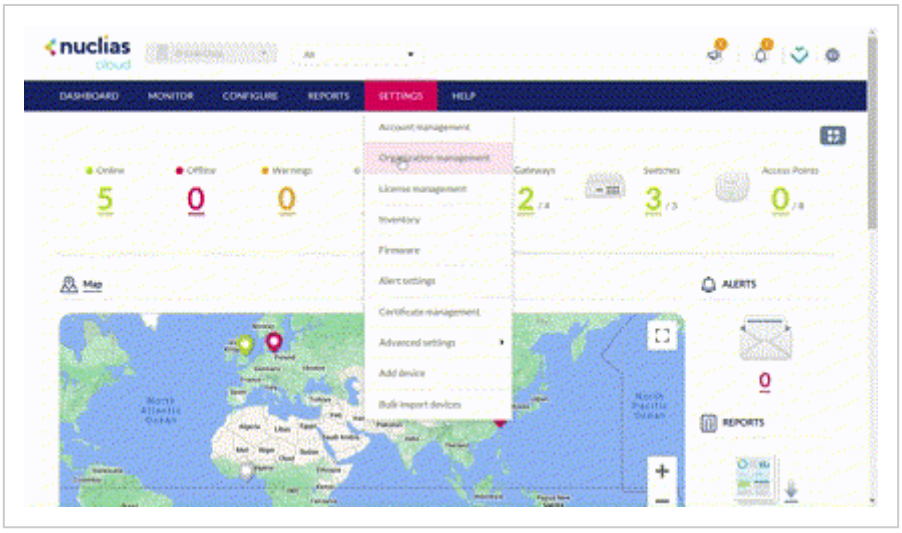
1. Navigate to **Settings > Account Management**.
2. From the user account list, click the checkbox next to the user account(s) you wish to delete.
3. Click **Delete**.



4. When prompted to confirm, enter your user password.
   Note: This is the password of the managing user and not the password of the user to be deleted.
5. Click **Yes**.
   Note: The deleted user will receive a notification email to confirm the account was deleted.

Organization Management

From the Organization Management window, you can view more information about all organizations linked to the user account including device status and amount. You can also create Site and Site Tags, and invite new users depending on the account privilege.



Note: The availability of the organization management features depends on the account role and privilege level of the managing user.

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 you 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. You may also use a SIte Tag if you wish to group Sites together.
Country and Local Time Zone	Select a country and time zone from the respective drop-menu. Wireless products will select legible channels according to your selection of country. The time zone will be used for the scheduling such as firmware management
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.
Devices Credentials	Enter the Password of the admin account used to access the Device's web interface.
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 **Apply**.

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 Tag Name	Enter a name for the Site Tag

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**.

Inviting 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.
Managed Site	Based on the selected Site tag, select a Site. This determines which Sites of the organization can be viewed by the user. Selecting **All** will allow the user to see all Sites under the selected organization.

Role	Select a role for the user. Roles determine the degree of editing and viewing privileges of the user. Admin: Full editing and full viewing rights. Editor: Partial editing and full viewing rights. Monitor: Full viewing rights. Viewer: Limited viewing rights.

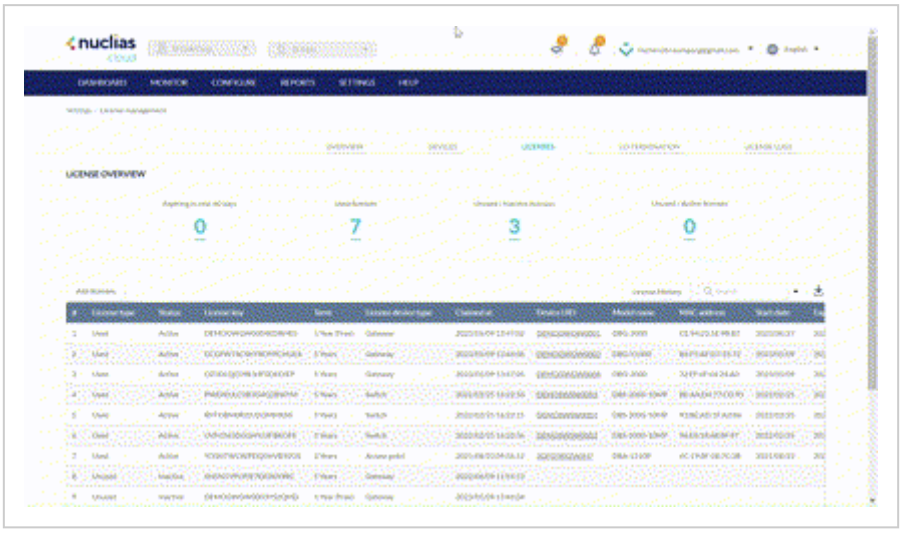
4. Click **Submit**.
5. The user will then receive an email to validate the email address and set a password.

Deleting an Organization

Organizations can be deleted if the admin is the last remaining member of the Organization. Once the Organization has been deleted, the remaining licenses will be transferred to the admin.

License Management

The License Management window provides more detailed information for all licenses assigned to the selected organization, including status, term, activation and expiration dates, and the device type for a license as well as its remaining time. It also allows you to add or import license keys and view license history of expired licenses.



Note: The availability of the License Management page depends on the account role and privilege level of the managing user.

License Overview

1. Navigate to **Settings > License Management**.
2. Click the **Licenses** tab.
3. The License Overview displays licenses in the following category:

Expiring in Next 60 days	Licenses that will expire in 60 days. Click to obtain detailed information about these licenses.
Used Licenses	Licenses that have been assigned to devices; the licenses can be either active or inactive, depending on whether the license period has been started.
Unused Inactive Licenses	Licenses that have neither been assigned to devices nor been activated.

Unused Active Licenses	Licenses that have been activated but have not been assigned to devices.

Adding a License Key

License keys can be added to the organization so they can be manually assigned to devices at a later point.

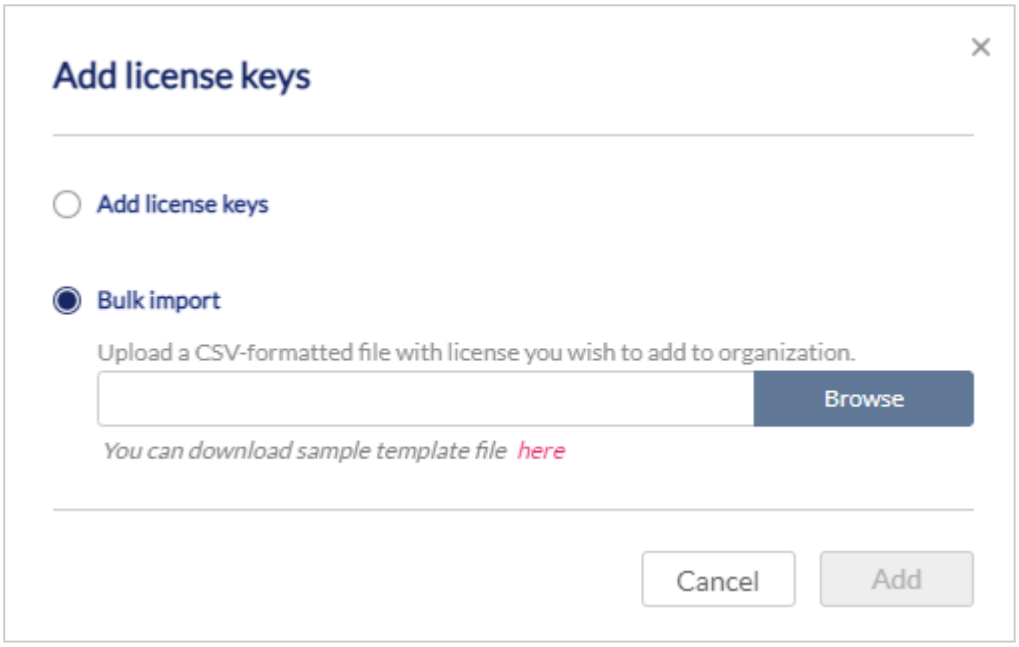
1. Navigate to **Settings > License Management**.
2. Click the **Licenses** tab at the top.
3. Click **Add Licenses**.
4. In the License Key window, enter the required information:

License Key	Enter a valid license key.

4. Click **Add** to add more keys.

   To add multiple licenses at once:

1. Click **Bulk Import.**
2. [Optional] Download the reference sample template.
3. Click **Browse**.
4. Locate the CSV-formatted file containing the license keys using the following format: [License key]
5. [Optional] Download the reference sample template.



6. Click **Add**.

Searching for a License Key

1. Navigate to **Settings > License Management**.
2. Click the **Licenses** tab at the top.
3. From the license key list, click the Search field.
4. Enter a keyword to search for all fields.
   [Optional] Click the filter drop-down menu to display the search criteria: License Type, Status, License Device Type, License Key, and Expiration Date.
5. **Note**: Multiple filters can be populated to narrow down the search result.
6. The results are displayed as the refined table listing with the following properties:

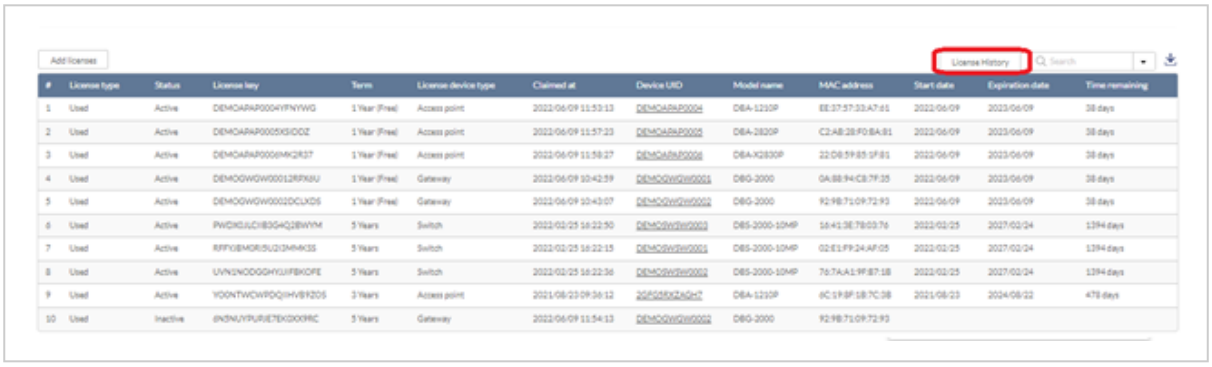
License Type	The type of the license: Used – has been assigned to a device. Unused – has not been assigned to a device.
Status	The current status of the license: either Inactive and Active.
License Key	License key serial number.
Term	Length of the license; 1 Year, 3 Years, etc.

Claimed at	Date and time the license was added to the organization in the format yyyy/mm/dd hh:mm:ss (24-hour clock).
License Device Type	The associated device type of the license.
Device UID	UID of the device the license is assigned to.
Model Name	Model name of the device the license is assigned to.
MAC Address	MAC address of the device the license is assigned to.
Start Date	License start date in the format yyyy/mm/dd.
Expiration Date	License expiration date in the format yyyy/mm/dd.
Time Remaining	The number of days that is left on the license until it expires.

Viewing the License History

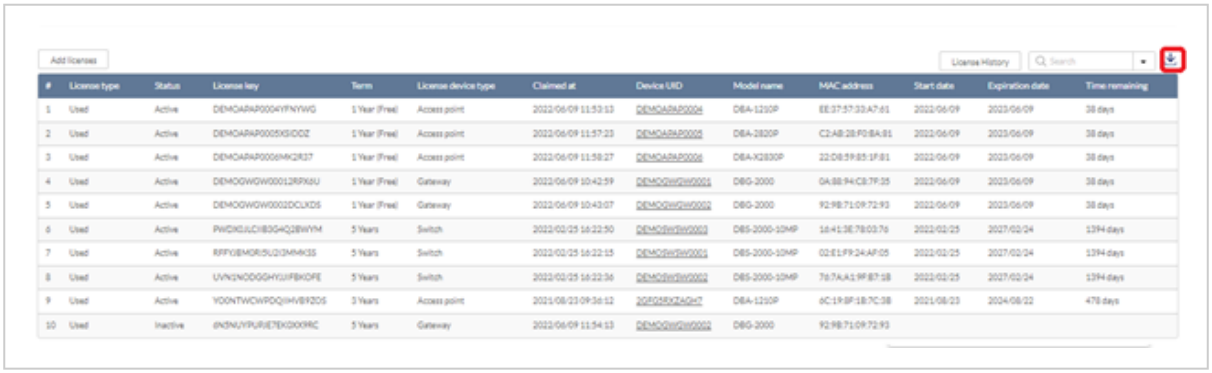
The License History shows the licenses that are already expired.

1. Navigate to **Settings > License Management**.
2. Click the **Licenses** tab at the top.
3. From the license key list, click **License History**. The License History shows the licenses that are already expired with the following information: License Key, Term, Claimed at, Organization, and Model name. You can select a time slot (number of days) that defines the time that the license was expired.



Downloading License Key List

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



Viewing the License Log

Operations performed on the organization licenses or important events of the licenses such as license expiration can be searched and viewed in the License Log.

1. Navigate to **Settings > License Management**.
2. Select the License Logs tab from the top menu. The table displays the licenses management activities history including the Time, Account that performed the license activity, License key, Action that was performed, and Details about the activity.

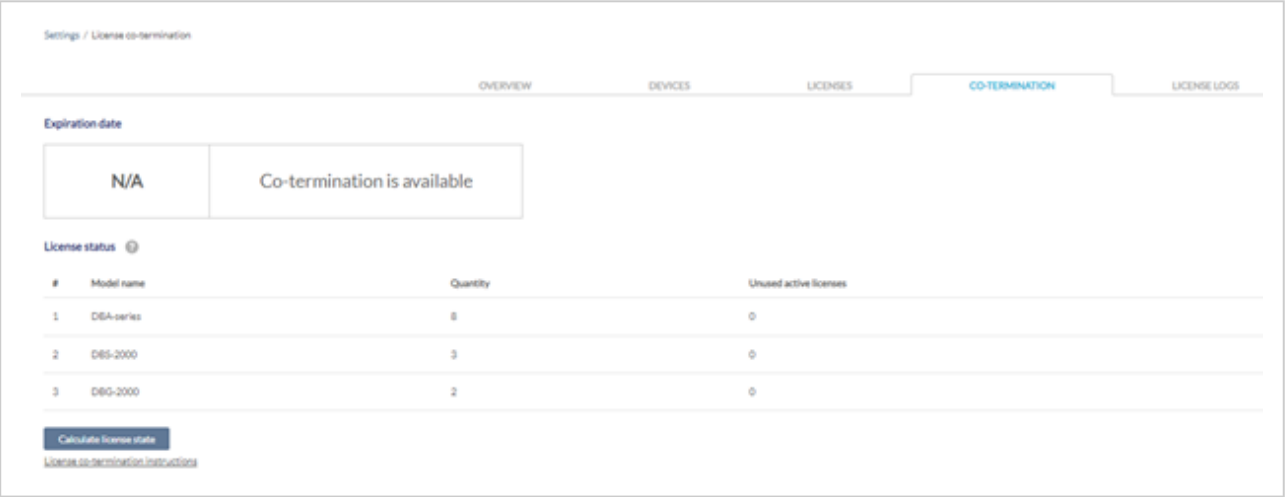


License Co-termination

License co-termination eases license management by terminating all licenses of the participating devices on the same date regardless of their original expiration date.

Note: The operation of license co-termination is irreversible, and the original license cannot be recovered.

Devices from the same Organization that can participate for Co-termination include devices with active licenses and expired licenses. Licenses from the same organization that can be used for co-termination include active and inactive licenses bound on devices and unused active licenses (but not the unused inactive licenses). Moreover, the Co-termination formula is a weighted average calculated by multiplying the remaining days by the device weight and dividing the sum by the total weights of all devices.



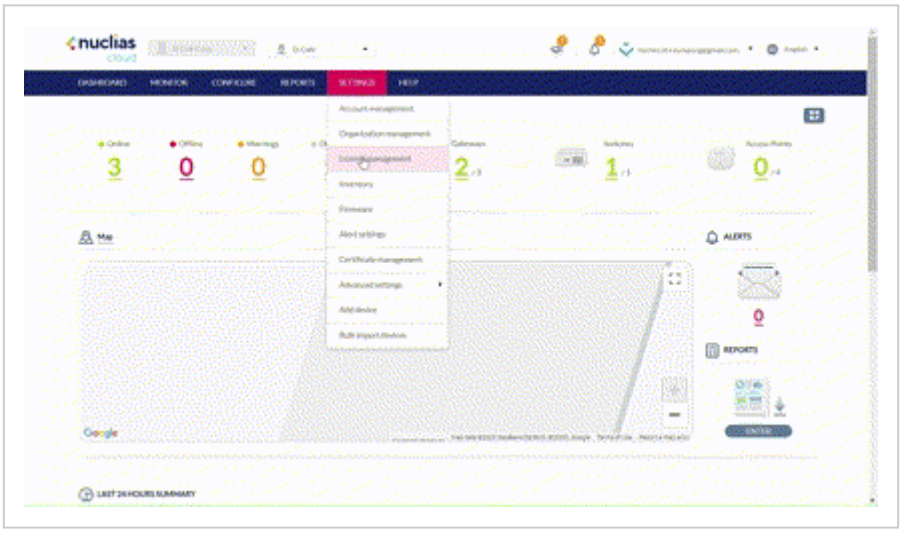
To co-terminate licenses:

1. Navigate to **Settings > License Management**.
2. Select the Co-Termination tab from the top menu.
3. Click **Calculate License State**. The estimated Expiration date and the remaining number of days until expiration will be displayed.
4. [Optional] Click the License co-termination instructions link to learn the principles of the license co-termination calculation.
5. Click **License co-terminate** at the bottom to proceed with the process.
6. A window will appear to display important notice about the operation. Note that the operation cannot be reversed, and the original license would be terminated and replaced by the new license keys with the co-termination date.
7. After reading the notice, click **I understand the terms and still wish to proceed**. Then click **Confirm.**
8. You should receive a notification email once the licensing co-termination has been applied.

Inventory

The inventory can be seen as the virtual stock that you may first add multiple devices to, then assign to the selected Site and Profile or register with licenses later.

From the Inventory window, you can consult comprehensive information about all the devices currently assigned to designated access level, including status, hardware information, license status, and which Site and Profile the devices are assigned to.



Note: The displayed devices are based on the user's access level.

Device Overview

1. Navigate to **Settings > Inventory**.
2. Select the **Devices** tab.
3. The Device Overview displays devices in the following categories:

Total Devices	The total number of devices that are in the organization's inventory.
Access Points	The number of access points.
Switches	The number of switches .

Gateways	The number of gateways.

And the table displays the following information about the devices for each category:

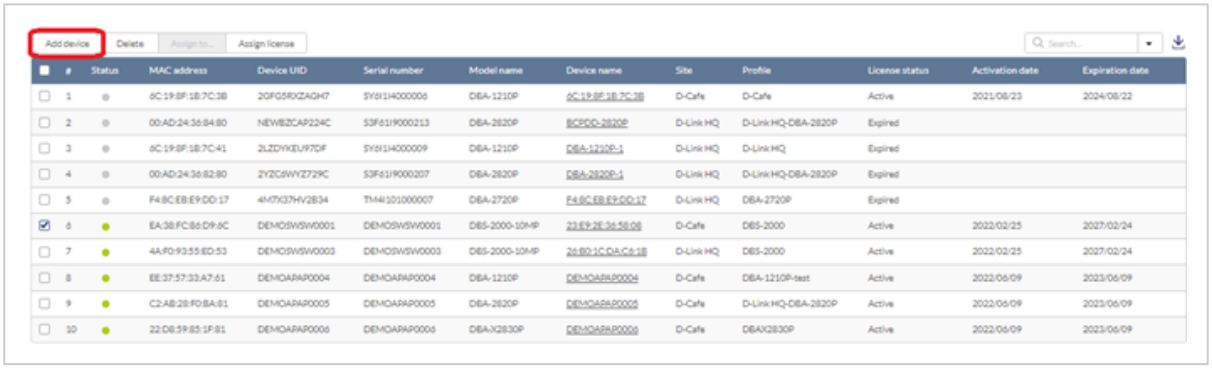
Status	The operation status of the device.
Device Name	The device name that the license has been registered to.
MAC Address	The MAC address of the device.
Device UID	The device's UID.
Serial Number	The device's serial number.
Model Name	The model name of the device.
Site	The site that the device has been assigned to.
Profile	The profile that has been assigned to the device.
Reg. Status	The registration status of the device.
License Status	The status of the device's license. It will display active as long as the device has one active license. For detailed license information, go to **Settings > License Management**.
Activation Date	The date that the license activates. For detailed license information, go to **Settings > License Management**.
Expiration Date	The date that the license expires (after adding up all the license terms). For detailed license information, go to **Settings > License Management**.

Adding Devices to the Inventory

After adding a new device, assign a Site and Profile to a device to allow 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 XXXXXXXXXXXX. When entering the UID, do not include dashes.

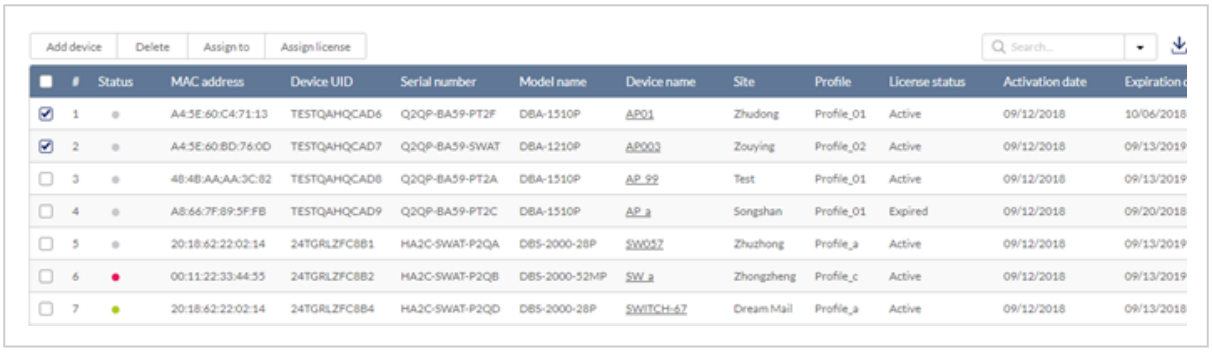
To bulk import new devices to the Inventory:

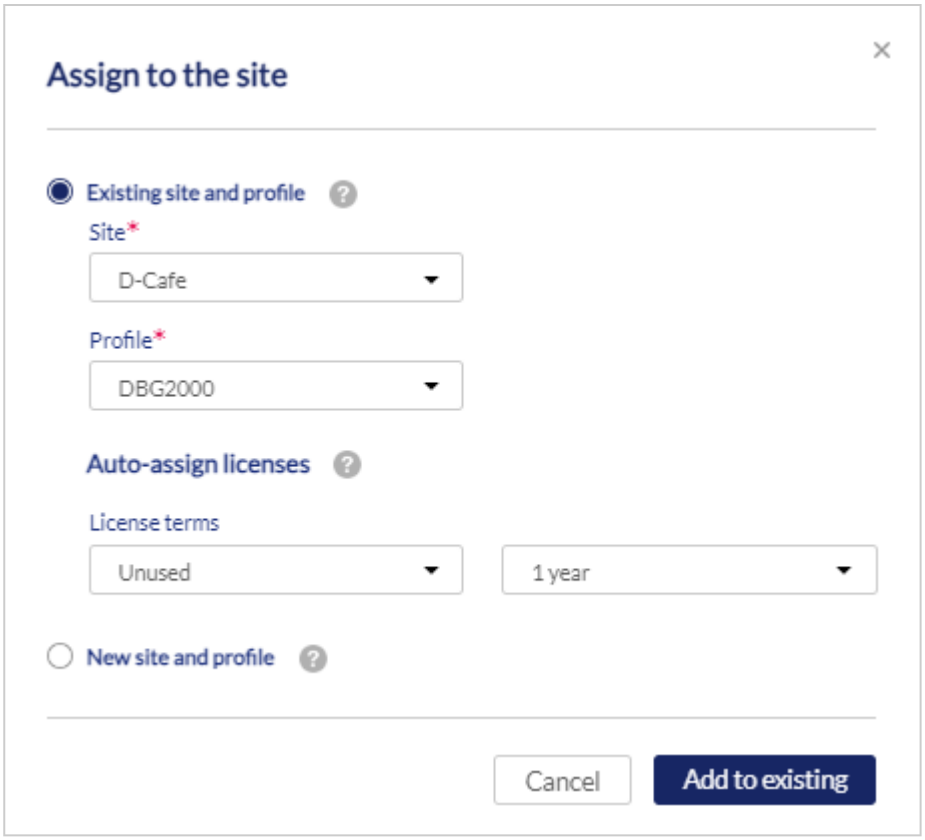
4. Click **Bulk import**. You can download the reference sample template.
5. Click **Browse**.
6. Locate the CSV-formatted file containing the UIDs of the devices.
   Note: To add devices to the inventory, use the following format: [UID].
7. Click **Save**.

Assigning Devices to a Site

Registering a new device to the Inventory requires manually assigning it to a Site and Profile.

1. Navigate to **Settings > Inventory**.
2. Select devices and click **Assign to**.





3. Specify the following information:

Site	Select a Site to link this device to. Or you can select **New site and profile** and enter the following information for a site: Site, Country, Time zone, and Address. Then click **Create site and add**.
Profile	Select a Profile for this device. The device will use the settings configured in that profile.
Auto-assign License	[Optional] Auto-assign license allows you select an available license by license term.

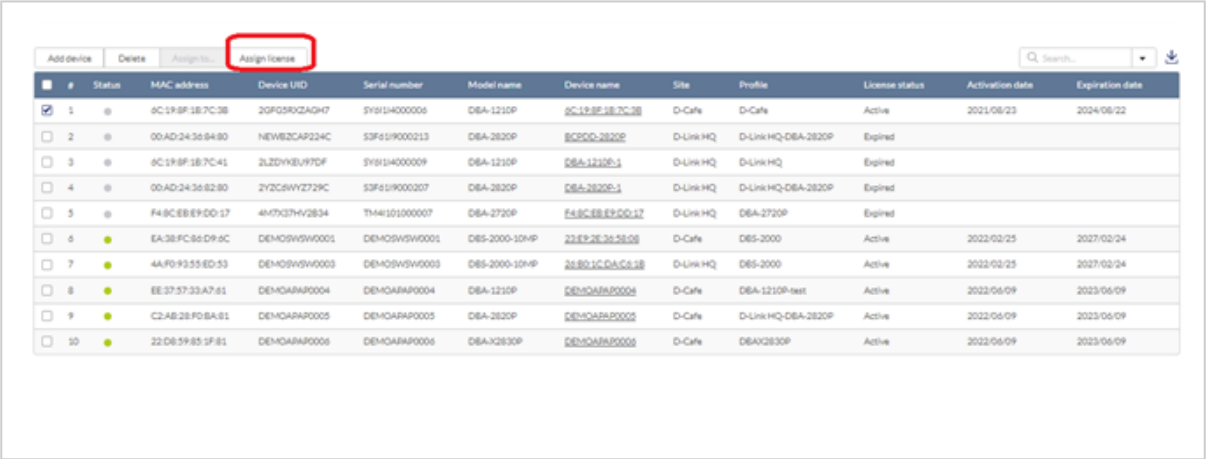
	Note: Every new device will be issued a one-year free license key. Once expired, an additional license must be purchased to continue using the device.

6. Click **Add to Existing**.

Assigning Licenses to a Device

Product Registration requires you to enter a valid license key to activate the service.

1. Navigate to **Settings > Inventory**.
2. Select the devices and click **Assign license**.

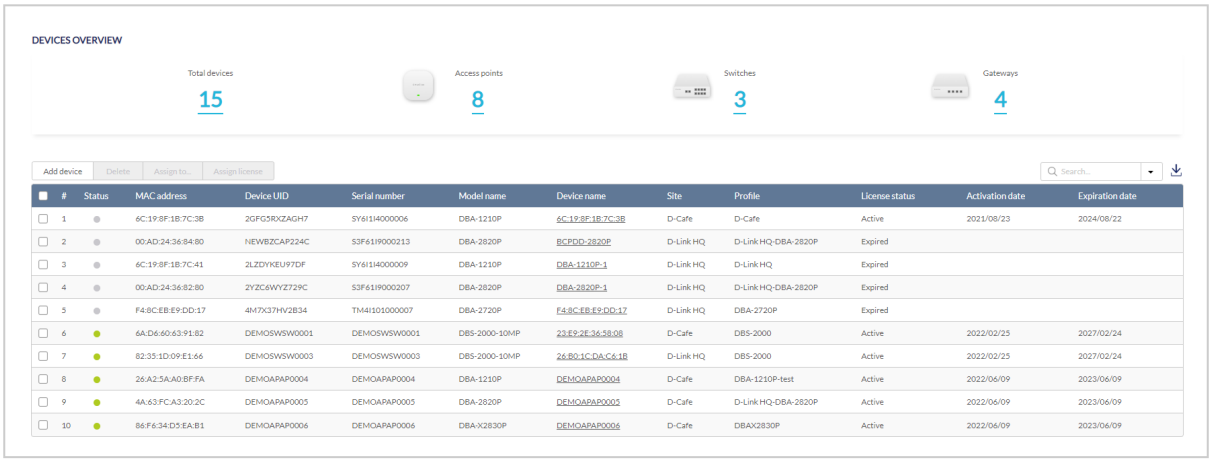


3. According to the device's product category, specify the license terms to look for available licenses. Click **Add**to add more licenses with the desired terms.The system will display **Insufficient Licenses** if there are no available licenses for the selected term.
4. Click **Assign** to let the system assign the license keys to devices automatically. The licenses will be listed under Used licenses with information such as start and expiration date.

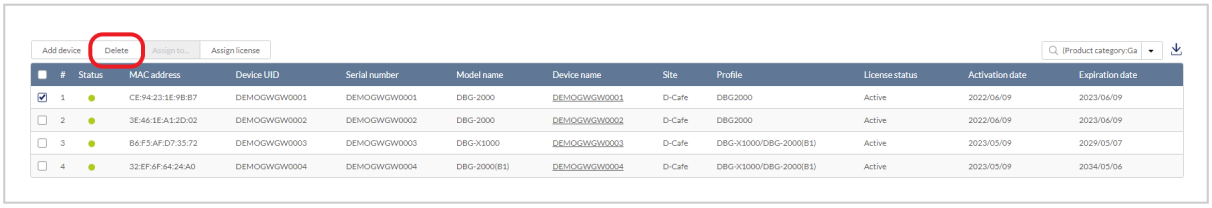
Deleting Devices from the Inventory

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 **Devices** list to filter the devices by category.



3. From the device list, click the checkbox next to the device(s) you wish to delete.
4. Click **Delete**. You will be asked if you would like to delete this device permanently from Nuclias.



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

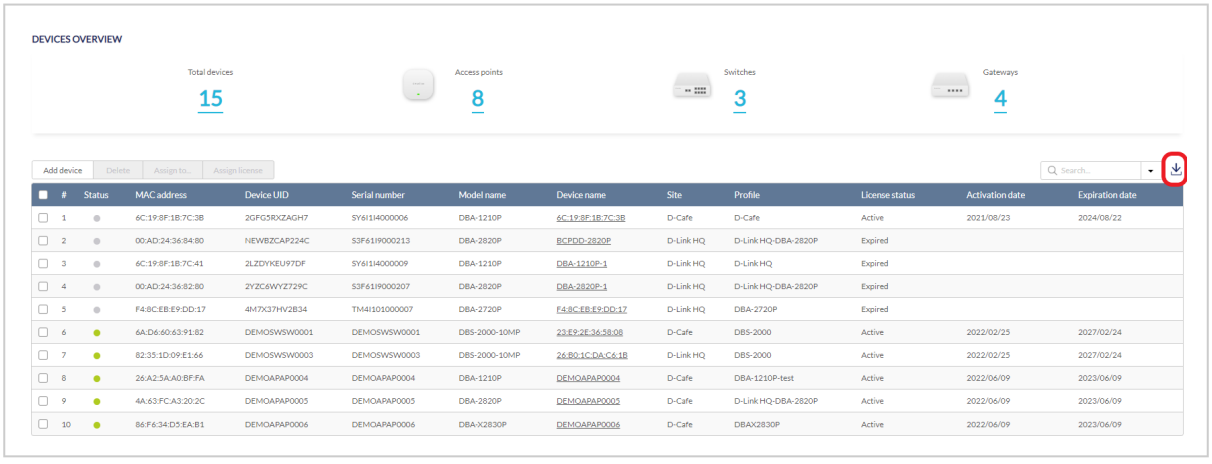
Searching for a Device

1. Navigate to **Settings > Inventory**.
2. Click the **Devices** tab.
3. From the device list, click the Search field to bring up search criteria: Status, Product category, Model name, Used/Unused (for license status), Expiration date (for license information), MAC (manually enter the device's MAC address), Device UID, and Serial number.



Exporting the Inventory List

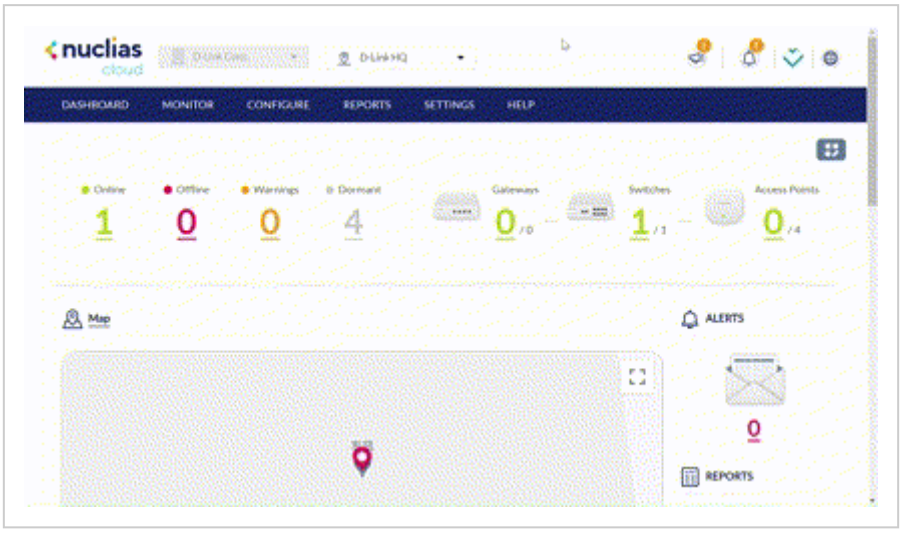
1. Navigate to **Settings > Inventory**.
2. Click the **Devices** tab .
3. Refer to the above **Searching for a Device** section to refine the table listing with the Search function.
4. From the device list, click the **Download** icon in the top-right.



5. The table listing will be exported as a single .CSV file in your browser's default download folder.

Firmware

From the Firmware window, you 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.

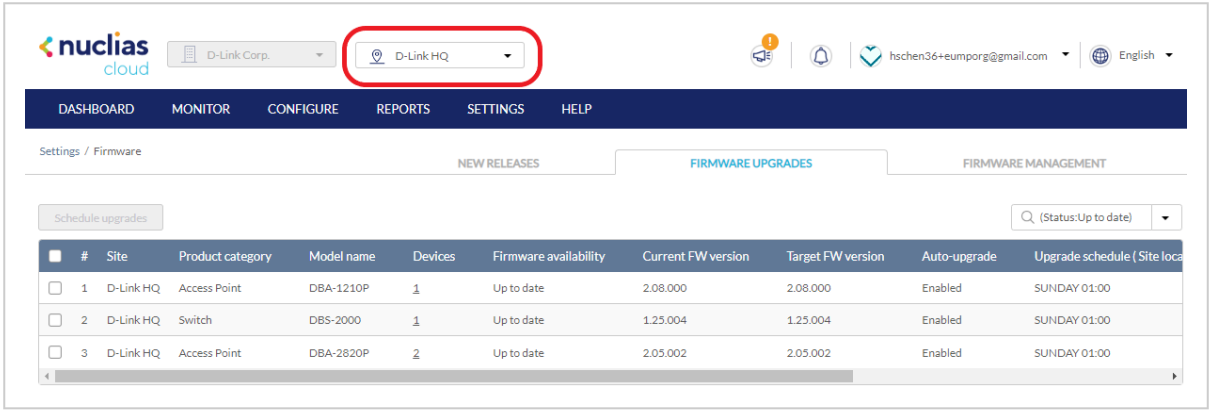


Notes: The Firmware page is only available to users with the Editor role and above.

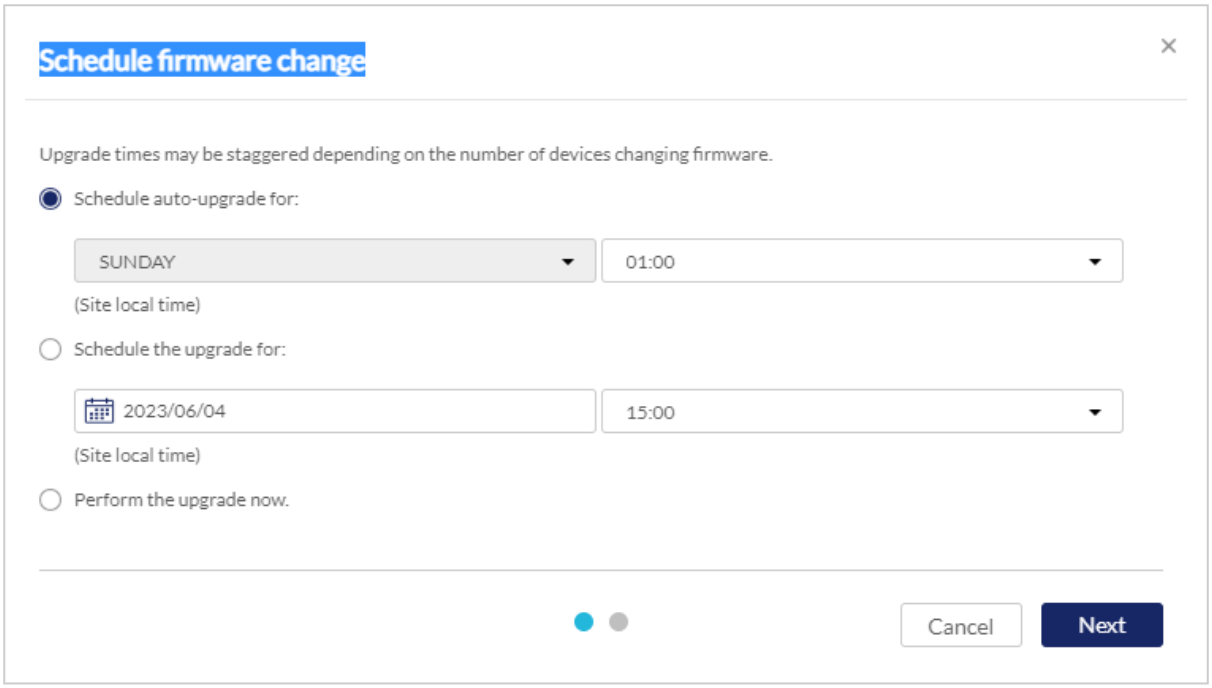
Setting an Automatic Upgrade

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.

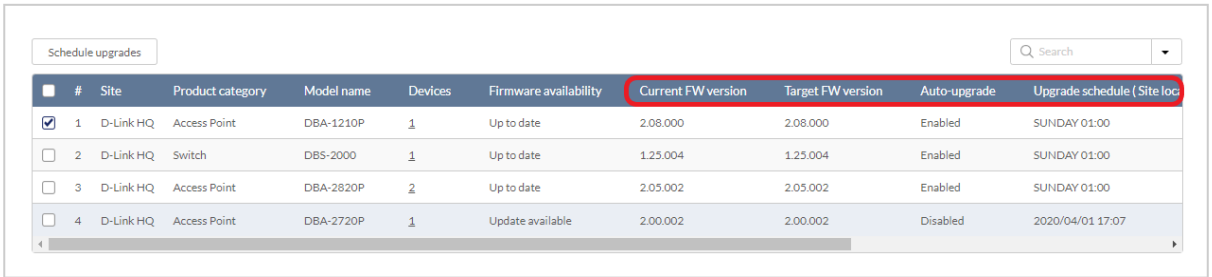
1. Navigate to **Settings > Firmware**.
2. Select a Site from the Site menu in the top of the screen.



3. Select a model from the list and click Schedule upgrades at the top left.
4. In the Schedule firmware change window, select the option Schedule auto-upgrade for: to set a automatic firmware upgrade schedule



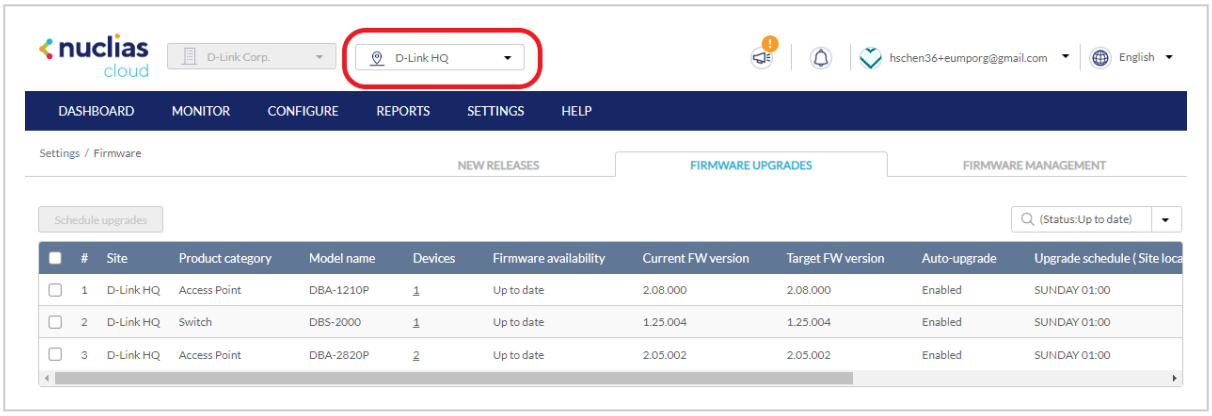
5. Select a day of a week and time of day from the drop-down menu. Select **Next** to continue.
6. Check the current firmware and the target firmware which will be the latest firmware set for the upgrade.
7. Click **Schedule changes** to confirm the upgrade. A result window will appear showing the settings of the schedule upgrade.
   The configuration will be reflected in the Current FW version, Target FW version, Auto-upgrade, and Upgrade schedule column of the FW upgrade list.



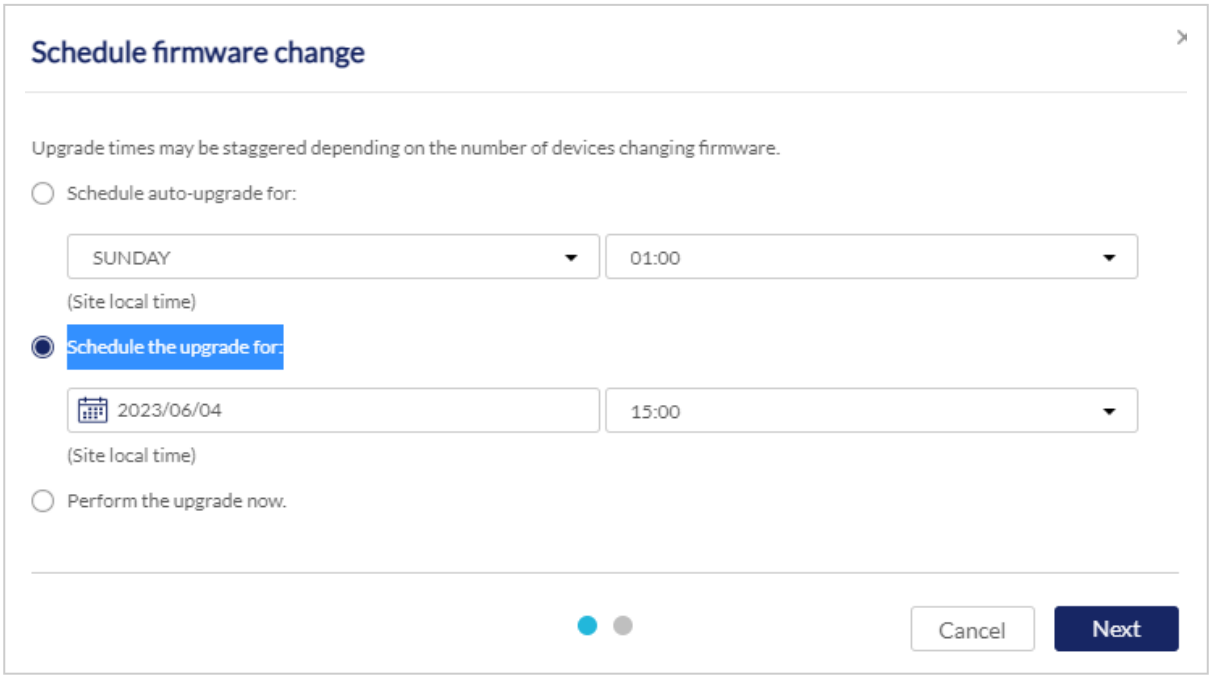
Setting a Custom Device Upgrade

You can define a specific time and date to scan for firmware updates which override 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 the Firmware Upgrades tab.
4. Select a model from the list and click Schedule upgrades.
5. In the Schedule firmware change window, select the option Schedule the upgrade for: to set a scheduled firmware upgrade with a desired firmware version for the designated device model.

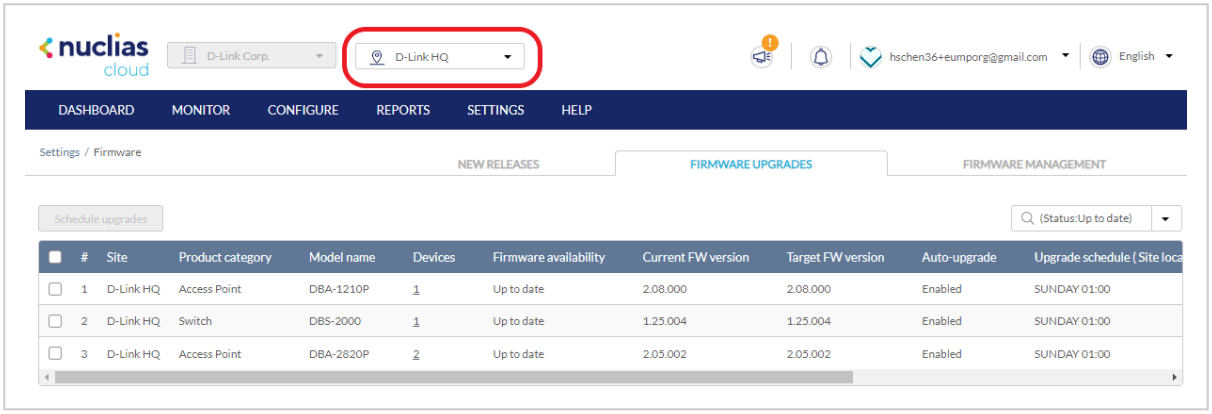


6. Select a day of a week and time of day from the drop-down menu. Then click **Next** to continue.
7. For Target FW versionSelect the desired firmware to upgrade to.
8. Click **Schedule changes** to confirm the upgrade. A result window will appear showing the settings of the schedule upgrade.
   The configuration will be reflected in the Current FW version, Target FW version, and Upgrade schedule column of the FW upgrade list.

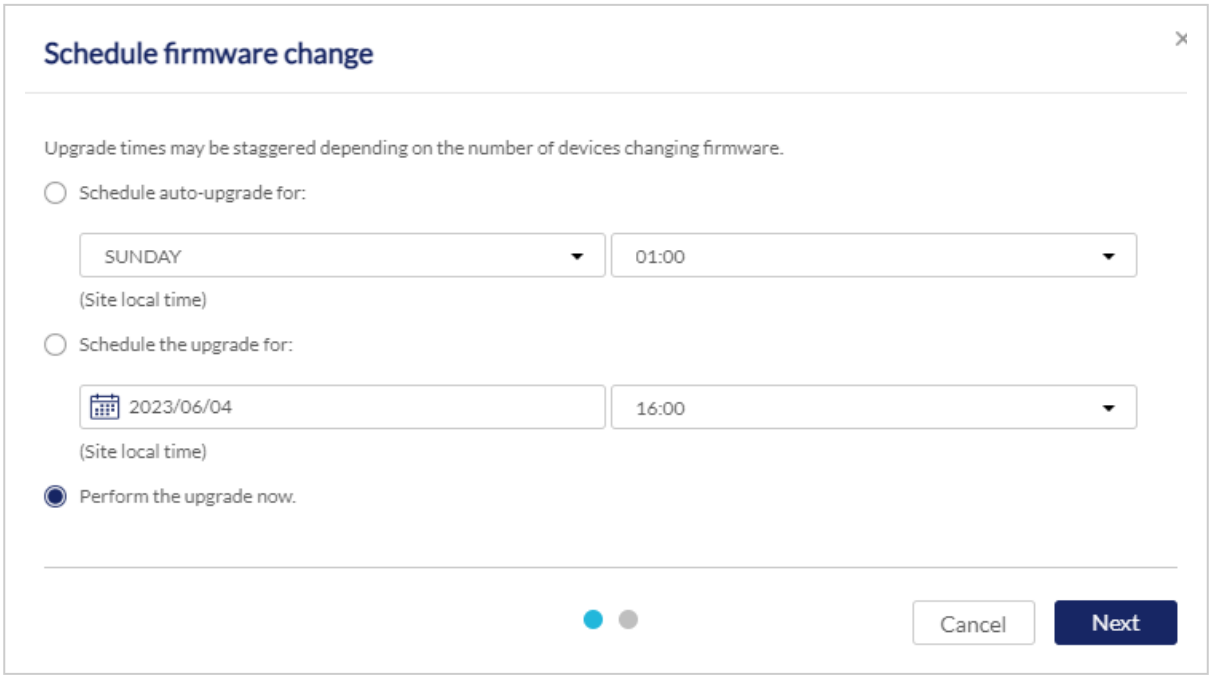
Performing a Manual Firmware Upgrade

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 the Firmware Upgrades tab.
4. Select a model from the list and click Schedule upgrades.
5. Select the option **Perform the upgrade now** to perform a manual upgrade now. Then click **Next** to continue.



6. Check the current firmware and select the target firmware to upgrade to.
7. Click **Schedule changes** to perform the upgrade immediately.
8. A result window which summarizes the upgrade task with the device and firmware information will be displayed. You can click Download at the top right to download the summary report in your local drive.

Getting Firmware Management Information

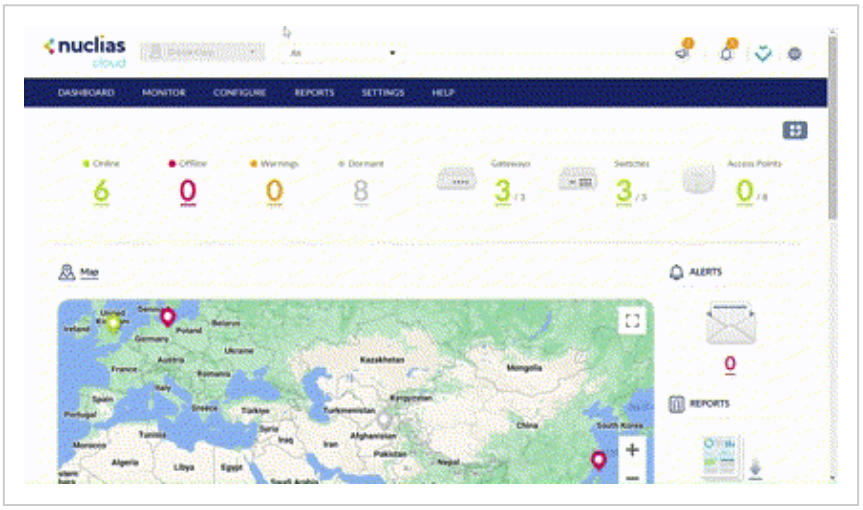
You can obtain the firmware management information such as the the update status, automatic upgrade schedule, availability of newer releases, and the last upgrade time. You can also customize the report and download it to your local drive.

To generate a firmware management report:

1. Navigate to **Settings > Firmware**.
2. Select the **Firmware Management** tab.
3. Select a model from the **Device Model** drop-down list to display data only for the model. Select **All** to display all models.
4. Select **Update Available** to display firmware that has new releases or **Up to Date** to display devices having up-to-date firmware. Select **All** to display both types.
5. Click **Preview** to display the results.
6. Click **Download** to download the displayed report as a single file in your browser's default download directory.

Alert Settings

New alerts will be displayed at the top right  to notify you after you log in. Alerts can also be accessed by clicking **Reports > Alerts**. You will also receive the configured alerts by email.



Note: Users of the Viewer role type cannot configure alert settings here and they are configured per user. Each user with the required editing rights within the organization can configure the types of alerts to be notified.

Configuring Alert Notifications

You can customize what types 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 Site-wide section, select the event types to receive alert notifications for:

Device Registry	A new device has been registered to a site and/or profile.
Device Firmware Has Upgraded Successfully	Sends an alert notification when a device firmware's version has successfully upgraded.
Device Firmware Upgrade Has Failed	Sends an alert notification when a device firmware upgrade failed.

Device Site and/or Profile Has Been Updated	Sends an alert notification when a device has been assigned to a different site or profile.
Device Has Connected to the Nuclias Cloud Successfully	Sends an alert notification when a device has successfully connected to Nuclias cloud.
Device Profile Configuration Has Been Applied Successfully	Sends an alert notification when a configuration update has been successfully pushed to affected devices.
Device Profile Configuration Update Has Failed	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 both the cloud portal (go to **Reports > Alerts)** and email 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 both the cloud portal (go to **Reports > Alerts)** and email whenever the device goes offline for longer than the selected time period.
5. Select **Any port** or a specific port from the drop-down menu, select a time (in minutes) from the drop-down menu, and check the respective checkbox to receive notifications by both the cloud portal (go to **Reports > Alerts)** and email whenever the selected port(s) (by port tags) are down for longer than the selected time period.)
6. In the Gateway section, select the event types to receive alert notifications for:

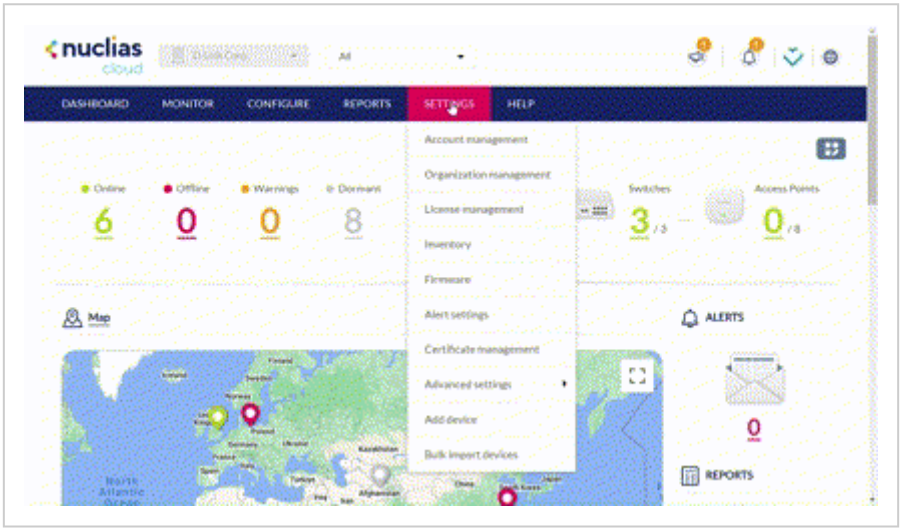
Gateway Has Been Offline for	Select a time (in minutes) from the drop-down menu, and check the respective checkbox to receive notifications by both the cloud portal (go to **Reports > Alerts)** and email whenever the device goes offline for longer than the selected time period.
A DHCP Lease Pool Falls Below 10%	Sends an alert notification when the available addresses of a DHCP lease pool falls below 10%.

An IPsec Tunnel Is Connected	Sends an alert notification when an IPsec tunnel is established.
An IPsec Tunnel Is Disconnected	Sends an alert notification when an IPsec tunnel is disconnected.
A WAN Port Is Connected	Sends alert notification when a WAN port of the device is connected.
A WAN Port Is Disconnected	Sends an alert notification when a WAN port of the device is disconnected.
Network Usage Exceeds	Sends an alert notification when the network volume exceeds the configured threshold value in a defined time frame.

7. Click **Save**.

Certificate Management

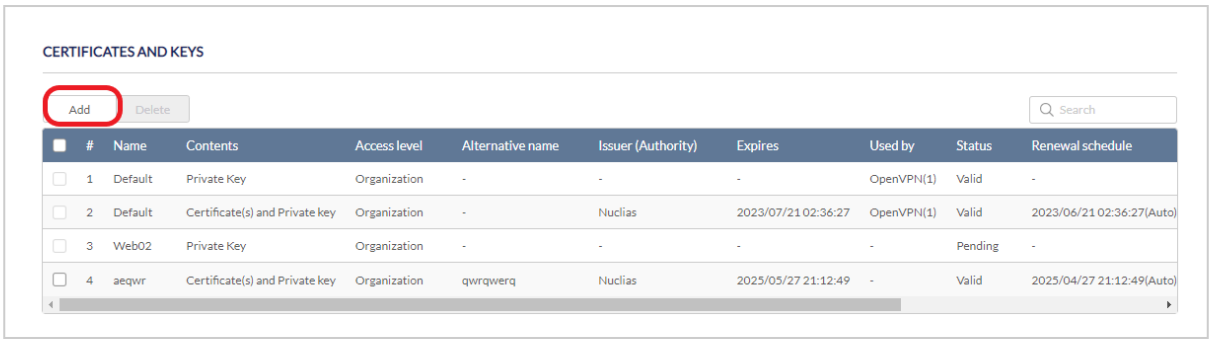
The Certificate window manages certificates that will be used in application authentication such as VPN and websites. You can obtain a digital certificate from a wellknown certificate authority (CA) such as VeriSign, or generate and sign your own certificate using the provided functionality. You can also upload certificates issued by a certificate authority (CA) or generate a certificate signing request (CSR) to pass it to the CA for signing.



Adding Certificates

A certificate can be added to the organization so it can be can be used by an application that requires secure communication.

1. Navigate to **Settings > Certificate Management**.
2. In the Certificates and Keys table, click **Add**.



3. Select the type of certificate to be generated or import a certificate.
4. If you wish to issue certificate signing request, enter the required information:

Common Name	Enter a name for the certificate.
Alternative Name	Enter an alternative name for the certificate.
Signed by	Select the certificate authority.

5. If you would like to generate a certificate by uploading a Certificate Signing Request file, enter the following:

Signed by	Select the certificate authority.
Upload Certificate Signing Request (CSR)	Click Browse to upload a CSR file.

6. If you would like to import a certificate to the database, choose one of the following:

Upload PEM-encoded Private key	Click Browse to upload a PEM-encoded private key (a PEM file).
Upload PEM-encoded Certificate	Click Browse to upload a PEM-encoded certificate (a PEM file).
Upload PEM-encoded Certificate Chain	Click Browse to upload a PEM-encoded certificate chain (a PEM file that contains one or more certificates).

7. If you would like to generate a private key using Diffie–Hellman key exchange (DH) or Transport Layer Security (TLS) encryption, enter the following:

Key Name	Enter a name for the key.
Key Type	Select either DH or TLS encryption method.
Key Size	Select the key size in bits.

8. If you would like to import a private key with Diffie–Hellman key exchange (DH) or Transport Layer Security (TLS) encryption, enter the following:

Key Name	Enter a name for the key.
Upload Your Private Key	Click Browse to upload your private key file.

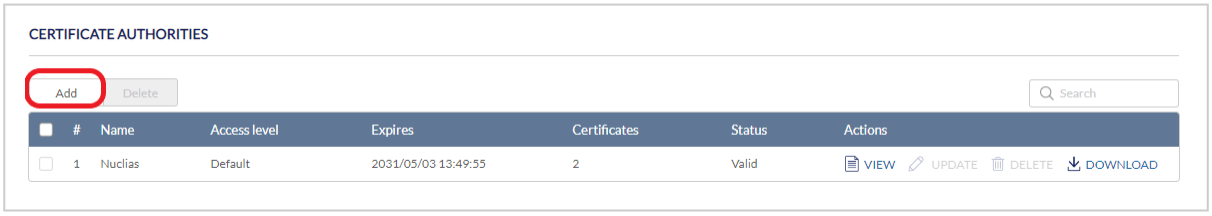
9. Select Access level to specify the accessibility of the generated certificate or key in the organization.
10. Click **Save**.

Adding Certificate Authorities

You can manage the certificate issuing authorities in the certificate database.

To add a certificate authority:

1. Navigate to **Settings > Certificate Management**.
2. In the Certificate Authorities table, click **Add**.



3. Select the Access level for the accessibility of the CA in the organization
4. Upload your RSA private key in unencrypted PEM format for the certificate authority (CA)*
5. Upload your X.509 certificate in PEM format for the certificate authority (CA)*
6. Click **Save**.

Searching for a Certificate

The Certificates and Keys list allows you to view a list of certificates (both from a CA and self-signed) currently loaded on the system. The following certificate data is displayed in the list:

Name/Alternative Name	The Name/Alternative Name of the certificate.
Contents	Whether this is a private key or certificate or both.
Accessl Level	The accessibility level of this certificate.
Issuer Name	The CA name that issued this certificate.
Expiry	The date after which this certificate becomes invalid
Used by	The VPN configuration with IKE profiles that uses this certificate.
Status	Whether this is valid.
Renewal schedule	The planned renewal time for this certificate.
Actions	Click View, Update, Delete, or Download to perform the respective opertion on the certificate.

To search for a certificate:

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

2. Enter a keyword in the search field at the top right of the Certificate Table or Certificate Authorities Table to search for all fields.

   All certificate or keys matching the value entered in the field will automatically appear.

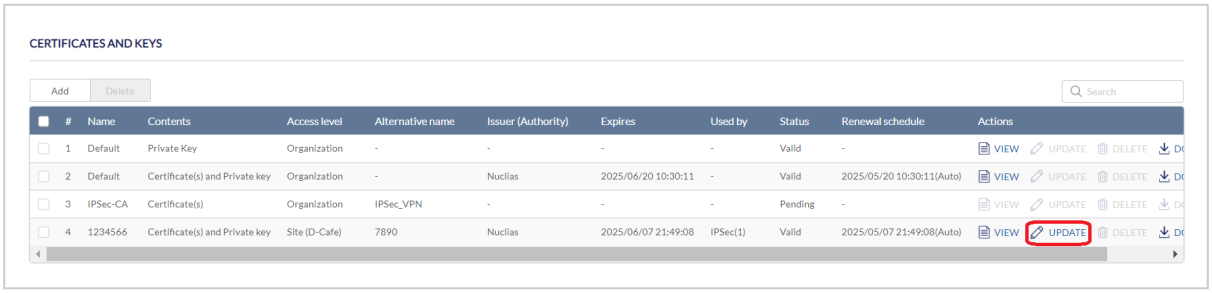
Viewing the Certificate Information

1. Navigate to **Settings > Certificate Management.**
2. From the Certificate or Certificate Authorities list, select desired entry, then click **View** to view more information about the content of the certificate or key.



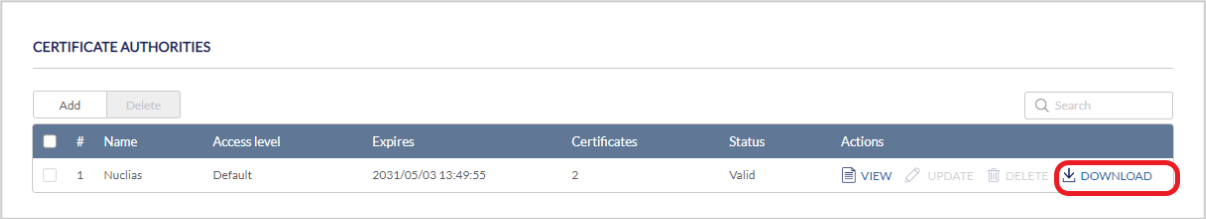
Updating the Certificate Information

1. Navigate to **Settings > Certificate Management.**
2. From the Certificate or Certificate Authorities list, select desired entry, then click Update to renew an expiring certificate or replace an invalid certificate or regenerate a private key.



Downloading Certificate or Key Files

1. Navigate to **Settings > Certificate Management**.
2. From the Certificate or Certificate Authorities list, select the desired entry, then click **Download** to download a certificate file or private key file in PEM format.



Managing Local User Certificates

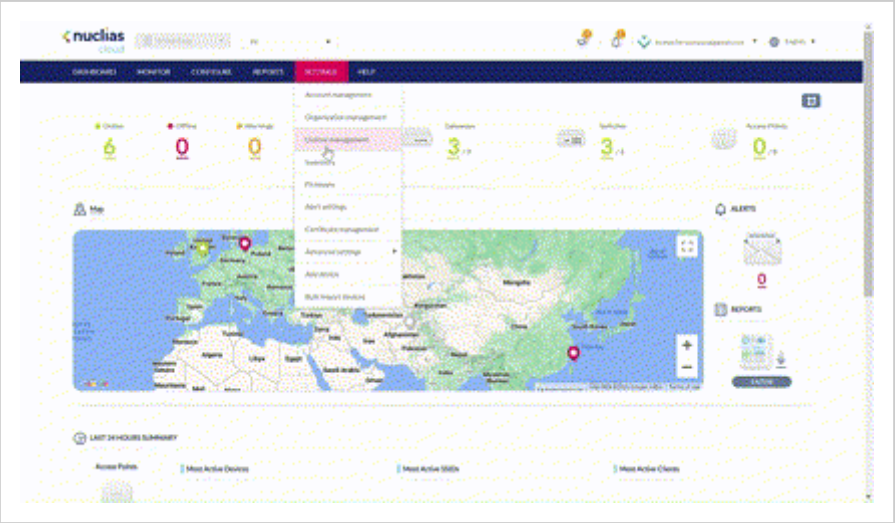
Local User Certificates used for OpenVPN server settings can be revoked or resumed its validity. Go to the Client List in **VPN > Open VPN** in Device Configuration page of a gateway .

1. Navigate to **Settings > Certificate Management**.
2. From the Local User Certificates list, select the desired entry, then click **Download** to download a local user certificate file. To revoke a local user certificate, select the desired entry, then click **Revoke** to revoke the certificate. To resume the certificate's validity, click **Resume**.

   After a local user certificate is added successfully, you can reference where the certificate is applied in OpenVPN profiles by clicking the **Used by** field in the table.

Advanced Settings

The Advanced Settings provide configuration menus for Security Assertion Markup Language (SAML), SMS and Syslog Server.



Note: The Advanced Settings page is only available to users with the editor role and above.

SAML Configuration

Security Assertion Markup Language (SAML) is an XML standard used for the exchange of user authentication data. With SAML authentication, single sign-on (SSO) experience can be achieved across application service domains between an identity provider (IdP) and Nuclias Cloud.

Before you can set up SSO via SAML, please obtain identity provider (IdP) information by visiting their the help centers. For example, Set up your own custom SAML application from Google.

To enable SAML on the system:

1. Navigate to **Settings > Advanced settings > SAML Configuration.**
2. Select **Enable** SAML SSO. The Entity ID (a globally unique name) and URL (Assertion Consumer Service URL) of the service provider (Nuclias) is displayed.
3. Click **Add** to add a trusted identity provider (IdP) and enter the following information:

URL	Enter the sign-on URL from the IdP.
Issuer	Enter the name or URI of the issuer.

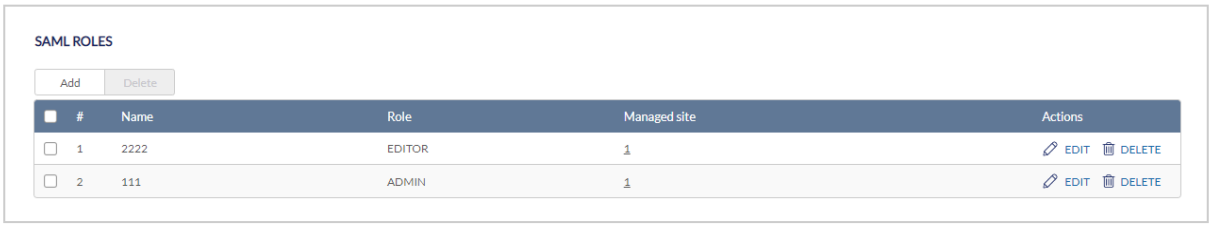
Certificate	Upload a PEM certificate from the IdP.
Logout URL	When users log out, this URL is used for web redirection.
X.509 Cert SHA1 Fingerprint	The x509 certificate is used to establish trust communication with the IdP.
Import IdP Metadata	Besides the above method of manual IdP configuration, you can also use the import method. Enter an IdP information by importing an IdP metadata XML file downloaded from the IdP.

4. Click **Save**.

Creating SAML Roles

After establishing a connection with an external IdP, you can grant access permissions to this SAML user by assigning roles and access level.

1. Navigate to **Settings > Advanced settings > SAML Configuration.**
2. In the SAML Roles section, click **Add** to add a new SAML role.



3. In the Add a SAML role window, enter the following information.

Name	Enter a name for this user authenticated through SAML (1-64 characters).
Access Privilege/ Role	Select the role to determine the access privilege level of this SAML user.
Managed Site	Select which Sites of the organization can be viewed by the user.

4. Click **Save**.

SMS Configuration

Short Message Service (SMS) containing one-time password can be sent from the system using Twilio SMS. The SMS authentication is used for user request for network access in Captive Portal configuration.

To configure SMS authentication service:

1. Navigate to **Settings > Advanced settings > SMS configuration.**
2. Click **Add Twilio SMS settings.**
3. In the Add Twilio SMS settings window, enter the following:

Name	A name that identifies this account setting (1-64 characters).
Twilio Account SID	Your Twilio account SID (1-64 characters).
Twilio Auth Token	The authentication token (1-128 characters).
Twilio from Number	The number registered with Twilio.
Resend after (minutes)*	Enter the resend interval in minutes (0-60 minutes). 0 means that it can be resent immediately.
Maximum Resend (times)	Maximum number of times that the one-time password can be resent. 0 means it can only be sent once (0-60).
Maximum Request (times)	Maximum number of times a new one-time password can be requested. 0 means it can make unlimited requests (0-60).
Denial Period (minutes)	The length of time that clients must wait before they can request a one-time password after the above resend and request limits are reached (0-1440 minutes).
OTP Expires (minutes)	The length of time that a one-time password is valid (5-30 minutes).
Allowed Phone Prefix	Country calling codes that are permitted to use SMS. Separate the codes with “,” (e.g. +81,+91,+886). “*” means all codes are permitted.

Access Level	Select level of accessibility for this account setting.

4. Click **Save**.

Syslog Server Configuration

You can configure the system to send syslog messages to an external syslog server.

To configure a syslog server:

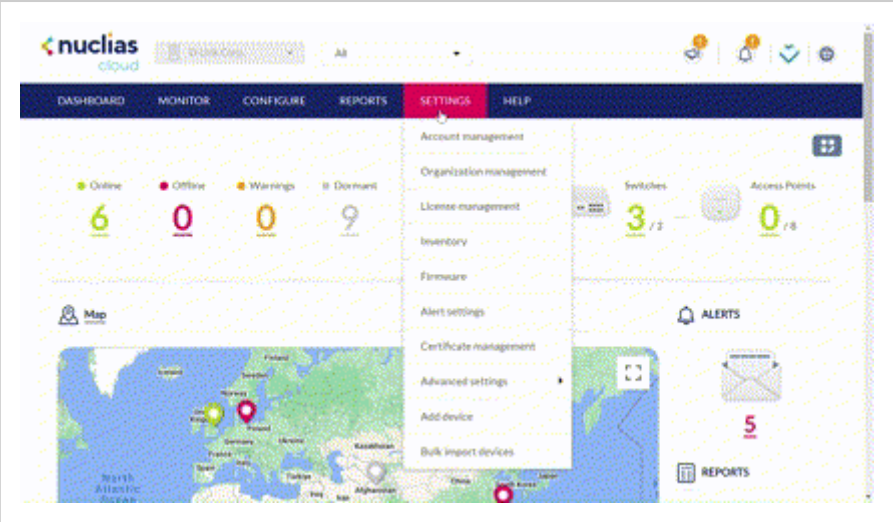
1. Navigate to **Settings > Advanced settings > Syslog server configuration.**
2. Click **Add.**
3. In the Add Syslog server settings window, enter the following:

Name	A name that identifies this syslog setting.
Syslog Server	Enter the syslog server's IP address or FQDN.
Syslog Server Port	The port used for the syslog service.
Protocol	The protocol to communicate with the syslog server.
Select Site	Select the site to allow for the syslog service.

4. Click **Apply**.

Add Device

Adding new devices to the Inventory without Site and Profile assignment keeps them inactive. If you wish to add devices with only UID information and register them at a later point, go to **Settings > Inventory** instead.



Note: The Add Device page is only available to users with the Admin role.

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

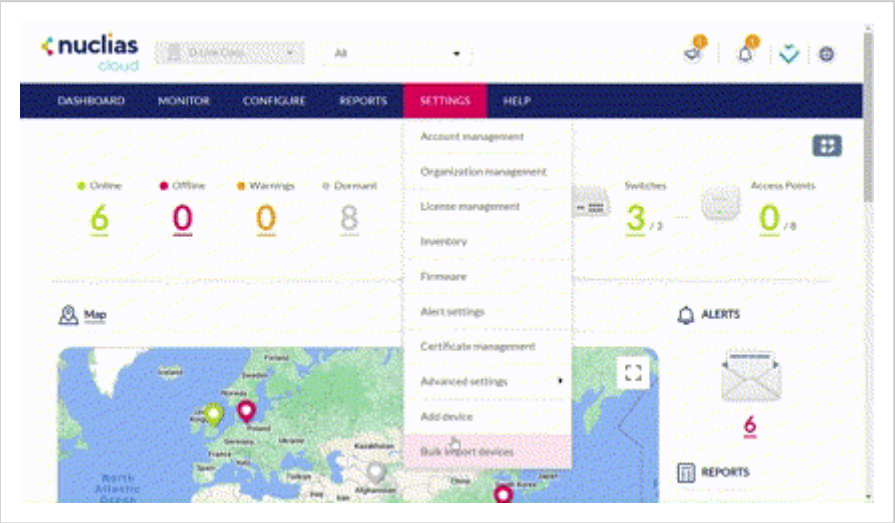
Device UID	Enter the device's Unique Identifier (UID) found on the label printed on the device. The UID may be listed in the format **XXXX-XXXX-XXXX** or **XXXXXXXXXXXX**. When entering the UID, do not include dashes.
Device Name	Enter a name for the device to easily find the desired device.
Site	Select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

Profile	Select a Profile for this device to apply that Profile's configuration settings. Click on the drop-down menu to display a list of available profiles for your model.
License Key	**[Optional]** Enter the license key. Click on the drop-down menu to display a list of available licenses for this device type. **Note:** Every new device will be issued a one year complimentary license key. You may add more license keys to extend the period of use. Once expired, an additional license must be purchased to continue using this device.

3. Click **Save**.

Bulk Import Devices

Devices can be bulk imported to the Inventory with basic configuration and registration information.



Note: The Bulk Import Devices page is only available to users with the Admin role.

Bulk Assigning Devices with Configuration

1. Navigate to **Settings > Bulk import devices**.
2. [Optional] Download the reference sample template. Note that you can add up to 1,000 devices for a single import.
3. Click **Browse**.
4. Locate the CSV file containing the UIDs and other required information such as Site and Time Zone (you can also enter Profile assignment and License keys for device registration) as shown in the following example:

UID	Device name	Site	Time Zone	Profile	License-1	License-2	License-3
FFFFEEEE0001	DBS	Taipei	Asia/Taipei				
FFFFEEEE0002	DBA	Hsinchu	Asia/Taipei				
FFFFEEEE0003	DBG	Hsinchu	Asia/Taipei				

5. Click **Upload**.

Help

Contact Technical Support

From the Contact Technical Support window, you 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 Technical Support

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

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

5. Our local technical support center will reply to the submitted case once received.

Troubleshooting

From the Troubleshooting page, you can allow the Nuclias Cloud support team to access your organization and site information.

Allow Nuclias Support

1. Navigate to **Help > Troubleshooting**.
2. Select to either Enable or Disable the support feature of Nuclias Cloud. If enabled, the Nuclias team will be able to access this organization and its sites. You will need to enable this feature to receive assistance.
3. When enabled, you will be provided a PIN code that the Nuclias team can use to access your account and help troubleshoot.

Tutorials

From the Tutorials tab, you will be navigated to the Nuclias Cloud tutorial video page which has instructional videos on how to complete various management tasks within Nuclias Cloud.

Navigate to **Help > Tutorials**.

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 App

The Nuclias App is available for iPads and Android tablets. 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 app from the App Store or Google Play Store, open the application and you will be prompted to enter your Nuclias Cloud account's email and password to log in to your Nuclias Account.

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

Cloud - Supported Devices

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 Smart Antenna Access Point



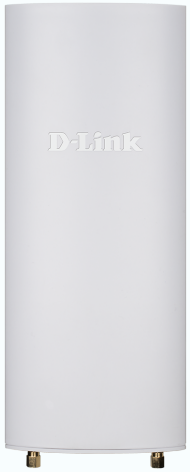
DBA-2720P

Nuclias Cloud Managed AC2200 Wave 2 Tri-Band 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



DBA-X2830P

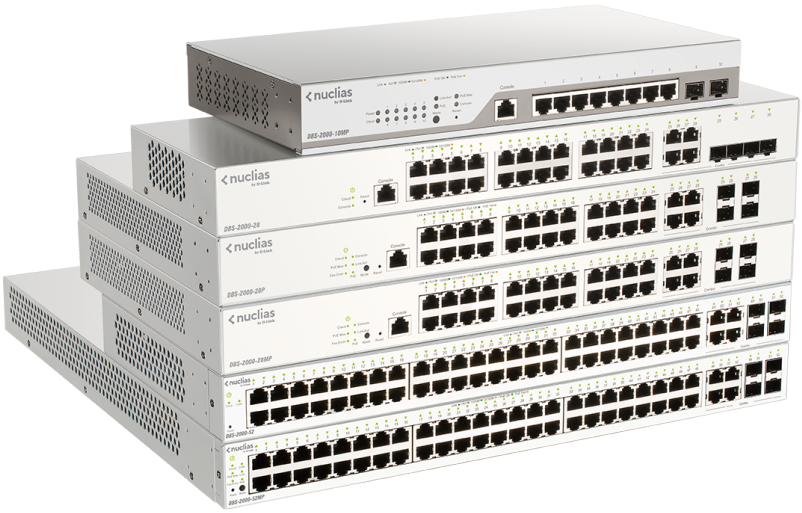
Nuclias Cloud Managed AX3600 Access Point



DBA-X1230P

Nuclias Cloud Managed AX1800 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



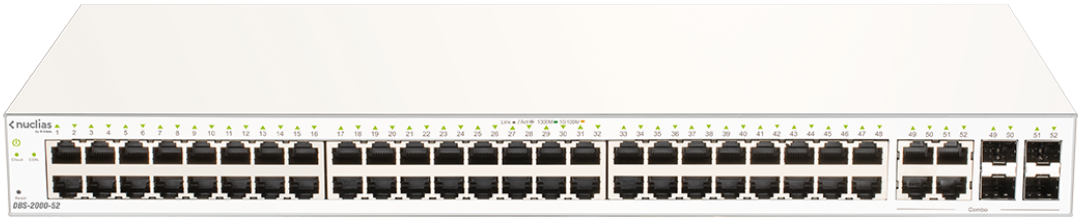
DBS-2000-28MP

28-Port Nuclias Cloud-Managed PoE Switch



DBS-2000-28P

28-Port Nuclias Cloud-Managed Switch



DBS-2000-52

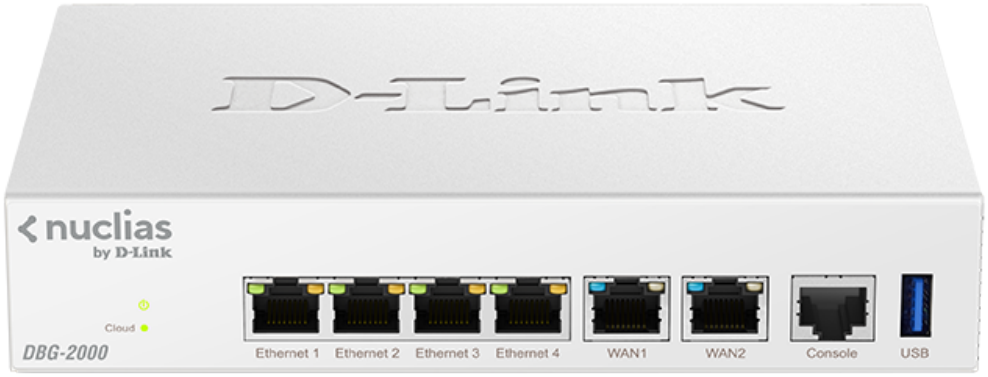
52-Port Nuclias Cloud-Managed Switch



DBS-2000-52MP

52-Port Nuclias Cloud-Managed PoE Switch

Gateways



DBG-2000

Nuclias Cloud SD-WAN Security Gateway



DBG-X1000

Nuclias Cloud Business Gateways