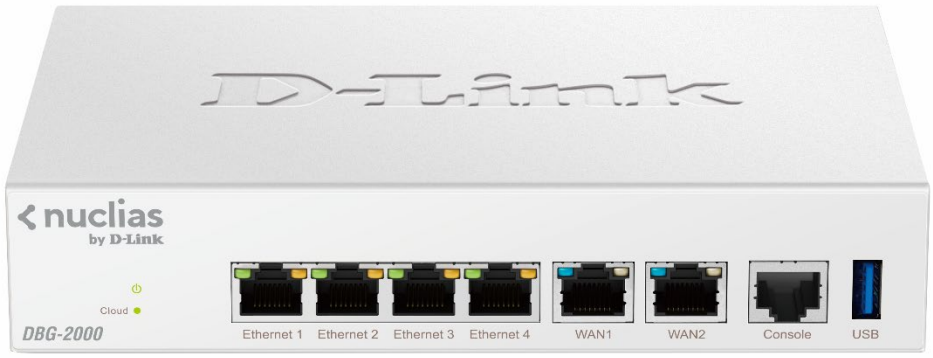
Version 2.2.0.9 | 11/21/2023



User Guide

Nuclias Cloud Gateway

DBG-2000

User Guide

D-Link Nuclias Cloud Gateway, DBG-2000, offers multiple features to be utilized for networking applications. However, to work with the device efficiently, you must understand the functionality of the device. For that, we would recommend you to read the User Guide. The user guide includes details of all the fields appearing on every page of the device user interface.

Version V2.2.0.9

Expand all Collapse all

Preface

The information here is subject to change without notice. The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the manufacturer to notify any person of such revision or changes.

Copyright notice

Limitations of Liability

UNDER NO CIRCUMSTANCES SHALL D-LINK OR ITS SUPPLIERS BE LIABLE FOR DAMAGES OF ANY CHARACTER (E.G. DAMAGES FOR LOSS OF PROFIT, SOFTWARE RESTORATION, WORK STOPPAGE, LOSS OF SAVED DATA, OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES) RESULTING FROM THE APPLICATION OR IMPROPER USE OF THE D-LINK PRODUCT OR FAILURE OF THE PRODUCT, EVEN IF D-LINK IS INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. FURTHERMORE, D-LINK WILL NOT BE LIABLE FOR THIRD-PARTY CLAIMS AGAINST CUSTOMER FOR LOSSES OR DAMAGES. D-LINK WILL IN NO EVENT BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE AMOUNT D-LINK RECEIVED FROM THE END-USER FOR THE PRODUCT.

Safety Instructions

To reduce the risk of physical injury, electrical shock, fire, and damage to the equipment, observe the following precautions:

- Observe and follow the service markings.
  - Do not service any product except as explained in your system documentation. For example, opening or removing covers marked with the triangular symbol with a lightning bolt may expose you to electrical shock.
  - Only a trained service technician should service components inside these compartments.
- If any of the following conditions occur, unplug the product from the electrical outlet and replace the part or contact your trained service provider:
  - The power cable, extension cable, or plug is damaged.
  - An object has fallen into the product.
  - The product has been exposed to water.
  - The product has been dropped or damaged.
  - The product does not operate correctly when you follow the operating instructions.
- Keep your system away from radiators and heat sources. Also, do not block cooling vents.
- Do not spill food or liquids on your system components, and never operate the product in a wet environment. If the system gets wet, see the appropriate section in your troubleshooting guide or contact your trained service provider.
- Do not push any objects into the openings of your system. Doing so can cause fire or electric shock by shorting out interior components.
- Use the product only with approved equipment.
- Allow the product to cool before removing covers or touching internal components.

- Operate the product only from the type of external power source indicated on the electrical rating label. If you are not sure of the type of power source required, consult your service provider or local power company.
- Also, be sure that the attached devices are electrically rated to operate with the power available in your location.
- Use only approved power cable(s). If you have not been provided with a power cable for your system or for any AC-powered option intended for your system, purchase a power cable that is approved for use in your country. The power cable must be rated for the product and the voltage and current marked on the product's electrical rating label. The voltage and current rating of the cable should be greater than the rating marked on the product.
- To help prevent electric shock, plug the system and peripheral power cables into properly grounded electrical outlets.
- These cables are equipped with three-prong plugs to help ensure proper grounding. Do not use adapter plugs or remove the grounding prong from a cable. If you must use an extension cable, use a 3-wire cable with properly grounded plugs.
- Observe extension cable and power strip ratings. Make sure that the total ampere rating of all products plugged into the extension cable or power strip does not exceed 80% of the ampere rating limit for the extension cable or power strip.
- To help protect your system from sudden, transient increases and decreases in electrical power, use a surge suppressor, line conditioner, or uninterruptible power supply (UPS).
- Position system cables and power cables carefully; route cables to not be stepped on or tripped over. Be sure that nothing rests on any cables.
- Do not modify power cables or plugs. Consult a licensed electrician or your power company for site modifications.
- Always follow your local/national wiring rules.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:
    - Install the power supply before connecting the power cable to the power supply.
    - Unplug the power cable before removing the power supply.
    - If the system has multiple power sources, disconnect power from the system by unplugging all power cables from the power supplies.
- Move products with care; ensure that all casters and/or stabilizers are firmly connected to the system. Avoid sudden stops and uneven surfaces.

Protecting Against Electrostatic Discharge

Static electricity can harm delicate components inside your system. To prevent static damage, discharge static electricity from your body before touching any of the electronic components, such as the microprocessor. You can do so by periodically touching an unpainted metal surface on the chassis.

You can also take the following steps to prevent damage from electrostatic discharge (ESD):

- When unpacking a static-sensitive component from its shipping carton, do not remove the component from the antistatic packing material until you are ready to install the component in your system. Just before unwrapping the antistatic packaging, be sure to discharge static electricity from your body.
- When transporting a sensitive component, place it in an antistatic container or package.
- Handle all sensitive components in a static-safe area. If possible, use antistatic floor pads, workbench pads, and an antistatic grounding strap.

Getting Started

Version: V2.2.0.9

The user guide of the D-Link Nuclias Cloud Gateway DBG-2000 includes information about all the features supported by the gateway. However, before reading about the features, you must know how to use and install the gateway, its features, and where to navigate for what. You will get a complete overview of these items and will also learn about the configuration of a few parameters in this section.

Introduction

D-Link Nuclias Cloud Gateway DBG-2000 offers a secure, high-performance, cloud-based networking solution to address the growing needs of small and medium businesses. Optimal network security is provided via features such as virtual private network (VPN) tunnels, IP Security (IPSec), Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and OpenVPN. Empower your road warriors with remote access anywhere and anytime using OpenVPN tunnels. With the D-Link Nuclias Cloud Gateway, DBG-2000, you can experience a diverse set of benefits.

- **Comprehensive Management Capabilities**
  The DBG-2000 includes WAN-Gigabit Ethernet, which provides policy-based service management ensuring maximum productivity for your business operations. The *failover* feature maintains data traffic without disconnecting when a landline connection is lost. The *Outbound Load Balancing* feature adjusts outgoing traffic across WAN interfaces and optimizes the system performance resulting in high availability. In addition, the solution supports configuring a port as a dedicated DMZ port allowing you to isolate servers from your LAN.
- **Zero-touch Provisioning**
  DBG-2000 is a cloud-supported gateway that gets synchronized with the cloud to attain its full functionalities. The D-Link Nuclias Cloud can virtually manage the widely deployed gateways and push configuration to them instantly. Also, the feature of configuring and associating profiles to multiple deployed gateways of an organization helps them to run with the same configuration.
- **Robust VPN features**
  A fully-featured virtual private network (VPN) provides your mobile workers and branch offices with a secure link to your network. DBG-2000 can manage multiple VPN tunnels simultaneously, empowering your mobile users by providing remote access to a central corporate database. Site-to-site VPN tunnels use IP Security (IPSec) Protocol, Point-to-Point Tunneling Protocol (PPTP), or Layer 2 Tunneling Protocol (L2TP) to facilitate branch office connectivity through encrypted virtual links. Hub and Spoke is a new Site-to-site topology that designates one DBG-2000 gateway as the “Hub” and all the remote sites as the “Spokes.” Hub-and-Spoke mode is beneficial in organizations where several auxiliary sites require a connection to the HQ. With this topology, the communication between the two sites could take place only through the Hub. This way, the Hub is always informed whenever two sites communicate with each other.

DBG-2000 Quick Start Guide

The DBG-2000 Quick Start Guide consists of the following topics:

Installation

Unpack the product

Open the shipping carton and carefully unpack its contents. Please consult the following packing list to make sure that all the items are present and undamaged. If any item is missing or damaged, please contact your local D-Link reseller for a replacement.

- One (1) DBG-2000 Nuclias Cloud Gateway
- One (1) Power adapter
- One (1) Console Cable (RJ-45 to DB-9 Cable)
- One (1) Ethernet (CAT5 UTP/Straight-Through) Cable
- One (1) Quick Installation Guide
- Two (2) Rack Mounting Brackets

Before you Begin

Ensure that you follow the precautions given below to prevent shutdowns, equipment failures, and injuries:

- Ensure that the room in which you operate the device has adequate air circulation and that the room temperature does NOT exceed 40C (104F).
- Allow 1 meter (3 feet) of clear space to the front and back of the device.
- Do NOT place the device in an equipment rack frame that blocks the air vents on the chassis sides. Also, ensure that enclosed racks have fans and louver sides.
- Before installation, please correct the following hazardous conditions: moist or wet floors, leaks, ungrounded or frayed power cables, or missing safety grounds.

Connect to your Network

The basic information about physically connecting the DBG-2000 to a network is as follows:

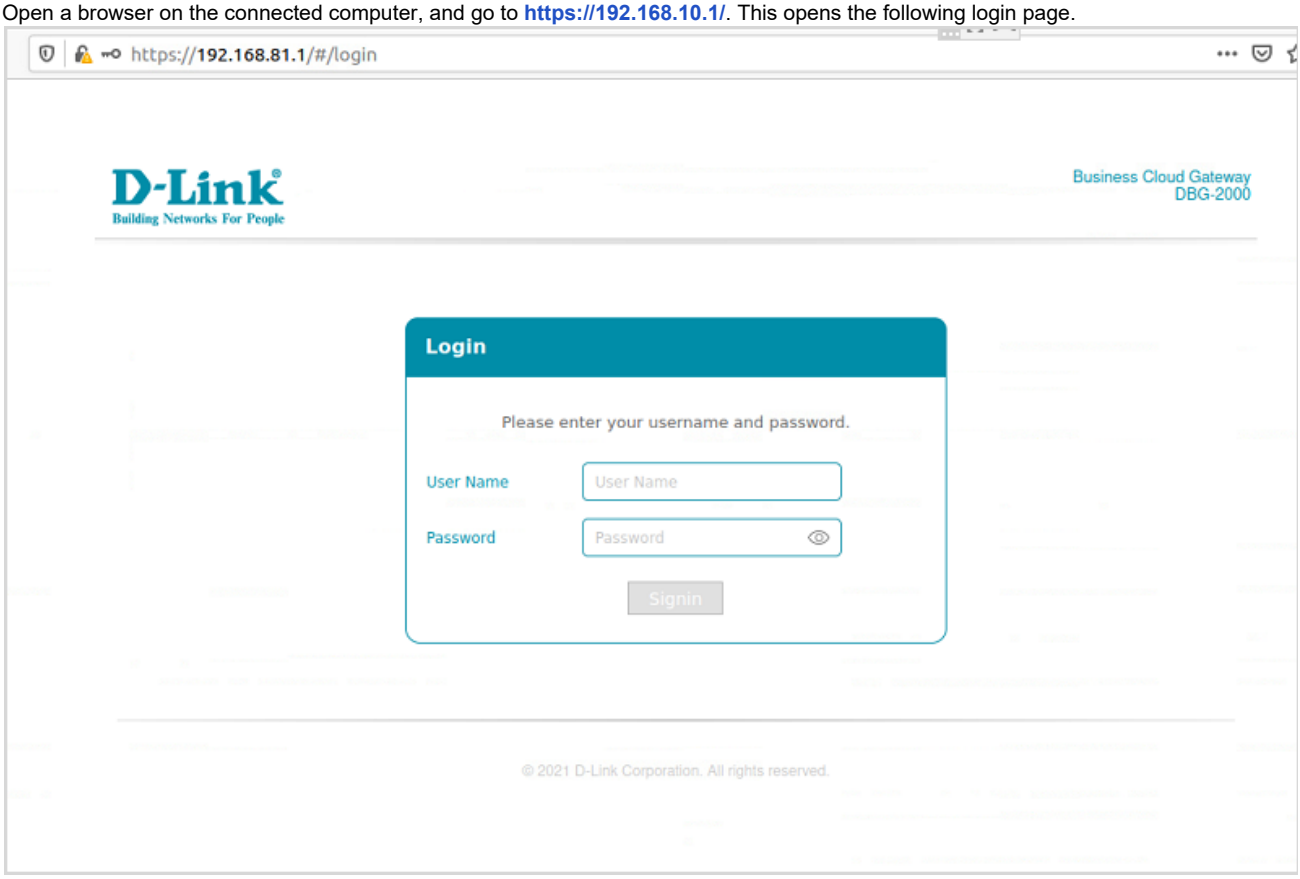
- Connect an Ethernet cable from the port labeled Ethernet 1 to the external router, modem, or ISP. The port Ethernet 1 is allocated to the WAN network segment.
- Connect an Ethernet cable from one of the LAN ports (Ethernet 2, Ethernet 3, or Ethernet 4) to a switch or a computer in the LAN network segment.

System Requirements

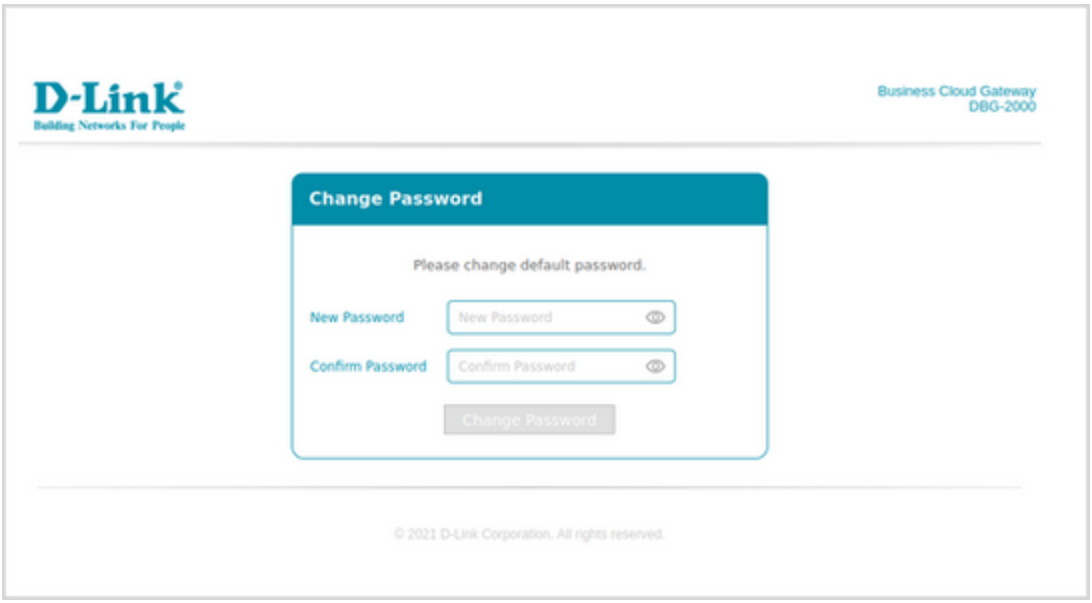
- A broadband Internet connection
- A computer with any of the following browsers:
  - Microsoft Internet Explorer (Version 9.0 or higher)
  - Mozilla Firefox (Version 20 or higher)
  - Opera (Version 77.0 or higher)
  - Apple Safari (Version 5.0 or higher)
  - Google Chrome (Version 25 or higher)

Web-based Setup

1. Open a browser on the connected computer, and go to **https://192.168.10.1/**. This opens the following login page.



2. Enter **admin** as your username and **admin$123** as the password.
3. If you are logging in for the first time and the device is not synchronized with the Nuclias cloud, you will be redirected to the **Change Password** page. You must change the default password and enter a new password. If the device is Nuclias cloud synchronized, you cannot change the password.



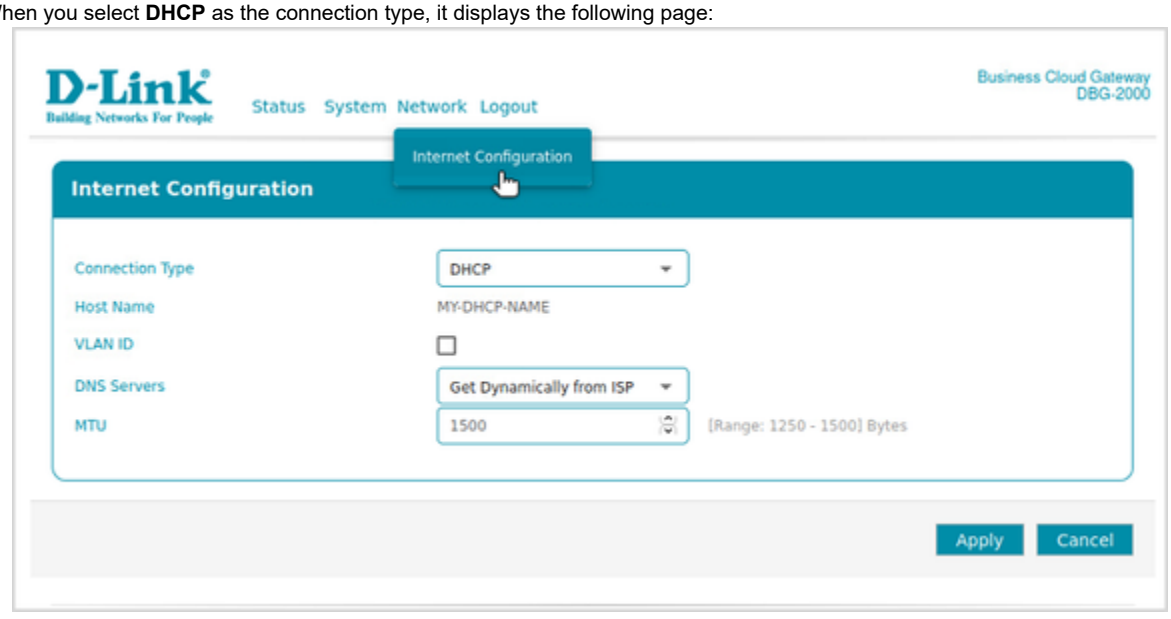
4. Enter your new password and re-enter it to confirm the new password.
5. Click **Change Password**.
6. If the device is synchronized to the Nuclias cloud before logging in to the device, the user is not redirected to the “Change password” page. Instead, the user can directly log in with the Nuclias cloud UI password for the associated profile.
7. After successful login, the **Overview** page will appear.

How to connect your device to the Internet?

To get connected to the Nuclias cloud, you must configure the Internet configuration.

Note: *Ethernet 1 and Ethernet 4 ports are configured as default WAN and LAN ports, respectively.*

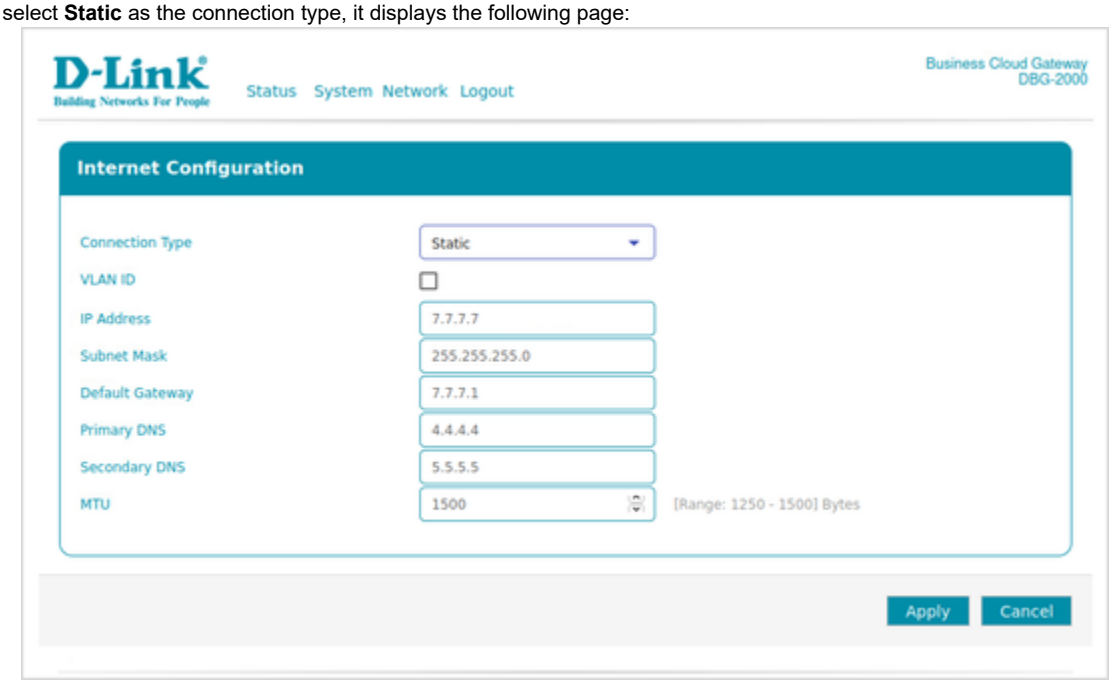
1. Go to the **Network** menu, and click **Internet configuration**.
2. Select the connection type based on your ISP from the drop-down list. The options are DHCP, Static, PPTP, L2TP, and PPPoE.
3. Enable or disable the VLAN ID on the configured WAN port. If you enable the VLAN ID, enter the **VLAN ID**.
4. Enter details as per the selected connection type.
    a. When you select **DHCP** as the connection type, it displays the following page:



Fields	Description
DHCP	

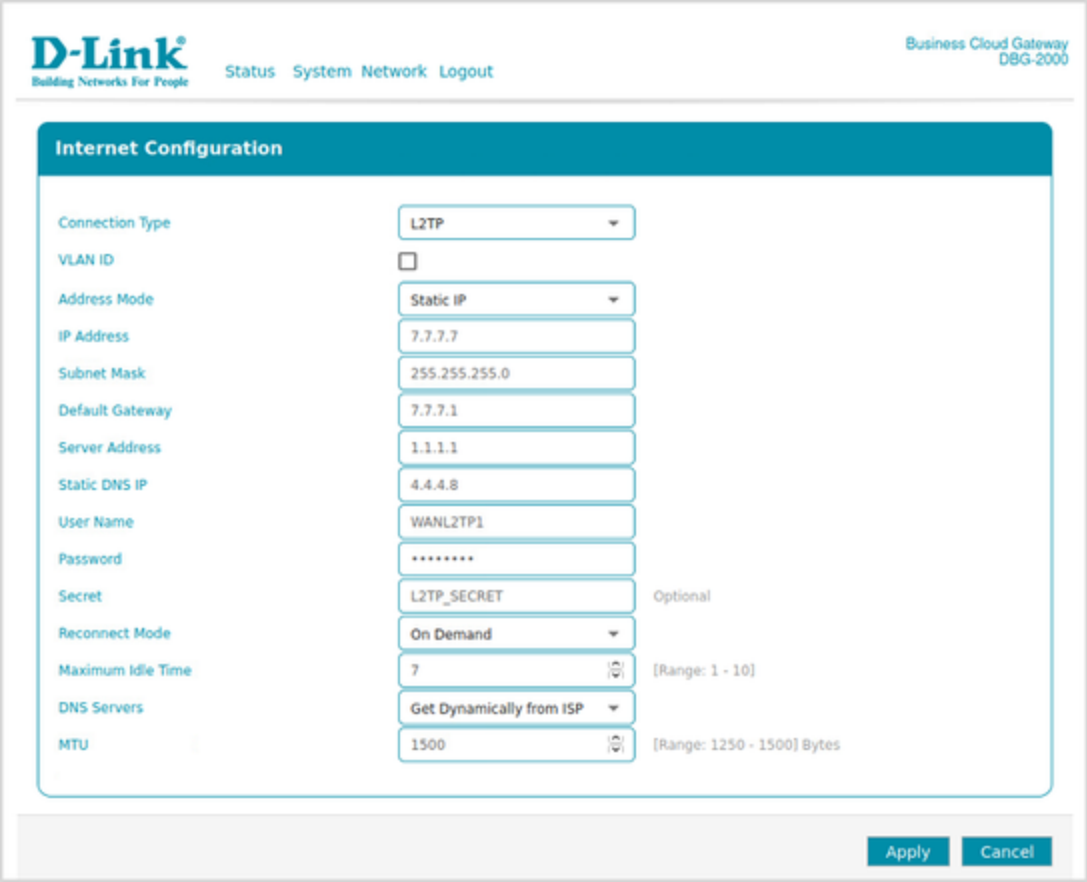
Hostname	Enter the hostname if required by your ISP.
DNS Servers	Select either **Get dynamically from ISP** or **Use these DNS servers** to enter DNS servers manually.
Primary DNS	If you select **Use these DNS servers**, enter the primary DNS server IP address.
Secondary DNS	If you select **Use these DNS servers**, enter the secondary DNS server IP address. It is an optional field.
MTU	The MTU (Maximum Transmit Unit) is the largest packet that can be sent over the network. The standard MTU value for Ethernet networks is usually 1500 Bytes.

b. When you select **Static** as the connection type, it displays the following page:



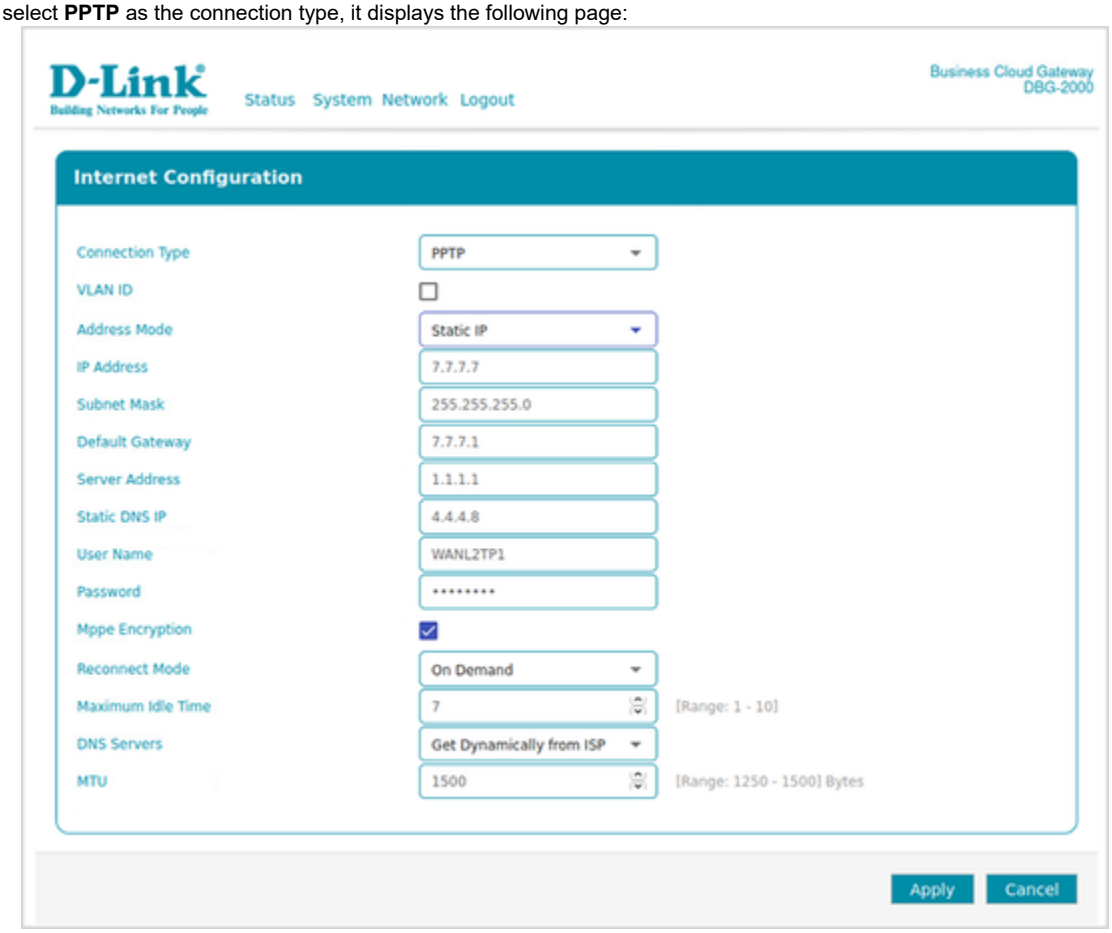
Fields	Description
Static	
IP address	Enter the static address that your ISP assigned to you. This address will identify the router to your ISP.
Subnet mask	Enter the IP subnet mask.
Default gateway	Enter the default gateway IP address.
Primary DNS	Enter the primary DNS server IP address.
Secondary DNS	Enter the secondary DNS server IP address. It is an optional field.
MTU	The MTU (Maximum Transmit Unit) is the largest packet that can be sent over the network. For example, the standard MTU value for Ethernet networks is usually 1500 Bytes.

c. When you select **L2TP** as the connection type, it displays the following page:



Fields	Description
L2TP	
Address mode	Select **Dynamic IP** or **Static IP** (IP settings supplied by your ISP).
Server address	Enter your L2TP server address.
IP address	If you select **Static IP** as the address mode, enter the IP address supplied by your ISP.
Subnet mask	If you select **Static IP** as the address mode, enter the subnet mask supplied by your ISP.
Default gateway	If you select **Static IP** as the address mode, enter the gateway IP address supplied by your ISP.
Static DNS IP	If you select **Static IP** as the address mode, enter the static DNS IP address in the respective subnet.
User name	Enter your L2TP user name.
Password	Enter your L2TP password.
Secret	Enter a shared secret.
Reconnect mode	Some ISPs may require you to pay for usage time. Select **On-Demand** if this is the case. This will have the gateway connect to the Internet only when you initiate an Internet connection. Select **Always On** to have the gateway stay connected to the Internet.
Maximum idle time	Enter the number of minutes in the *Maximum Idle Time* field. This feature is useful if your ISP charges you based on the time you are connected. This field is available only when **On-demand** is selected.
DNS Servers	Select either **Get dynamically from ISP** or **Use these DNS servers** to enter DNS servers manually.
MTU	The MTU (Maximum Transmit Unit) is the largest packet that can be sent over the network. For example, for all the L2TP connections, MTU is 1460 Bytes.

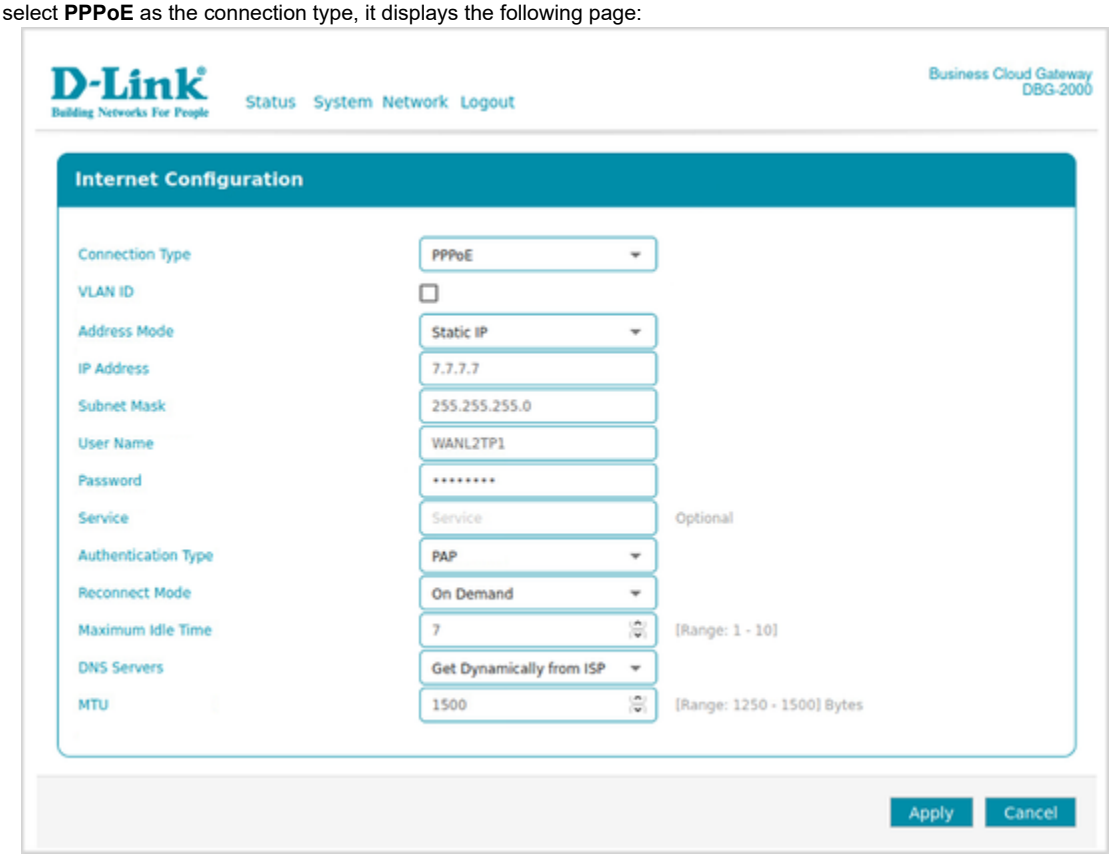
d. When you select **PPTP** as the connection type, it displays the following page:



Fields	Description
PPTP	
Address mode	Select **Dynamic IP** or **Static IP** (IP settings supplied by your ISP).
IP address	If you select **Static IP** as the address mode, enter the IP address supplied by your ISP.
Subnet mask	If you select **Static IP** as the address mode, enter the subnet mask supplied by your ISP.
Default gateway	If you select **Static IP** as the address mode, enter the gateway IP address supplied by your ISP.
Server address	Enter your PPTP server address.
Static DNS IP	If you select **Static IP** as the address mode, enter the static DNS IP address in the respective subnet.
User name	Enter your PPTP user name.
Password	Enter your PPTP password.
Mppe Encryption	Enable it if the PPTP server supports this feature.
Reconnect mode	Some ISPs may require you to pay for usage time. Select **On-Demand** if this is the case. This will have the gateway connect to the Internet only when you initiate an Internet connection. Select **Always On** to have the gateway stay connected to the Internet.
Maximum idle time	Enter the number of minutes in the *Maximum Idle Time* field. This feature is useful if your ISP charges you based on the time you are connected. This field is available only when **On-demand** is selected.
DNS Servers	Select either **Get dynamically from ISP** or **Use these DNS servers** to enter DNS servers manually.

MTU	The MTU (Maximum Transmit Unit) is the largest packet that can be sent over the network. For PPTP connections, it is 1492 Bytes.

e. When you select **PPPoE** as the connection type, it displays the following page:

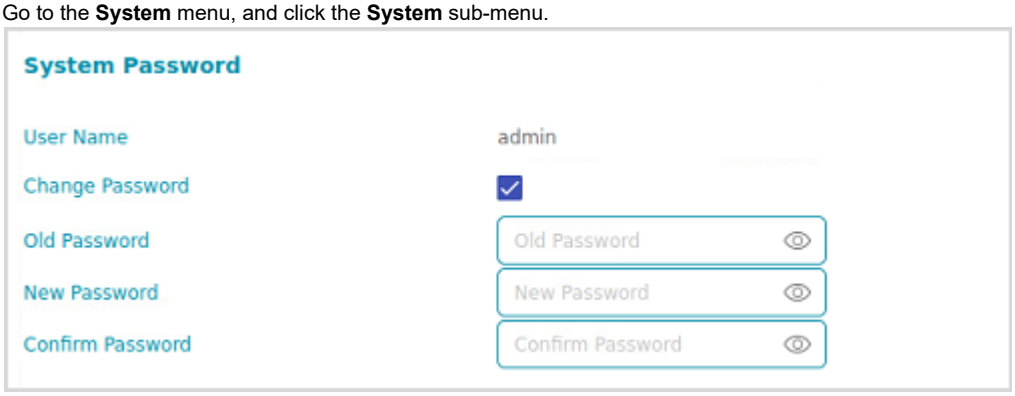


Fields	Description
PPPoE	
Address mode	Select **Dynamic IP** or **Static IP** (IP settings supplied by your ISP).
IP address	If you select **Static IP** as the address mode, enter the IP address supplied by your ISP.
Subnet mask	If you select **Static IP** as the address mode, enter the subnet mask supplied by your ISP.
User name	Enter your PPPoE user name.
Password	Enter your PPPoE password.
Service	If your ISP supports Service, enter the service name. It is an optional field.
Authentication type	Select the type of Authentication to use (Auto-Negotiate, PAP, CHAP, MS-CHAP, or MS-CHAPv2).
Reconnect mode	Select one of the following options: • **Always on:** The connection is always on. • **On-demand:** The connection is automatically ended if it is idle for a specified number of minutes.
Maximum idle time	Enter the number of minutes in the *Maximum Idle Time* field. This feature is useful if your ISP charges you based on the time that you are connected. This field is available only when **On-demand** is selected.
DNS Servers	Select either **Get dynamically from ISP** or **Use these DNS servers** to enter DNS servers manually.
MTU	The MTU (Maximum Transmit Unit) is the largest packet that can be sent over the network. For PPPoE connections, it is 1492 Bytes.

5. Click **Apply** to apply your settings to the device.

How to change your password?

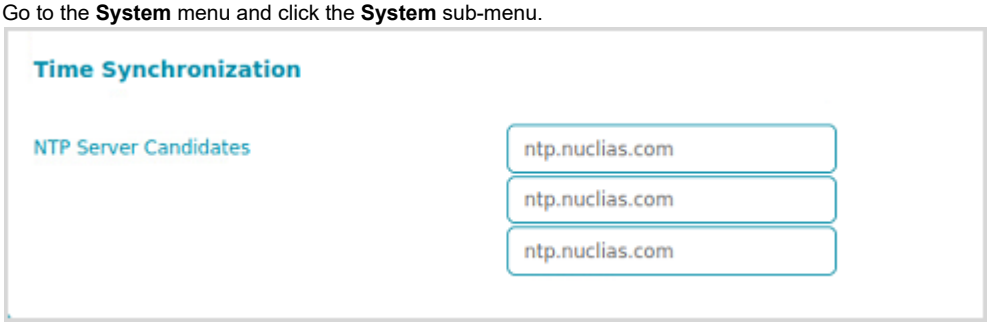
1. Go to the **System** menu, and click the **System** sub-menu.



2. Select the **Change password** checkbox.
3. Enter your **Old password**.
4. Enter your **new password**.
5. Retype your new password to confirm it and click **Apply**.

How to change NTP Server?

1. Go to the **System** menu and click the **System** sub-menu.

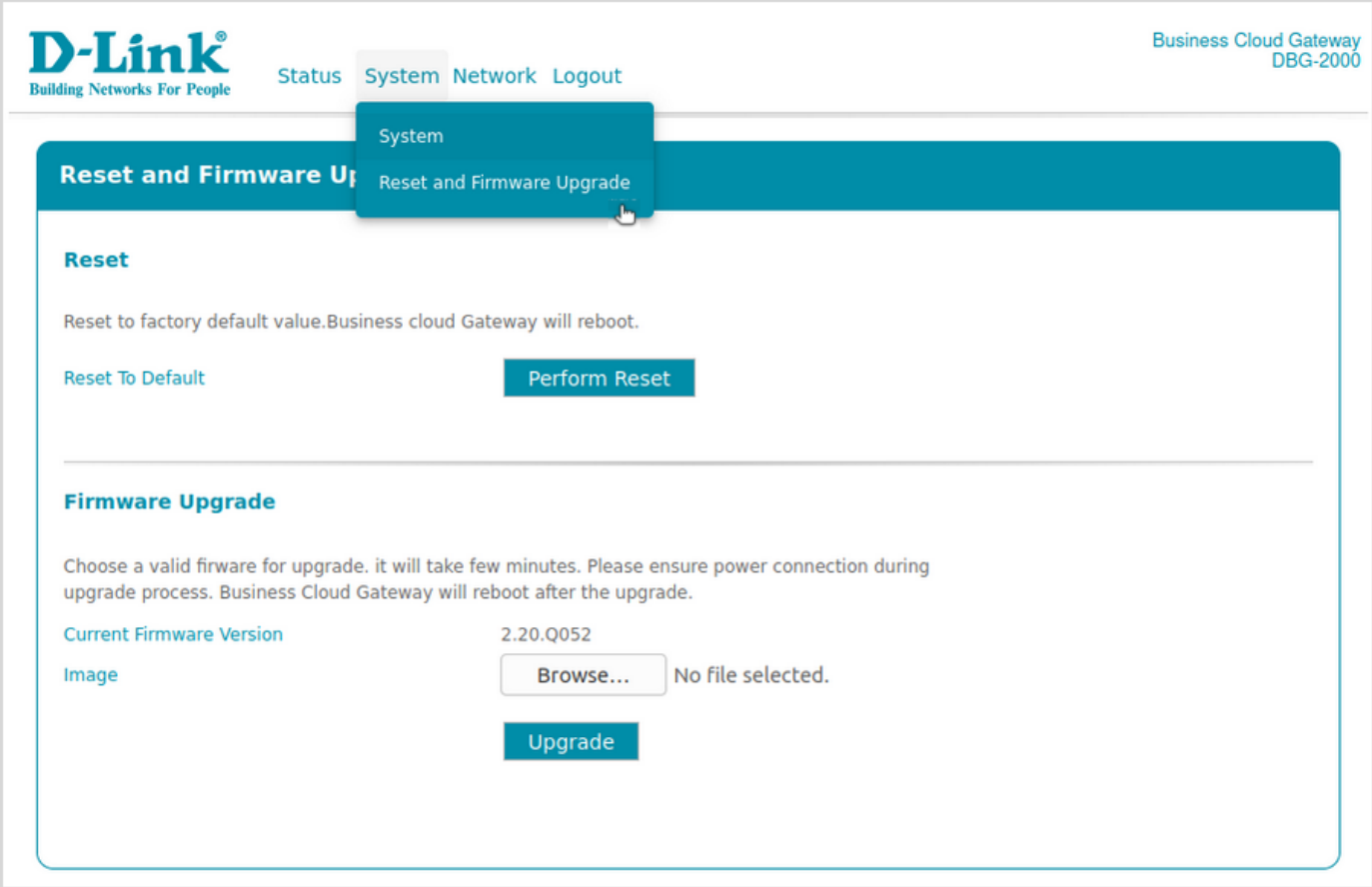


2. Under Time Synchronization, enter the Server IP address or the domain name where the NTP server is running.
3. You will be configuring primary, secondary, and tertiary NTP servers.
4. Click **Apply**.

How to Reset & Firmware Upgrade?

To reset the device and to upgrade its firmware, go to ***System > Reset and Firmware Upgrade***.

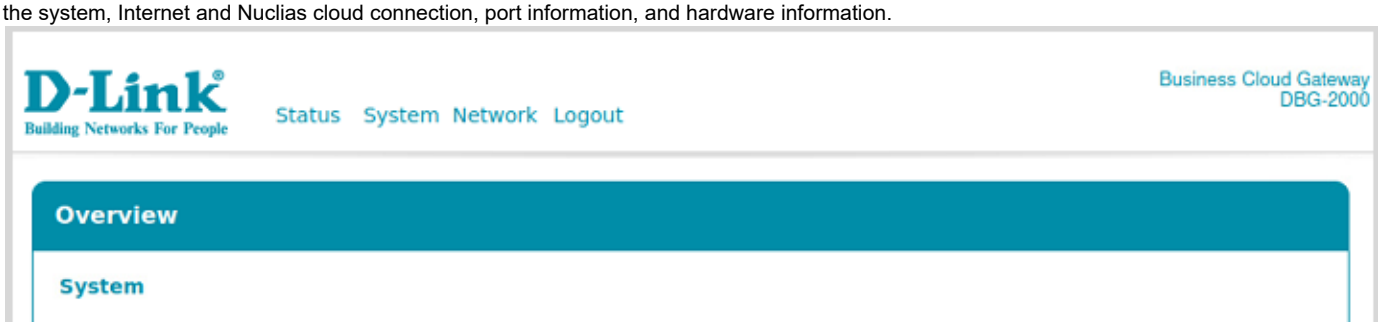
Note: You can perform reset only through the device GUI and not from the Nuclias Cloud portal.



Fields	Description
Reset	
Reset to default	If you reset the device to its default settings, it returns to the state when it was new — all changes you made to the default configuration are lost. *Note: If your device is synchronized with the Nuclias cloud, it gets associated with a profile, and the Internet Configuration settings are saved in that profile. After reset, when the device gets synchronized with the Nuclias cloud, by default, the same configuration gets pushed to the device.*
Firmware Upgrade	
Current Firmware version	It displays the firmware version running on the gateway.
Image	Click **Browse** and locate the firmware file.
Upgrade	Click **Upgrade** to start the firmware upgrade.

Status Overview

The **Status** menu of the gateway provides a brief overview of the device's status and its configuration. In addition, it provides details related to the system, Internet and Nuclias cloud connection, port information, and hardware information.



Model	DBG-2000
Current Firmware	2.20.Q049
Local Time	Wed Apr 07 2021 02:42:58 PM

Internet Connection

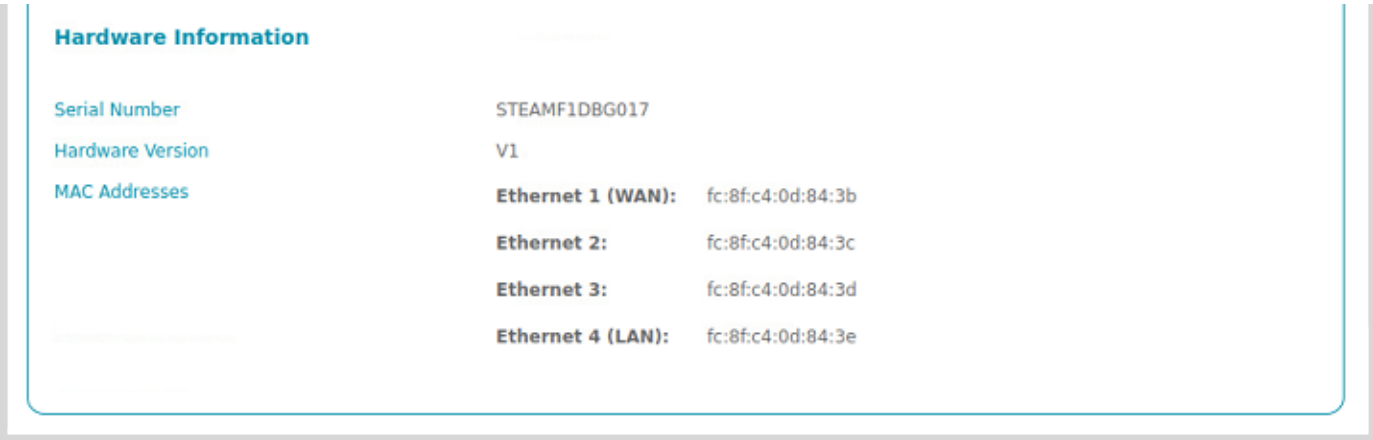
WAN1	**Connection Type:**	DHCP
	Address:	192.168.98.121
	Netmask:	255.255.248.0
	Gateway:	192.168.98.1
	DNS1:	192.168.98.1
	DNS2:	0.0.0.0
	Connected:	01h 45m 04s

Cloud Details

Cloud Connectivity Status	Connected
Internet Status	Connected
Device UID	TEAMF1DBG017
Registered	Yes
Registered Date	2021-04-06 16:59:53.261491
Nuclias	https://login.nuclias.com

Port Information

Ethernet 4 (LAN)	**IP Address:**	192.168.81.1
	Subnet Mask:	255.255.255.0
	DHCP Server:	Enabled
	Starting IP:	192.168.22.2
	Ending IP:	192.168.22.50
	Default Gateway:	192.168.22.1
	Domain Name:	lan.nuclias.com
	Lease Time:	1440
Ethernet 3 (LAN)	**IP Address:**	192.168.121.1
	Subnet Mask:	255.255.255.0
	DHCP Server:	Enabled
	Starting IP:	192.168.121.2
	Ending IP:	192.168.121.50
	Default Gateway:	192.168.121.1
	Domain Name:	lan.nuclias.com
	Lease Time:	1440



Fields	Description
System	
Model	It displays the name of the model.
Current version	It displays the firmware version running on the gateway.
Local time	It displays the time as per the time zone set on the gateway.
Internet Connection	
WAN1	
Connection type	It displays the connection type being used to set up an Internet connection.
Address	It displays the IP address that is obtained or configured for the WAN interface.
Netmask	It displays the subnet mask for the IP address.
Gateway	It displays the gateway IP address.
DNS1	It displays the IP address of the primary DNS server.
DNS2	It displays the IP address of the secondary DNS server.
Connected	It provides the status of the Internet connection.
Cloud Details	
Cloud connectivity status	It displays if the device is connected to the Nuclias Cloud or not.
Internet status	It provides the Internet status of your connection.
Device UID	It displays the unique identification of the device.
Registered	It displays whether your device is registered with the Nuclias cloud.
Registered Date	If your device is registered, it displays the date and time when it got registered.
Nuclias	It displays the website link of the Nuclias cloud.
Port Information	
Ethernet	
IP address	It displays the IP address for the gateway.
Subnet mask	It displays the subnet mask for the network.
DHCP Server	It displays if the DHCP Server is enabled or disabled.
Starting IP	It displays the starting IP address.
Ending IP	It displays the ending IP address.

Default gateway	It displays the default gateway IP address.
Domain name	It displays the domain name for LAN configuration.
Lease time	It displays the duration for which IP addresses will be leased to clients.
Hardware Information	
Serial number	It displays the serial number of your gateway.
Hardware version	It displays your device's hardware version.
MAC address	It displays the MAC address of each port.

Want to learn about the Nuclias Cloud portal? Go to Where to Go from Here.

Where to Go from Here

After installing the Nuclias cloud gateway, you can operate it using the factory default settings. These settings should be suitable for most users and in most situations. In addition, the Nuclias Cloud Gateway provides basic and advanced configuration settings for users to use as per their requirements. The following chapters provide the advanced settings of the cloud gateway:

Chapter 1 - Basic

This chapter describes the Device Information, Location, WAN Interface, and Site and Profile.

Chapter 2 - Summary

This chapter describes the Status, Statistics, DHCP, and VPN Status of the cloud gateway.

Chapter 3 - Network

This chapter describes the Ethernet, Addressing, Routing, Services, Traffic Management, and High Availability.

Chapter 4 - Security

This chapter describes the firewall, IPS, ALG, WCF, and Application Control.

Chapter 5 - VPN

This chapter describes the Site to Site VPN, PPTP/L2TP, OpenVPN, and GRE Tunnel.

Chapter 6 - Tools

This chapter describes the supported diagnostic tools.

Chapter 7 - License

This chapter provides license information.

Standard Web Management Interface Features

The standard features that are available on the web management interface are as follows:

Table content search allows you to search for information in the table by typing a word into the search box. The search box is always located in the upper-right corner of the table.

Previous/Next (on the table): The information is shown on multiple pages. Use Previous or Next to switch pages, and between them, the current page number is displayed. The pagination is always located in the lower-right corner of the table.

It indicates the number of entries displayed on the table on one page. The system can list 5, 10, 20, 40, and 100 entries on one page.

The **Add** button adds a new entry to the current table, and the **Delete** button deletes the selected entry or multiple entries. The **Add** and **Delete** buttons are located in the upper-left corner of the table.

It helps you to filter the content that you want to display in the table. Click the arrow and select the checkboxes of the items that you want to add as columns in the table. This icon is always located in the upper-right corner of the table.

The **Apply** button pushes the configuration to the connected device. This button is present in the upper-left side beside the device tabs and is available only for the following tabs: Basic, Network, Security, and VPN.

Configuration pages

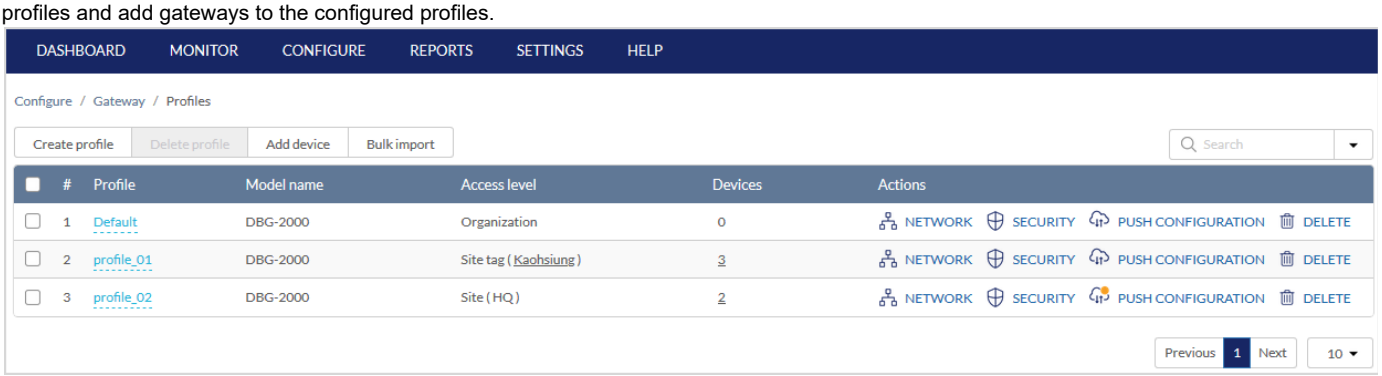
This section of the user guide comprises a set of UI pages used to configure the important parameters, like profiles, devices, authentication servers, schedule policies, and splash page editor. These parameters are further required to configure a few features of the Nuclias cloud gateway. The configuration pages provide a list of configured parameters and also help you to configure them.

This section consists of the following topics:

Profiles

A profile is defined as a predefined configuration that is directly pushed to any newly added or existing gateways and shared among multiple gateways. Rather than configuring each added device independently, a set of network and security settings parameters can be saved as Profiles. When a device is added to the cloud, it must get associated with one of these configured profiles. You can also edit this profile configuration based on the requirement.

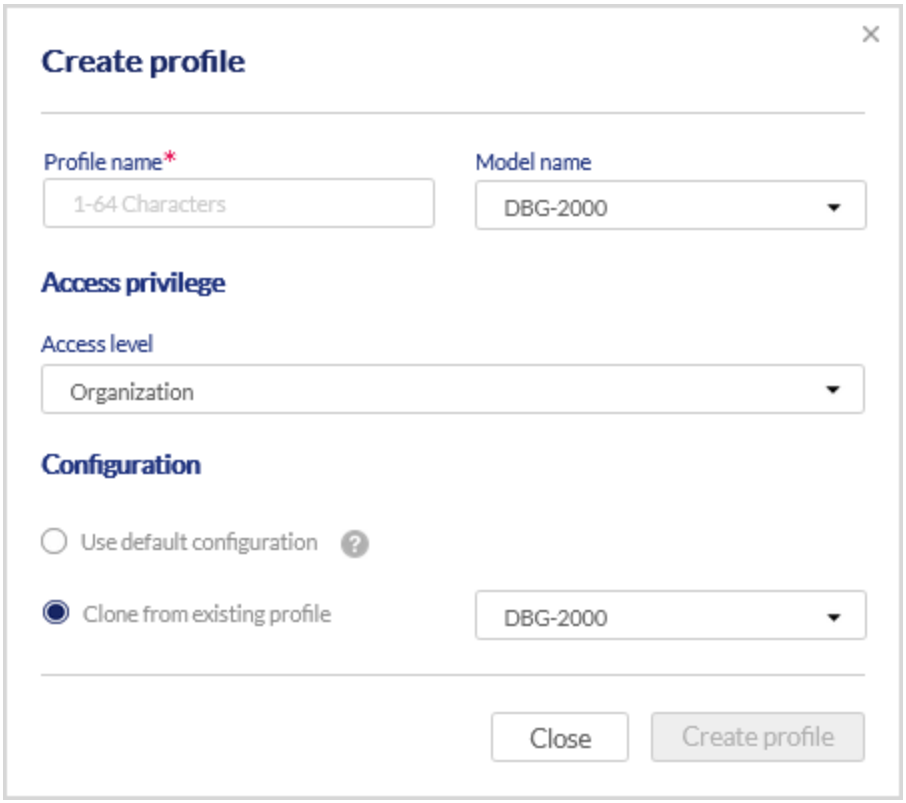
The path to reach the *Profiles* page is *Configure* > *Gateway* > *Profiles*. This page lists all the configured profiles and allows the user to create profiles and add gateways to the configured profiles.



The fields present in the table are as follows:

Field	Description
Profile	It displays the name of the profile.
Model name	It displays the name of the model associated with the profile.
Access level	It displays the level where the user can use this.
Devices	It displays the number of devices associated with the profile.
Actions	It displays the following actions: • **Network**: Click the **Network** link, and it will redirect you to the Network tab of the device to configure the network-related parameters like Ethernet, Addressing, Services, Traffic Management, and Captive Portal. • **Security**: Click the **Security** link, and it will redirect you to the Security tab of the device to configure the security parameters like Firewall, IPS, Web Content Filter, and Application Control. • **Push Configuration**: Click **Push Configuration** to configure all the associated devices with that profile at one go. • **Delete**: Click **Delete** to delete the profile.

To create a new profile, click the **Create profile** button. This opens the *Create profile* page.



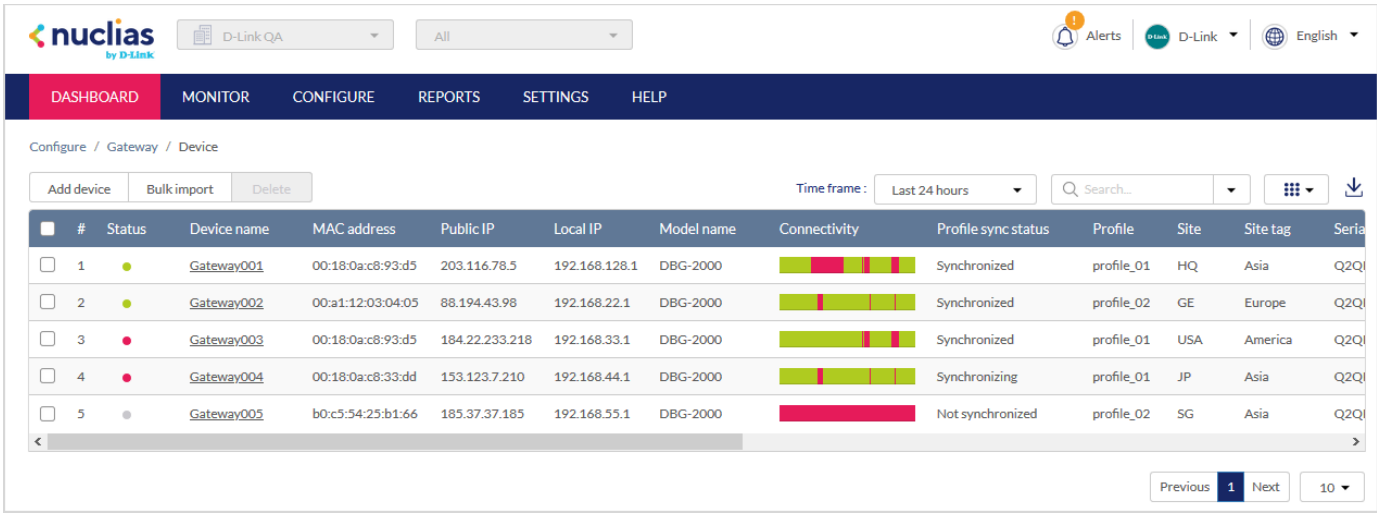
The fields available on this page are as follows:

Field	Description
Profile name	Enter a descriptive name of the profile.
Model name	Select the name of the model you want to associate with the profile.
Access level	Select the level where the user can use this profile. The options are Organization, Site tag, and Site. Based on the access level, select the **Managed site tag** and the **Managed site**.
Managed site tag	Select the managed site tag from the drop-down list. This field is available when you select “Managed site tag” as the **Access level**.
Managed site	Select the managed site from the drop-down list. This field is available when you select “Managed site” as the **Access level**.
Configuration	
Use default configuration	Choose this option if you want to use the default settings for the profile. You can edit the configuration anytime.
Clone from existing profile	If you want to use the configuration of one of the configured profiles, choose this option and then select that profile. This field is available when you select the “Organization” as the **Acc ess level**.
Create profile	Click **Create profile** to save the new profile.
Close	Click **Close** to close the *Create Profile* page.

To add a device, click **Add device**. This opens the *Add device* page. Refer to the Device section for more details.

Device

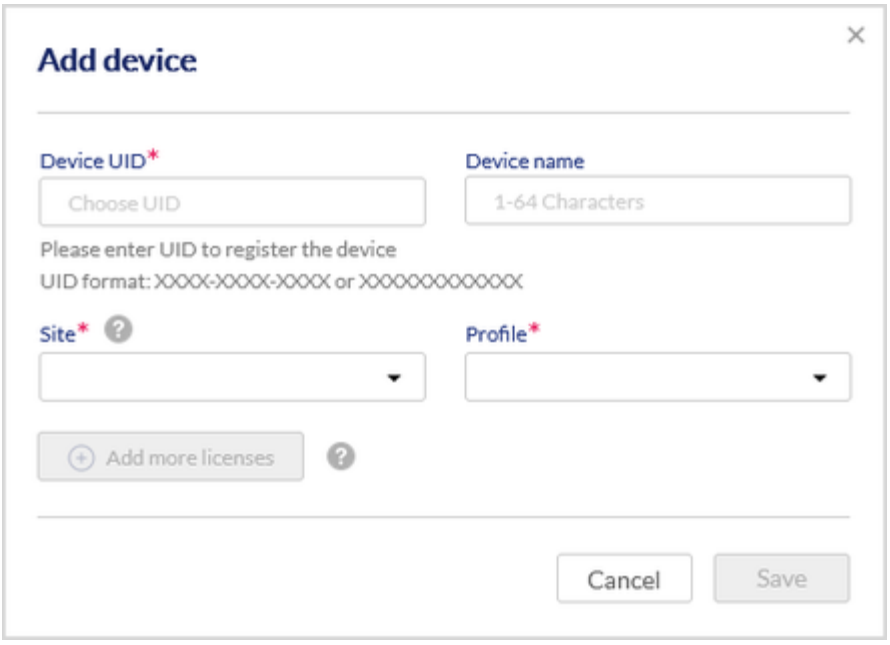
The path to reach the *Device* page is *Configure* > *Gateway* > *Device*. The *Device* page consists of a list of devices present in the device group for the selected time frame. It displays the hardware and firmware details of the devices and the profiles with which these devices are associated. It also allows the user to add new devices to the list, either separately or by bulk import.



The following fields are displayed on this page:

Field	Description
Status	It displays the status of the device present in the device group. The **Green** dot indicates that the device is connected to the cloud and the **Red** dot indicates that the device is not connected to the cloud.
Device name	It displays the name of the device.
MAC address	It displays the MAC address of the device present in the device group.
Public IP	It displays the IP address through which DBG is connected to the cloud server.
Local IP	It displays the IP address of the device.
Model name	It displays the model name of the device.
Connectivity	It provides the connectivity status history of that device in the form of a bar. When you hover over the bar, it displays when and for how long the device was connected or disconnected. The green zone indicates a connected gateway, and the red zone indicates “no connectivity.”
Profile sync status	When you push a configuration and the device is reachable, it displays **Synchronized**, and if the device is not reachable, it displays **Not synchronized**.
Profile	It displays the profile being used.
Site	It displays the site where the device is being operated.
Site tag	It displays the name of the sub-site it belongs to.
Serial number	It displays the serial number of the device.
Firmware version	It displays the current firmware version running on the device.
Last seen	It displays the date and time when the last time the device got connected.
License status	It indicates if the license is active or not.
Device UID	It displays the unique identification of the device generated by the Cloud team.
Activation date	It displays the time when the license was activated.
Expiration date	It displays the time when the license will be expired.

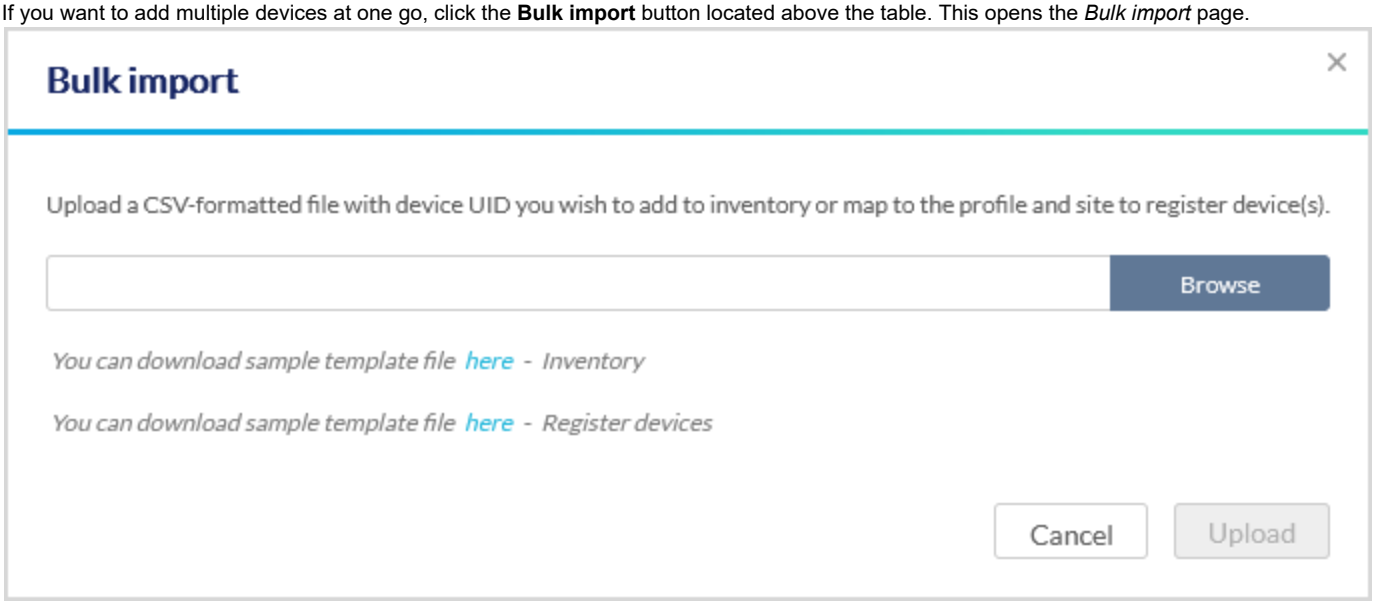
To add a new device to the device group, click the **Add device** button located above the table. This opens the *Add device* page. To delete multiple entries at once, select the corresponding checkboxes of the entries you want to delete, and click **Delete**.



The fields available on this page are given below.

Field	Description
Device UID	Enter the unique identification of the device generated by the Cloud team.
Device name	Enter the name of the device.
Site	Select the site where the device is being operated.
Profile	Select one of the configured profiles that you want to use.
License key #1	Click in the box to select any one of the available licenses.
Add more licenses	Click the **Add more licenses** button to add more licenses.
Save	Click **Save** to save your device details.
Cancel	Click **Cancel** to close the *Add device* page.

If you want to add multiple devices at one go, click the **Bulk import** button located above the table. This opens the *Bulk import* page.



Click **Browse** to select and open the file in CSV format, and click **Upload**. This will upload the file with device UID either to inventory or map to the profile and site to register device(s). You may also download the sample templates for the inventory and register devices here.

Authentication

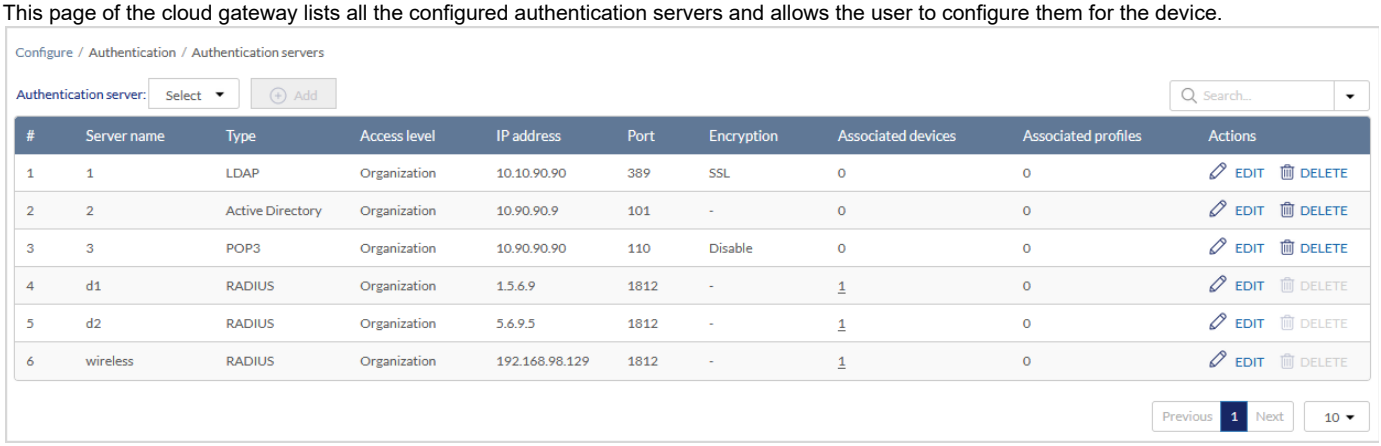
Network authentication refers to the security-related process required when a client tries to connect to your network. There are various ways in which the Nuclias cloud gateway supports the authentication process that includes the local authentication server and the external authentication servers. This section of the user guide will tell you about these servers and their configuration.

It consists of the following topics:

Authentication servers

The path for the **Authentication servers** page is *Configure* > *Authentication* > *Authentication servers*. An authentication server is a network service that provides credentials to the authenticated users to access the network. When a user enters these credentials into the login page, access to the network is granted. In addition, the authentication server maintains a database of users or an external authentication server configuration.

This page of the cloud gateway lists all the configured authentication servers and allows the user to configure them for the device.



The fields available in the table are as follows:

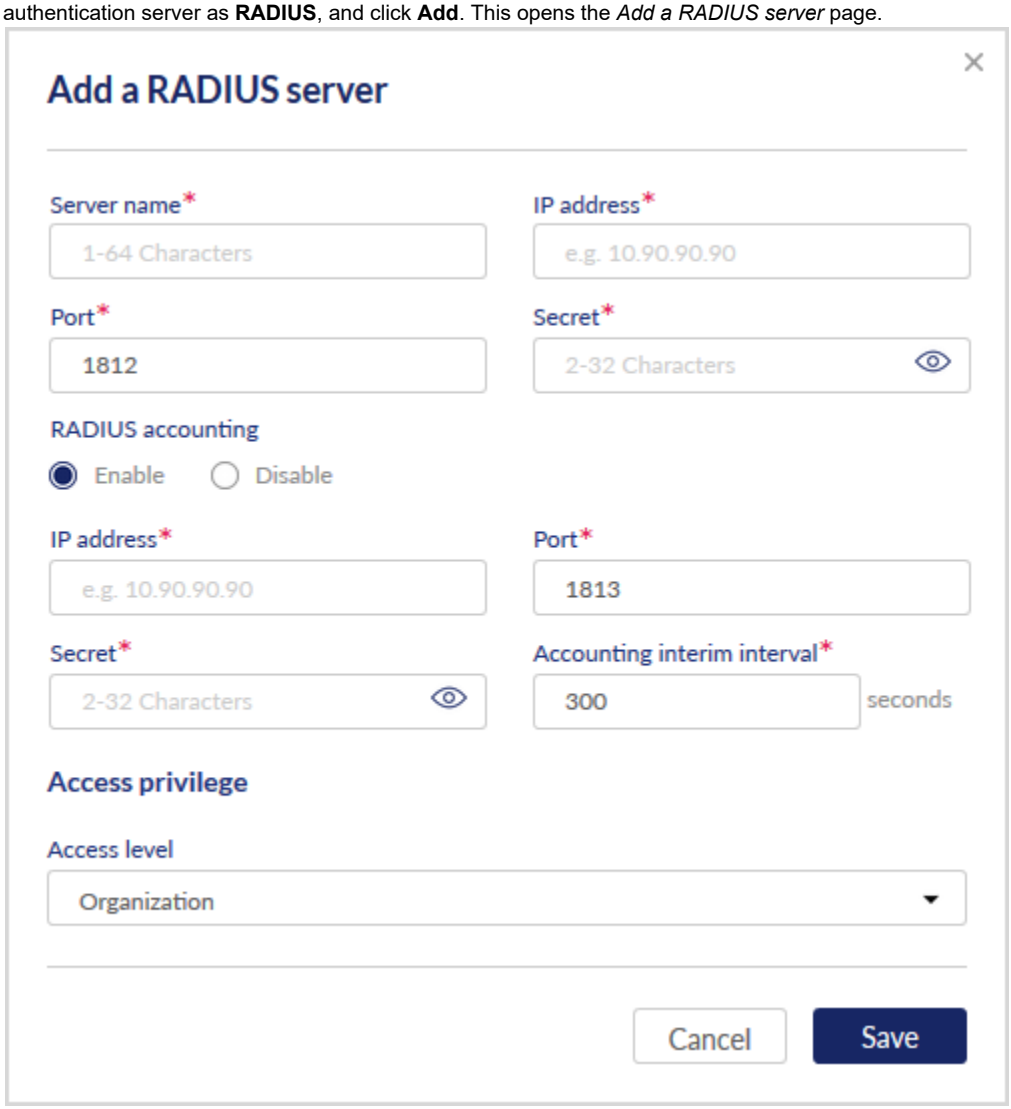
Field	Description
Server name	It displays the name of the server.
Type	It displays the type of server. It could be any of the following server types: RADIUS, LDAP, Active Directory, POP3, or NT Domain.
Access level	It displays the access level that is authorized to use the configured server.
IP address	It displays the IP address of the authentication server.
Port	It displays the authentication server port.
Encryption	It displays if the encryption is enabled.
Associated devices	It displays the devices that are associated with the server.
Associated profiles	It displays the number of profiles associated with the devices using the authentication server.
Actions	You can edit or delete the configured authentication server. Click **Edit** to make any changes to the existing authentication server. This opens the configuration page.

To add a new authentication server, select the authentication server type from the drop-down list present above the table, and then click the **Add** button. This opens the configuration page of the selected server type. Select one of the following authentication server types:

- RADIUS
- LDAP
- POP3
- Active Directory
- NT Domain

RADIUS

A RADIUS server can be configured and accessible by the gateway to authenticate client connections. To add a Radius server, select the authentication server as **RADIUS**, and click **Add**. This opens the *Add a RADIUS server* page.



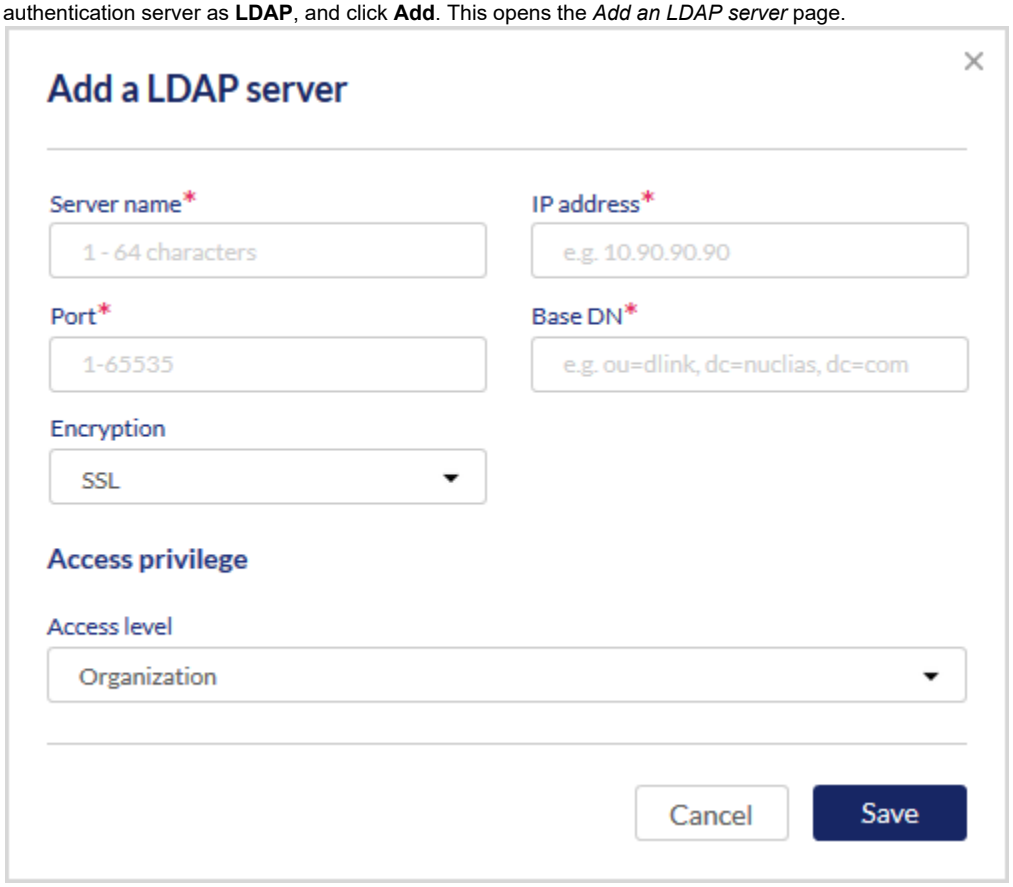
The fields available on this page are as follows:

Field	Description
Server name	Enter the name of the server.
IP address	Enter the IP address of the authentication server.
Port	Enter the RADIUS authentication server port.
Secret	Enter the secret key that allows the device to log into the configured RADIUS server. It must match the secret on the RADIUS server.
RADIUS accounting	Enable this feature to configure Accounting Interim Interval (in seconds), at which the device sends the traffic statistics of a session in accounting messages to the configured Radius Server.
IP address	Enter the IP address of the RADIUS accounting server.
Port	Enter the RADIUS accounting port.
Secret	Enter the secret key that allows the device to get authenticated with the RADIUS accounting server. All the radius accounting transactions between the client and the RADIUS accounting server are authenticated through this shared secret.

Accounting interim interval	Enter the interim interval, in seconds, at which the device should send the Radius Accounting (Interim-Update) packets. The value should be in the range of 300 - 3600. By default, it is 300.
Access privilege	
Access level	The access level decides the devices that can utilize this server. Select the access level.
Save	Click **Save** to save the authentication server.
Cancel	Click **Cancel** to revert to the previous settings.

LDAP

The LDAP authentication method uses LDAP to exchange authentication credentials between the gateway and an external server. The LDAP server maintains a large database of users in a directory structure, so users with the same user name but belonging to different groups can be authenticated since the user information is stored hierarchically. Also, note that configuring an LDAP server on Windows or Linux servers is considerably less complex than setting up NT Domain or Active Directory servers for user authentication. To add an LDAP server, select the authentication server as **LDAP**, and click **Add**. This opens the *Add an LDAP server* page.



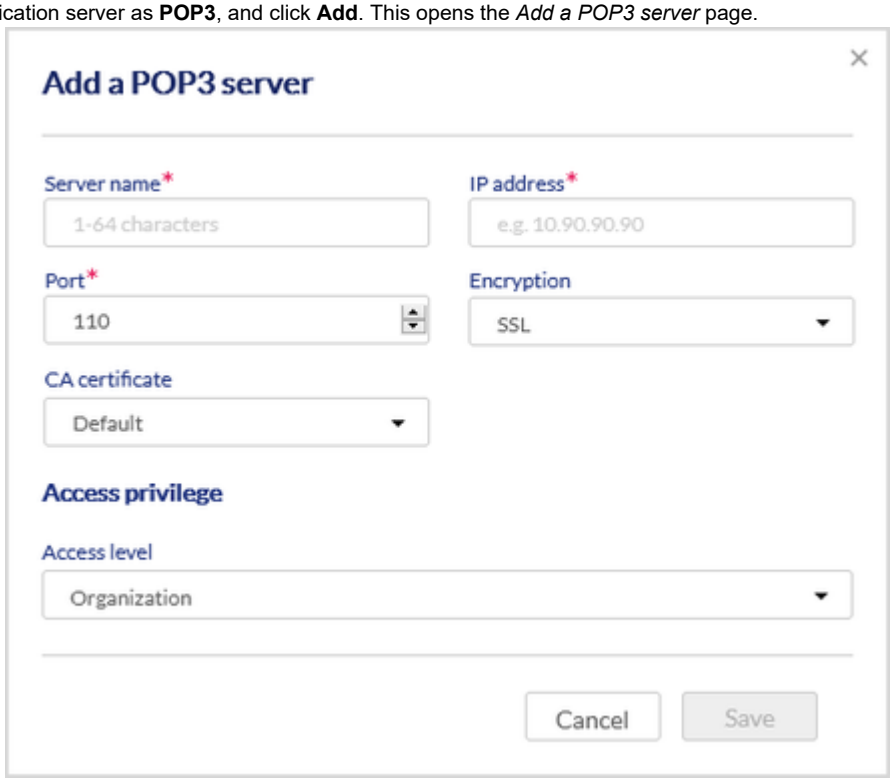
The fields available on this page are as follows:

Field	Description
Server name	Enter the name of the server.
IP address	Enter the IP address of the LDAP server.
Port	Enter the LDAP authentication server port.
Base DN	Enter the base domain name.
Encryption	You can enable encryption by selecting SSL or TLS from the drop-down list.
Access privilege	
Access level	The access level decides the devices that can utilize this server. Select the access level.

Save	Click **Save** to save the authentication server.
Cancel	Click **Cancel** to revert to the previous settings.

POP3

POP3 is an application layer protocol most commonly used for email over a TCP/IP connection. The authentication server can be used with SSL encryption over port 995 to send encrypted traffic to the POP3 server. A CA certificate verifies the POP3 server's certificate. To add a POP3 server, select the authentication server as **POP3**, and click **Add**. This opens the *Add a POP3 server* page.

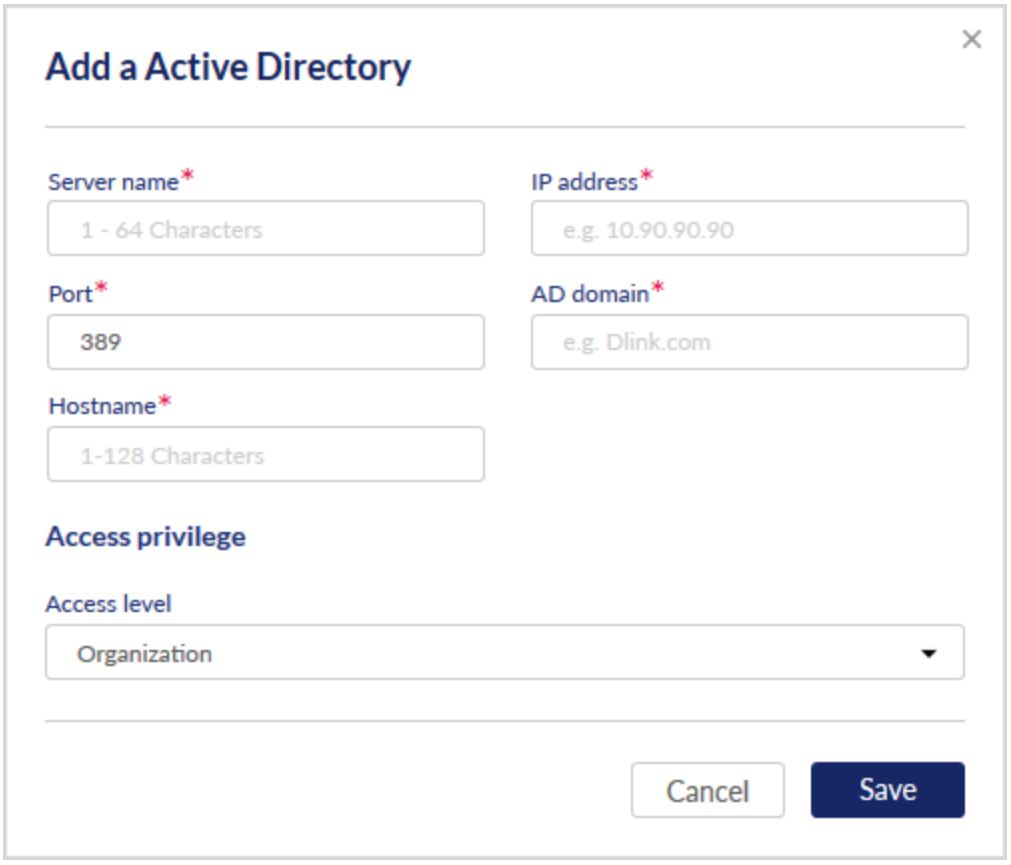


The fields available on this page are as follows:

Field	Description
Server name	Enter the name of the server.
IP address	Enter the IP address of the POP3 server.
Port	Enter the POP3 authentication server port.
Encryption	You can enable or disable the SSL support for POP3. If this option is enabled, it is mandatory to select a certificate authority for it.
CA certificate	Select a Certificate Authority to verify the POP3 server's certificate.
Access privilege	
Access level	The access level decides the devices that can utilize this server. Select the access level.
Save	Click **Save** to save the authentication server.
Cancel	Click **Cancel** to revert to the previous settings.

Active Directory

Active Directory authentication is an enhanced version of NT Domain authentication. The Kerberos protocol is leveraged for authentication of users grouped in Organizational Units (OUs). The configured Authentication Servers and Active Directory domain(s) are used to validate the user with the directory of users on the external Windows-based server. To add an Active Directory server, select the authentication server as **Active Directory**, and click **Add**. This opens the *Add an Active Directory* page.

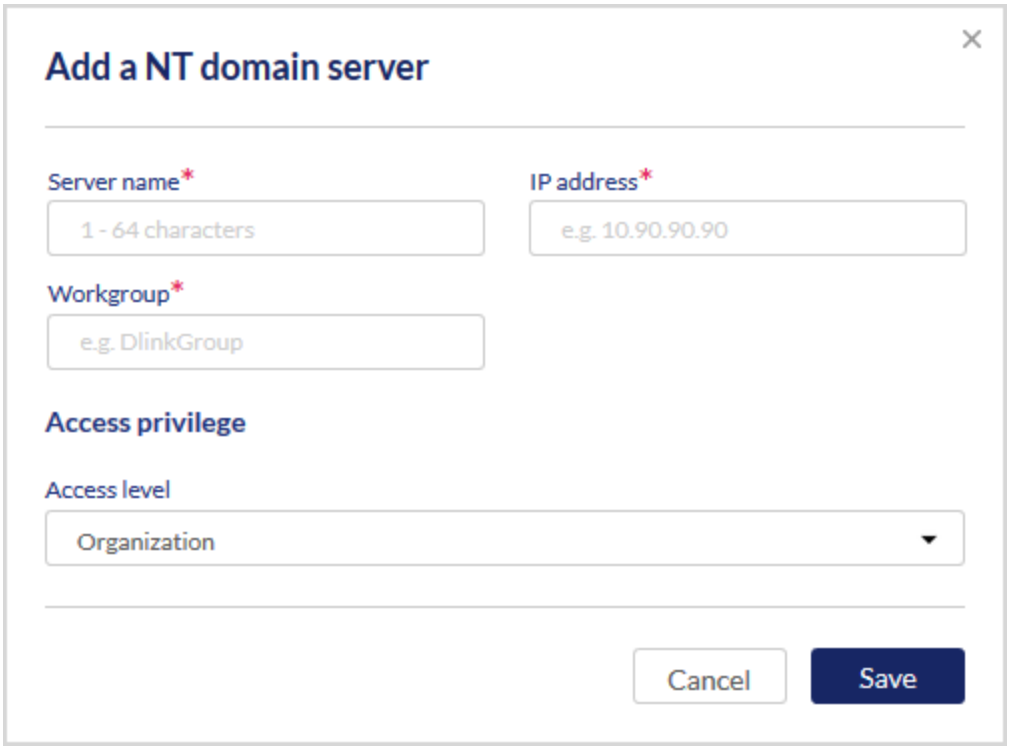


The fields available on this page are as follows:

Field	Description
Server name	Enter the name of the server.
IP address	Enter the IP address of the Active Directory server.
Port	Enter the Active Directory authentication server port.
AD domain	Since Active Directory is the chosen authentication type, you must enter the Active Directory domain name in this field. Users registered in the Active Directory database can now access the SSL VPN portal using their Active Directory username and password.
Hostname	Enter the server hostname for Active Directory.
Access privilege	
Access level	The access level decides the devices that can utilize this server. Select the access level.
Save	Click **Save** to save the authentication server.
Cancel	Click **Cancel** to revert to the previous settings.

NT Domain

The NT Domain server allows users and hosts to authenticate themselves via a pre-configured Workgroup field. Typically Windows or Samba servers are used to manage the domain of authentication for the centralized directory of authorized users. To add an NT domain server, select **NT domain** as the *Authentication Server,* and click **Add**. This opens the *Add an NT domain server* page.

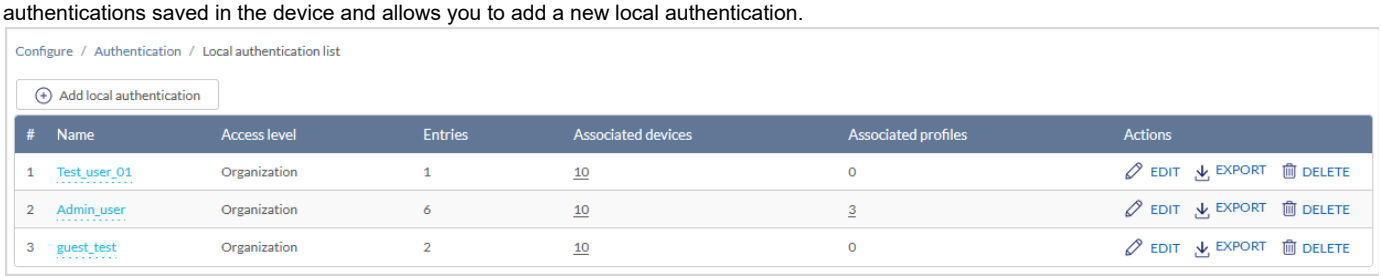


The fields available on this page are as follows:

Field	Description
Server name	Enter the name of the server.
IP address	Enter the IP address of the authentication server.
Workgroup	Enter the NT workgroup name(s).
Access privilege	
Access level	The access level decides the devices that can utilize this server. Select the access level.
Save	Click **Save** to save the authentication server.
Cancel	Click **Cancel** to revert to the previous settings.

Local authentication list

The path for the **Local authentication list** page is *Configure* > *Authentication* > *Local authentication list*. This section lists all the local authentications saved in the device and allows you to add a new local authentication.

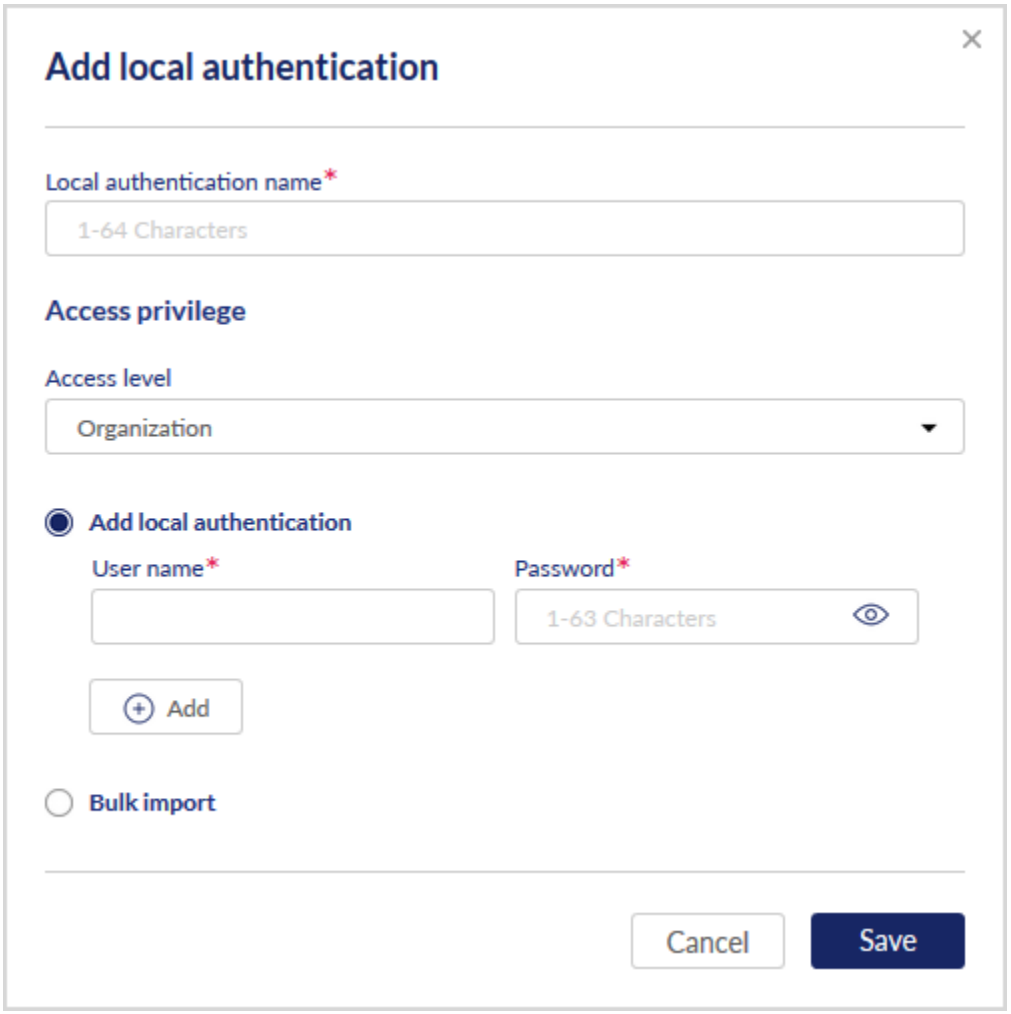


The fields that are displayed in the list are as follows:

Field	Description
Name	It displays the name of the server.
Access level	It displays the access level that is authorized to use the local authentication.

Entries	It displays the number of login credentials saved under that name.
Associated devices	It displays the number of devices that are associated with the server.
Associated Profiles	It displays the number of profiles associated with the devices using local authentication.
Actions	You can edit or delete the configured authentication server. Click **Edit** to make any changes to the existing authentication details. This opens the *Edit local authentication* page. You can export the details by clicking **Export**.

To add a new local authentication, click the **Add local authentication** button located above the table.



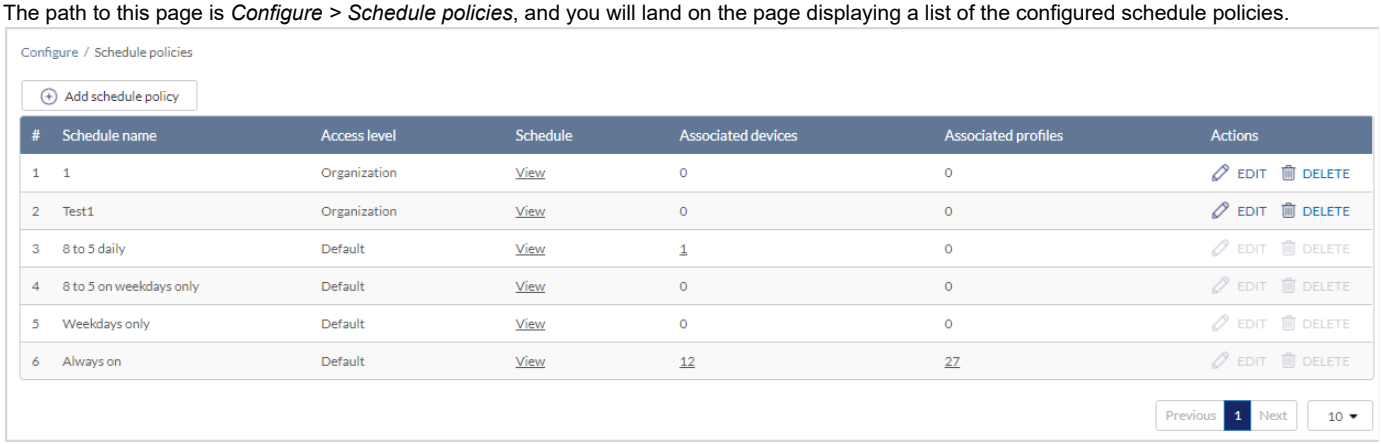
The fields available on this page are as follows:

Field	Description
Local authentication name	Enter the name of the server.
Access level	Select the access level from the drop-down list. The devices that fall under this level can access the configured local authentication.
Add local authentication	Enter the user name and password. To add more entries, click the **Add** button.
Bulk import	To add multiple entries at once, select **Bulk import**. Click **Browse** to locate and select the file in *.csv format and upload the entries. You may also download the sample template file here.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

Schedule policies

The *Schedule policies* page displays all the default and the configured schedule policies for the devices. These schedules are used to activate a few features of the gateway for a certain period of time. So, for features like web content filter, access control, etc., you can configure the schedules on this page, and then you can select one of these schedules from the drop-down list while configuring these features.

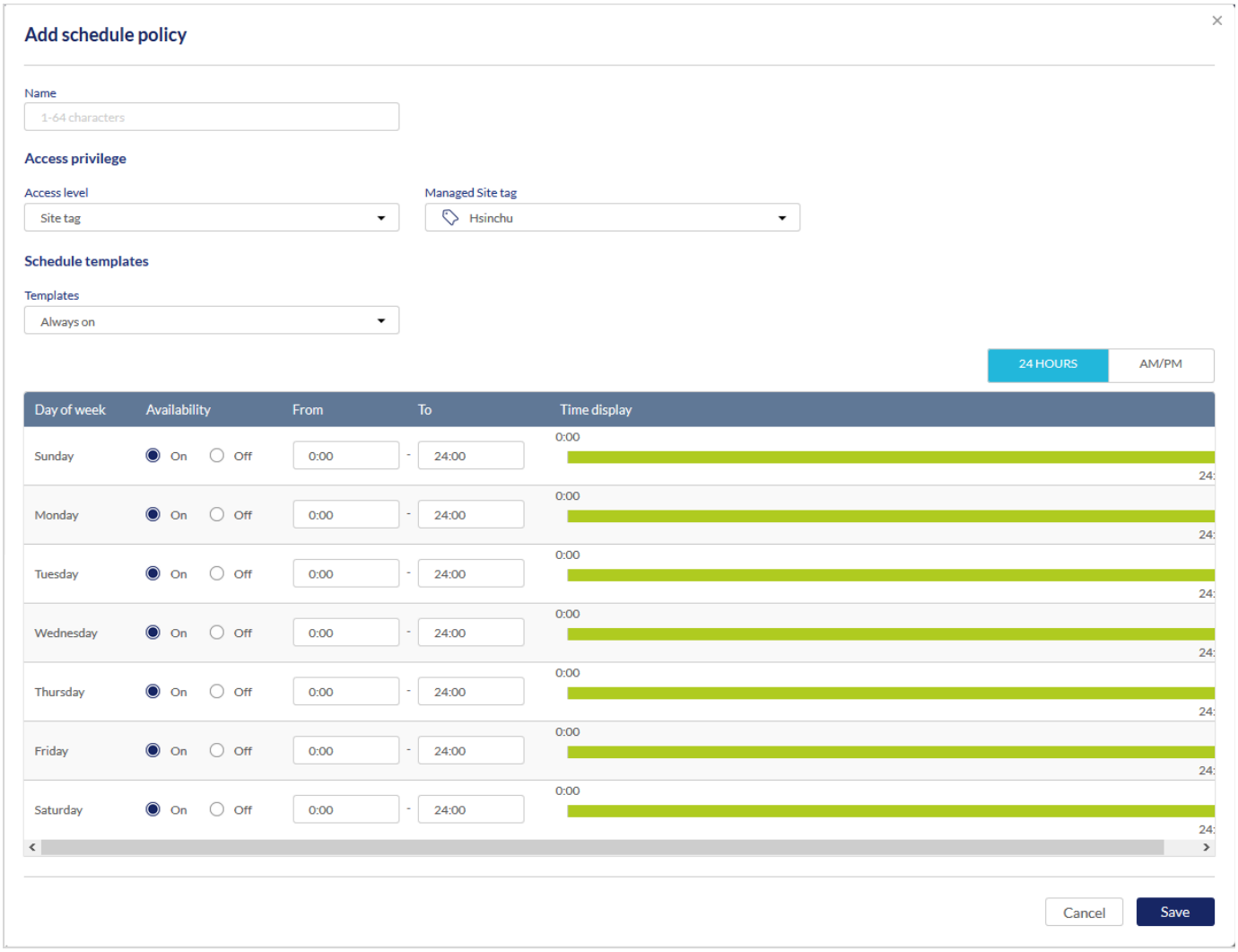
The path to this page is *Configure* > *Schedule policies*, and you will land on the page displaying a list of the configured schedule policies.



The fields displayed in the table are as follows:

Field	Description
Schedule name	It displays the name of the configured schedule.
Access level	It displays the level at which the schedule is applied.
Schedule	Click **View** to see the details of the schedule.
Associated devices	It displays the number of devices that are associated with this particular policy.
Associated profiles	It displays the number of profiles associated with the devices using the particular schedule policy.
Actions	You may click **Edit** or **Delete** to modify or delete the existing ones. ***Note:*** *The policies with access level as Default are templates' policies and cannot be edited or deleted; hence edit and delete options are not available.*

To add a new schedule policy, click the **Add schedule policy** button. This opens the *Add schedule policy* page.



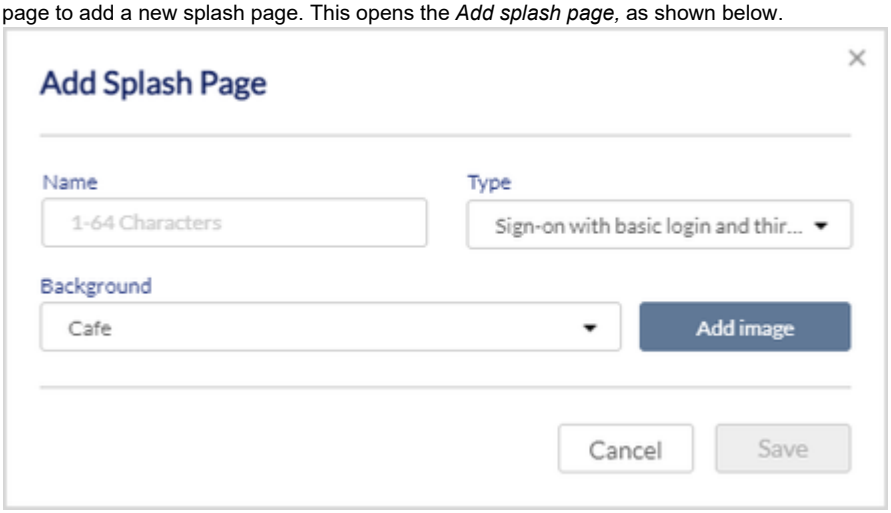
The fields available on this page are as follows:

Field	Description
Name	Enter a descriptive name for the schedule.
Access privilege	
Access level	Select the level at which the schedule is to be applied. The options are Organization, Site, and Site tag.
Managed site tag	Select the site tag where this scheduling policy will be available to the user to apply. This field is available only when you select the **Site tag** in the access level field.
Managed site	Select the site where this policy will be available to the user to apply. This field is available only when you select **Site** in the access level field.
Schedule templates	
Template	Select any one of the following pre-configured scheduled templates: *8 to 5 daily*, *8 to 5 on weekdays only*, *weekdays only*, and *Always on*.
Day of week	This column displays days of the week.
Availability	It indicates whether the rule is applied on the selected day at the mentioned time slot or not. If the availability feature is **On**, the rule is applied during the mentioned time slot, and if it is **Off**, the rule is applied other than the mentioned time slot. For example, the selected time slot is 1500 hrs to 1800 hrs. If the availability is On, then the rule is applied during these hours (3 hours), and if it is Off, the rule is applied to the time other than 1500 to 1800 hrs, i.e., for the rest of 21 hrs.

From	Enter the start time when the policy is applied or not applied.
To	Enter the end time when the policy is applied or not applied.
Time display	It displays the format (24 hours or 12 hours) in which you want to see the time.
Save	Click **Save** to add a new schedule policy.
Cancel	Click **Cancel** to revert to previous settings.

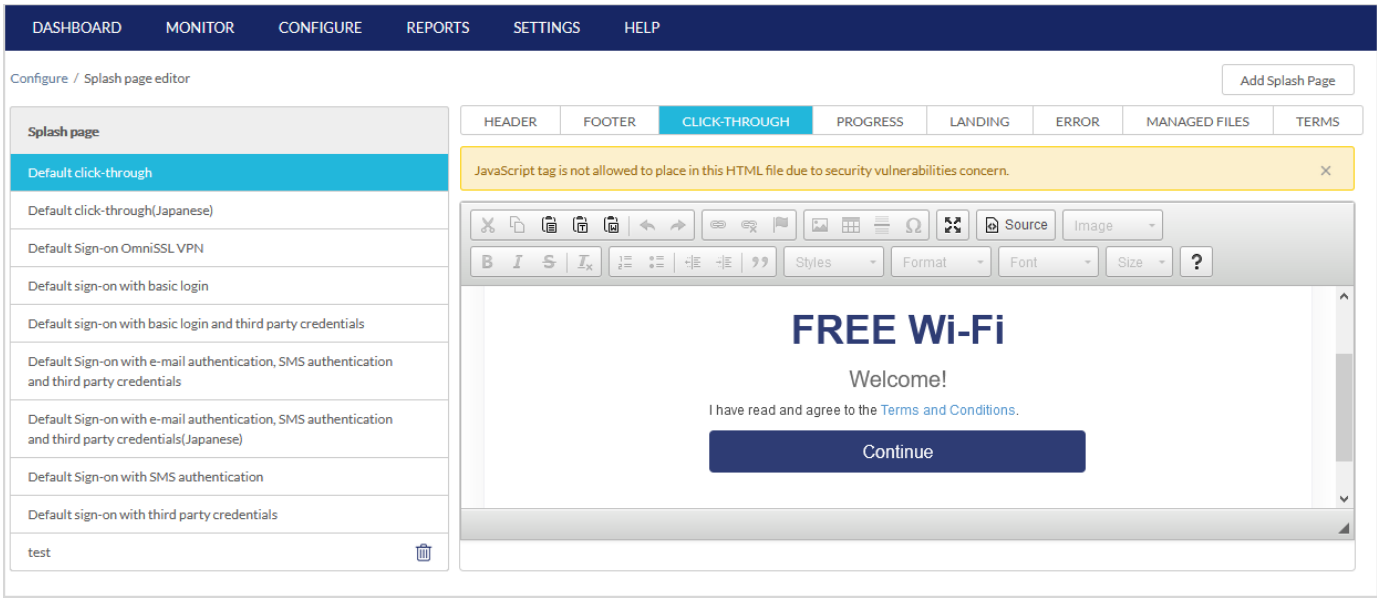
Splash page editor

The Nuclias cloud gateway, DBG-2000, allows its users to customize the splash page as per their requirements, e.g., they can add a company logo or change the color scheme. It allows you to create, edit, or delete the existing splash pages. Click the **Add Splash page** button present in the top-right corner of the page to add a new splash page. This opens the *Add splash page,* as shown below.



The fields available on the *Add splash page* are as follows:

Field	Description
Name	Enter a name for the splash page with a length of 1 to 64 characters.
Type	Select any one of the types of splash pages you want to create. You can create multiple splash pages for the same type. • Click-through • Click-through (Japanese) • Sign-on with basic login • Sign-on with basic login and third party credentials • Sign-on with e-mail authentication, SMS authentication, and third party credentials • Sign-on with e-mail authentication, SMS authentication, and third party credentials (Japanese) • Sign-on with SMS authentication • Sign-on with third party credentials ***Note**: Currently, DBG-2000 does not support SMS authentication and e-mail authentication.*
Background	You can either select one of the available backgrounds or can also add an image. Click **Add image** to upload your personalized image for the background.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

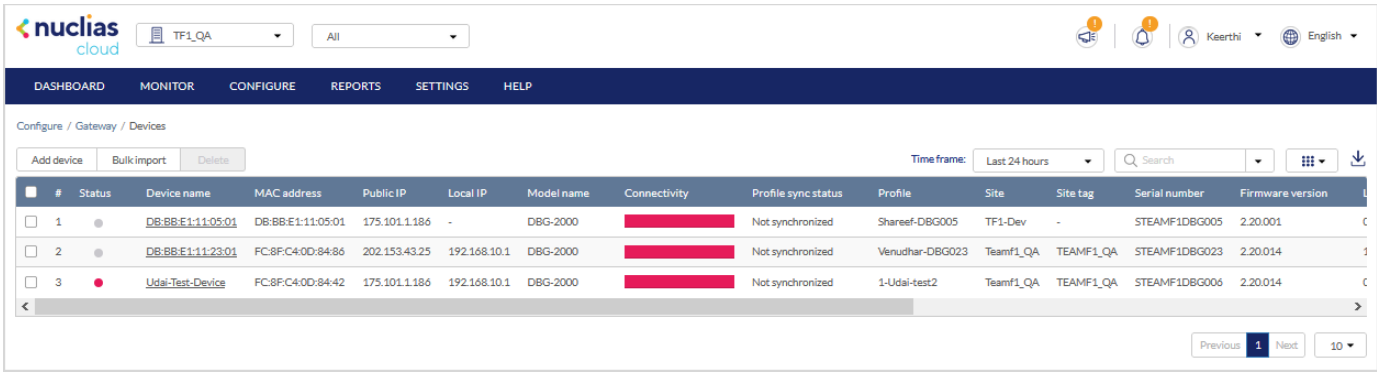


The fields available on the *Splash page editor* page are as follows:

Field	Description
Splash page	It lists all the types of splash pages. Click the required authentication type of the captive portal and add/edit/delete the page.
Header	You can edit the style and format of the splash page header.
Footer	You can edit the style and format of the footer of the splash page.
Click-through	You can edit the style and format of the click-through page. This tab is available when selecting either **Default click-through** or **Default click-through (Japanese)** as the splash page types.
Login	The login page displays the login page based on the selected sign-on splash page type.
Progress	It displays the page showing authentication is in progress.
Landing	It displays the page that appears after successful authentication.
Error	It displays errors to be shown when authentication fails.
Managed files	You can upload user-specific or organization-specific files.
Terms	It displays the terms and conditions that you have to follow while using the captive portal.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

Chapter 1 Basic

This chapter provides an overview of device-related information. To open the *Basic* page, follow the path *Configure* > *Gateway* > *Devices*, i.e., in the **Configure** menu, click **Gateway**, and then click **Devices**. This opens the **Devices** page. It consists of a list of devices present in the device group for the selected time frame. In the **Device Name** column, click any entry to open the *Basic* page of DBG-2000. The *Basic* page displays the following information: Device Information, Location, WAN Interface, and Site and Profile. To save the changes, click **Save**, and to revert to the previous settings, click **Cancel**.



This chapter covers the following topics:

Device Information

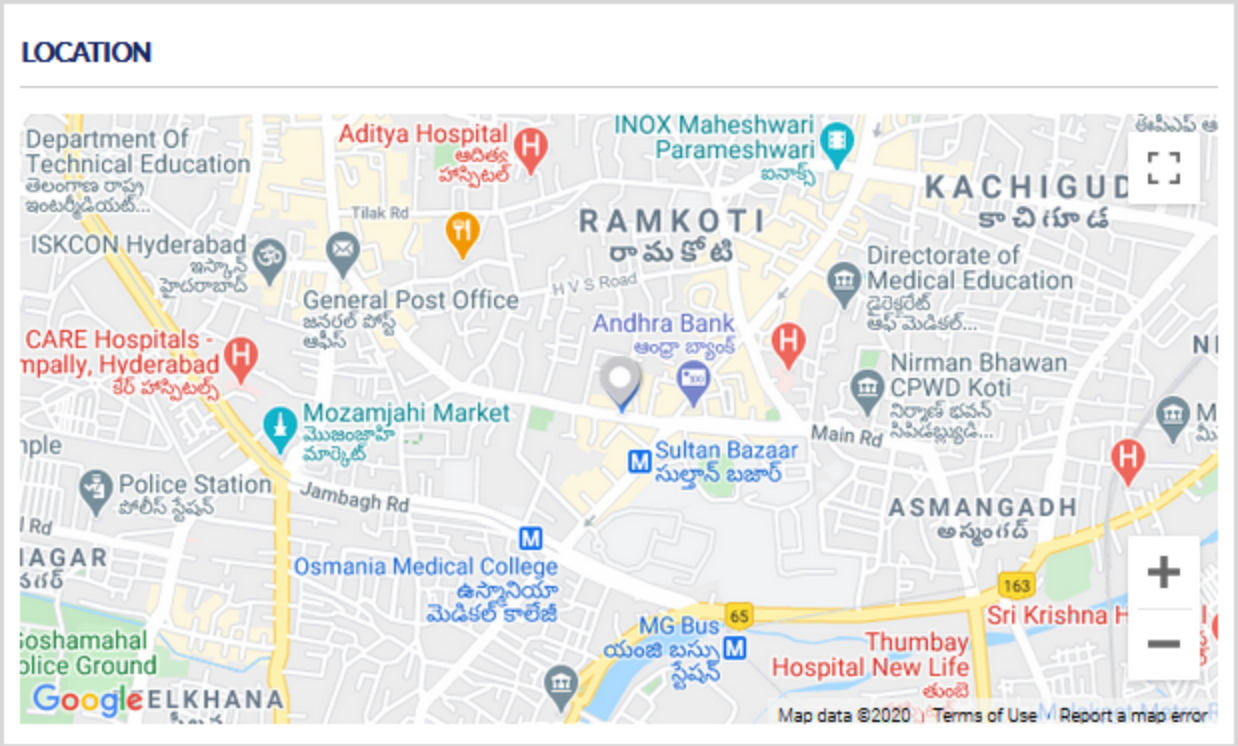
The *Device information* section provides details of the device, like the device name, serial number, MAC address, and local credentials.

The fields available on this page are as follows:

Field	Description
Device name	It indicates the name of the device. You can click and edit the device name.
Model name	It displays the model name of your device.
Device UID	It displays the unique identification of the device generated by the Cloud team for the licensing-related features.
Serial number	It displays the serial number of your device.
Local credentials	It displays the user name and the password to log in to the DBG-2000 web interface.
MAC address	It displays the range of MAC addresses.
Uptime	It displays the time duration since the last reboot.

Location

The *Location* section indicates the place on the map where the device is deployed.



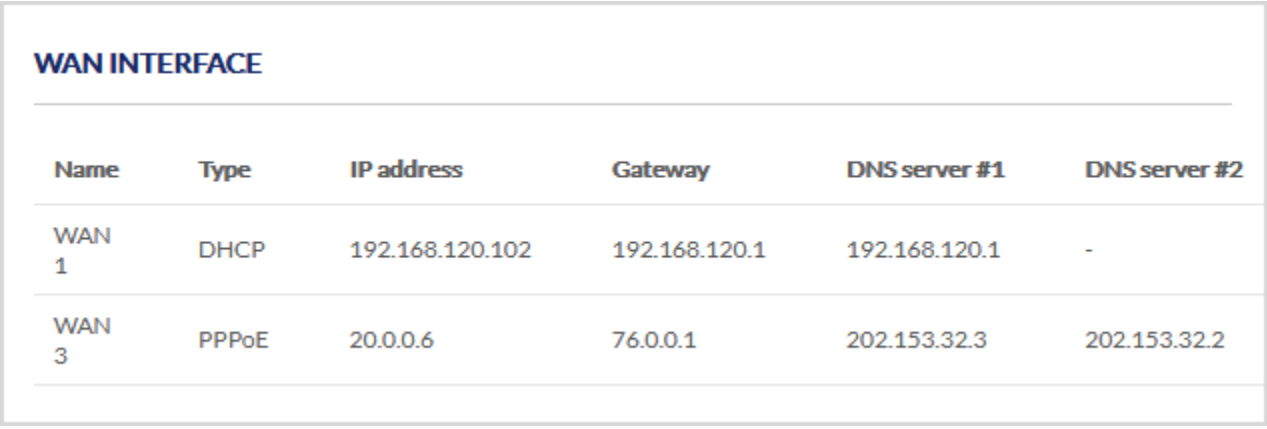
Use any of the following ways to adjust the map size:

- **Cntrl** key + scroll to zoom in or zoom out of the map
- Click "**+**" and "**-**" signs, located at the lower-right corner of the map, to zoom in and zoom out, respectively.

On the upper-right corner, select the full-screen icon to view the map in the full-screen. To exit the full-screen mode, press the **Esc** key or click the shrink icon at the upper-right corner to toggle it to the small screen.

WAN Interface

On the Basic page, this section provides WAN interface details of the device and displays the following information for the respective WAN interface (WAN1, WAN2, and WAN3).



WAN INTERFACE

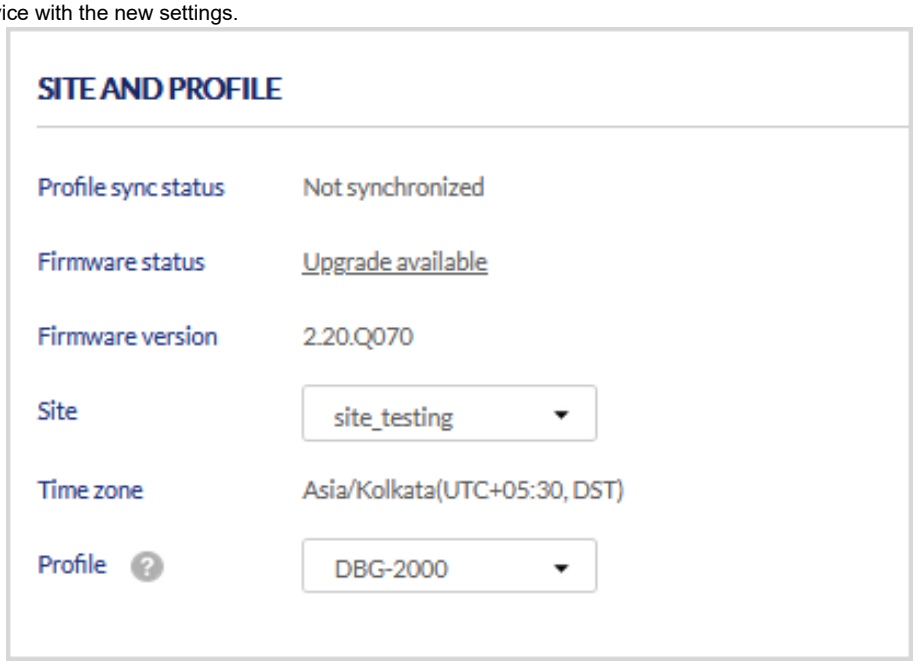
Name	Type	IP address	Gateway	DNS server #1	DNS server #2
WAN 1	DHCP	192.168.120.102	192.168.120.1	192.168.120.1	-
WAN 3	PPPoE	20.0.0.6	76.0.0.1	202.153.32.3	202.153.32.2

Field	Description
Name	It displays the name of the WAN interface.
Type	It displays the type of Internet connection used for the respective WAN port.
IP address	It displays the IP address that is obtained or configured for the WAN interface.
Gateway	It displays the gateway IP address.
DNS Server 1	It displays the IP address of the primary DNS server.

DNS Server 2	It displays the IP address of the secondary DNS server.

Site and Profile

The *Site and Profile* section details the profile synchronization, firmware, and the profile being used. In addition, it allows you to change the profile and re-configure the device with the new settings.



Field	Description
Profile sync status	When you push a configuration and the device is reachable, it displays **Synchronized**, and if the device is not reachable, it displays **Not synchronized**.
Firmware status	This field allows you to know if you have any firmware upgrades available at the server.
Firmware version	It displays the current firmware version running on your device.
Site	It displays the site to which the device belongs.
Time zone	It displays the current time zone of the device.
Profile	It displays the profile configuration applied to the device.

Chapter 2 Summary

This chapter provides port connectivity details of the device DBG-2000. It indicates the amount of the data uploaded or downloaded from the WAN interfaces and tells about Internet usage and its traffic at each port. It also includes an overview of the VPN usage and the VPN status of each VPN type.

This chapter covers the following topics:

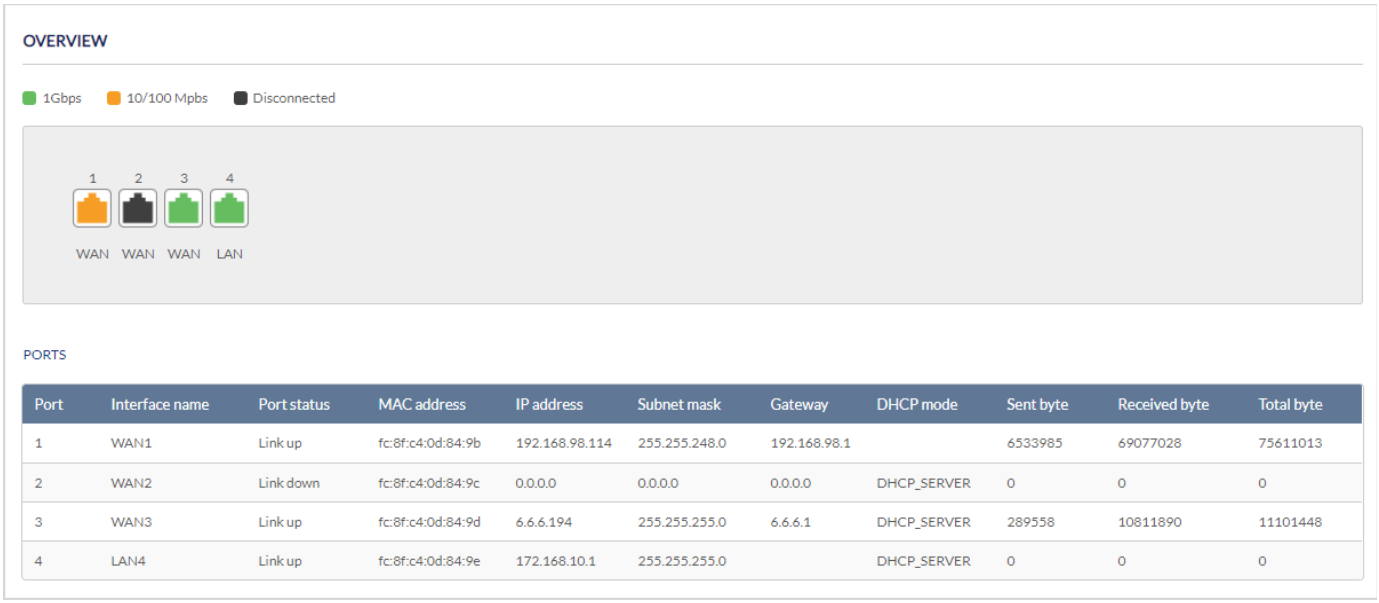
Status

The **Status** tab of the gateway web management interface provides the device's status that includes the port status, Internet traffic, and Internet usage. This page covers the following topics:

- Overview
- Internet Traffic
- Internet Usage

Overview

Under **Overview**, you will find details about all the ports of your device. The connected 1Gbps ports are indicated in **Green** color. If the interface is down, disconnected, or the ports are disabled, they are indicated in **Black**, and the connected 10/100Mbps ports are indicated in **Orange**.



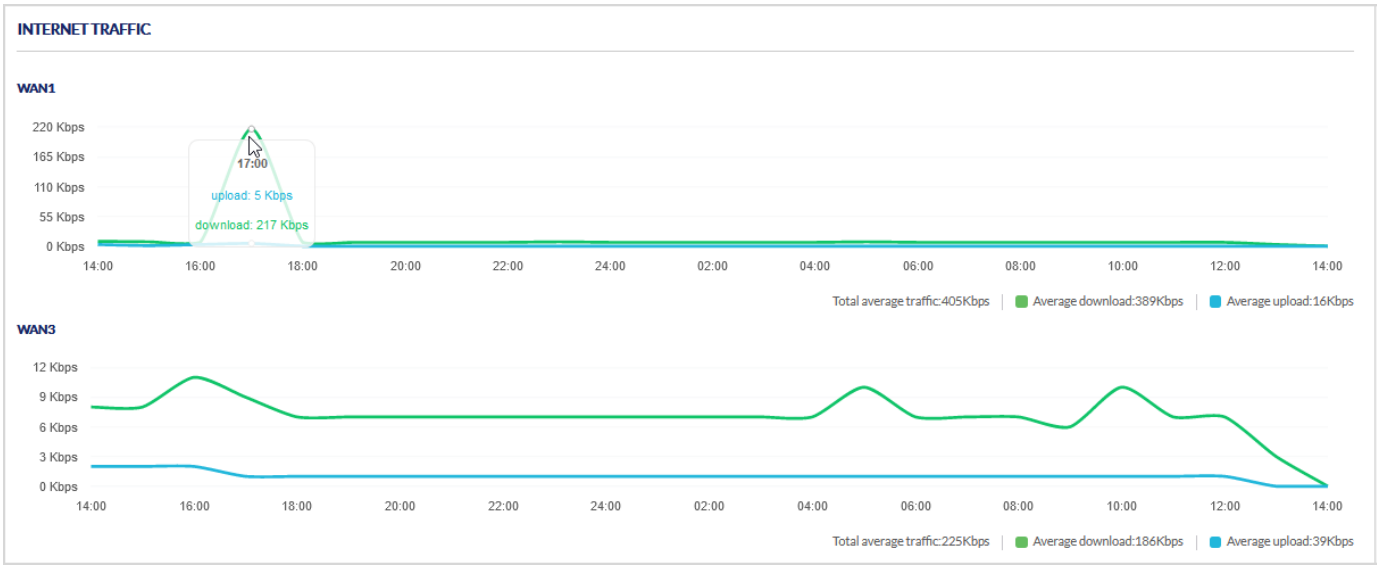
Port	Interface name	Port status	MAC address	IP address	Subnet mask	Gateway	DHCP mode	Sent byte	Received byte	Total byte
1	WAN1	Link up	fc:8f:c4:0d:84:9b	192.168.98.114	255.255.248.0	192.168.98.1		6533985	69077028	75611013
2	WAN2	Link down	fc:8f:c4:0d:84:9c	0.0.0.0	0.0.0.0	0.0.0.0	DHCP_SERVER	0	0	0
3	WAN3	Link up	fc:8f:c4:0d:84:9d	6.6.6.194	255.255.255.0	6.6.6.1	DHCP_SERVER	289558	10811890	11101448
4	LAN4	Link up	fc:8f:c4:0d:84:9e	172.168.10.1	255.255.255.0		DHCP_SERVER	0	0	0

The fields displayed in the *Ports* table are as follows:

Field	Description
Port	It displays the port numbers.
Interface name	It displays the interfaces of the device.
Port status	It displays whether the port links up or links down.
MAC address	It displays the MAC address of the port.
IP address	It displays the IP address of the port.
Subnet mask	It displays the subnet mask of the port.
Gateway	It displays the gateway IP address of the port.
DHCP mode	It displays the DHCP mode for the port. It could be **None**, **DHCP server,** or **DHCP Relay**.
Sent byte	It displays the number of bytes transmitted from this interface.
Received byte	It displays the number of bytes received at this interface.
Total byte	It displays the total number of bytes sent and received at this interface.

Internet Traffic

This section graphically displays the speed of the data at the configured WAN ports for the last 24 hours. It indicates the average download speed and the average upload speed of Internet traffic. When the mouse hovers over the graph, it specifies the upload and download speed at a specific time.

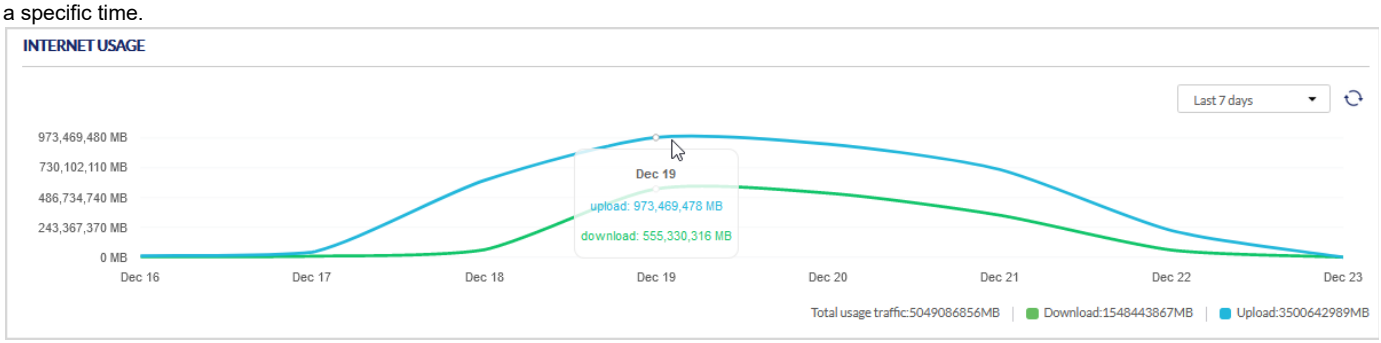


The fields displayed in the Internet traffic graph are as follows:

Field	Description
Total average traffic	It indicates the average of the total traffic moved through the WAN port.
Average download	It indicates the average download speed.
Average upload	It indicates the average upload speed.

Internet Usage

This section displays Internet usage graphically. It indicates the download, upload, and total usage of the Internet for the selected time frame. You may select the time frame from the drop-down list located in the upper-right corner of the graph. To update the graph with the latest data, click the *Refresh* icon next to the *Time frame* box. When the mouse hovers over the graph, it specifies the upload data and the download data at a specific time.



The fields displayed in the Internet usage graph are as follows:

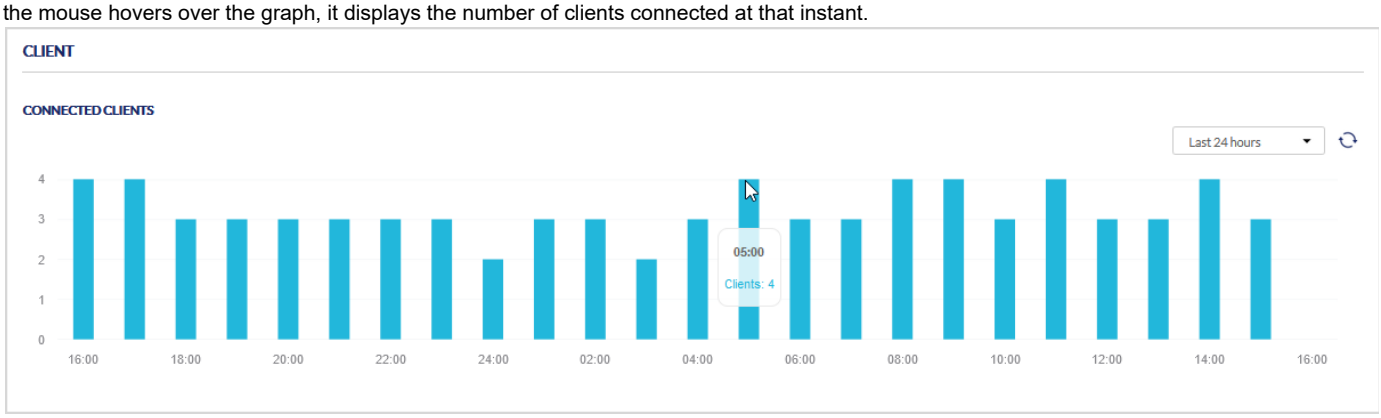
Field	Description
Time frame	Select the duration for which the Internet usage data is displayed.
Total usage traffic	It indicates the total data transferred through the WAN ports for the selected time frame.
Download	It indicates the total downloaded data through the WAN ports for the selected time frame.
Upload	It indicates the total uploaded data through the WAN ports for the selected time frame.

Statistic

The *Statistic* page provides an overview of the number of clients connected to your gateway, the gateway's WAN ports, and the VPN usage. It collects the data from the device and represents it graphically, viz. bar graph or line graph.

Client

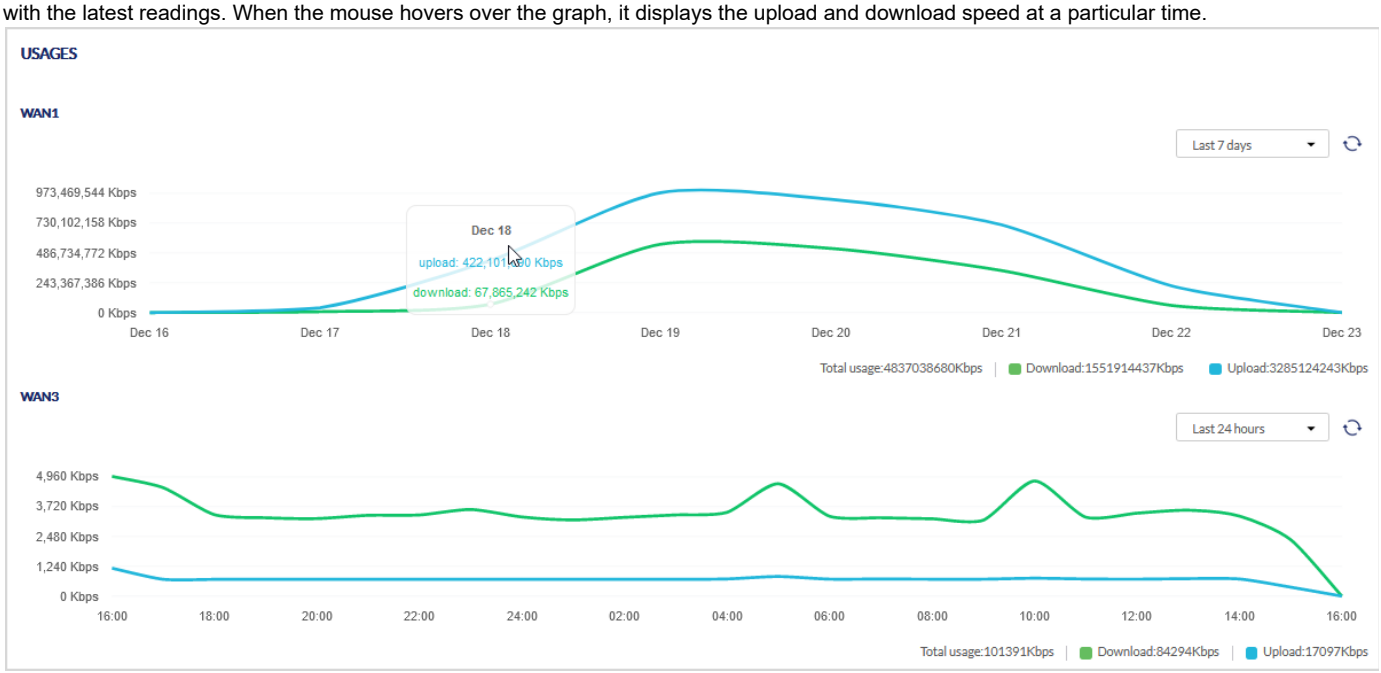
This section displays a bar graph of the number of clients connected to your gateway for the selected time frame. The *Time frame* field allows you to select the number of days you want to see the bar graph. You can click the *Refresh* icon to update the graph with the latest readings. When the mouse hovers over the graph, it displays the number of clients connected at that instant.



Usages

WAN

This section displays the speed at which the data is uploaded or downloaded from the particular WAN port for the selected time frame. You can select the *Time frame* from the drop-down list located in the upper-right corner of the graph and then click the *Refresh* icon to update the graph with the latest readings. When the mouse hovers over the graph, it displays the upload and download speed at a particular time.

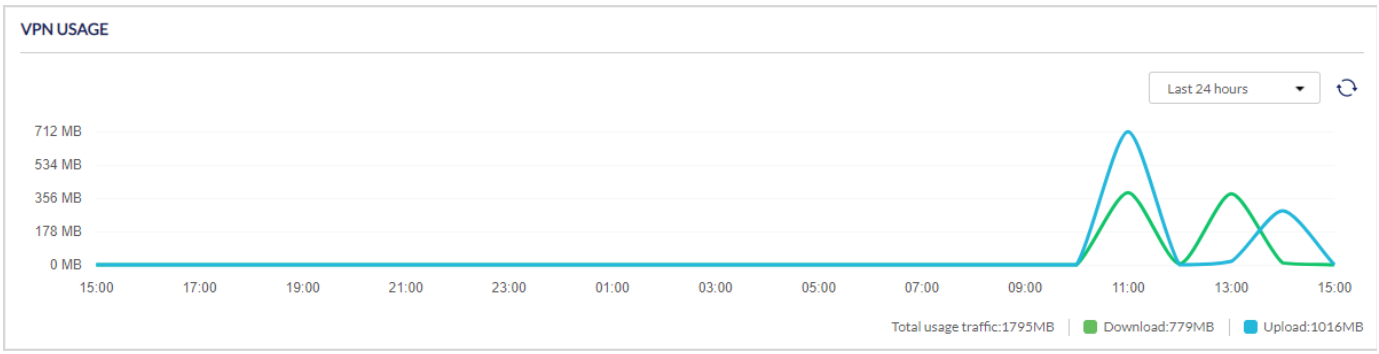


The fields displayed in the *WAN Usage* graph are as follows:

Field	Description
Total usage	It indicates the total speed at which the traffic moved through the WAN port in the selected time frame. It is located at the lower-right corner of the graph.
Download	It indicates the speed at which the data is downloaded through the WAN port in the selected time frame.
Upload	It indicates the speed at which the data is uploaded through the WAN port in the selected time frame.

VPN USAGE

VPN usage displays the total usage of the VPN tunnel for downloading and uploading the data. You can select the *Time frame* to display the VPN usage. When the mouse hovers over the graph, it displays the amount of data uploaded and downloaded through the VPN tunnel at that instant.



The fields displayed in the *VPN usage* graph are as follows:

Field	Description
Total usage	It indicates the total data uploaded and downloaded through the VPN tunnel at the selected time frame.
Download	It indicates the amount of data downloaded through the VPN tunnel at the selected time frame.
Upload	It indicates the amount of data uploaded through the VPN tunnel at the selected time frame.

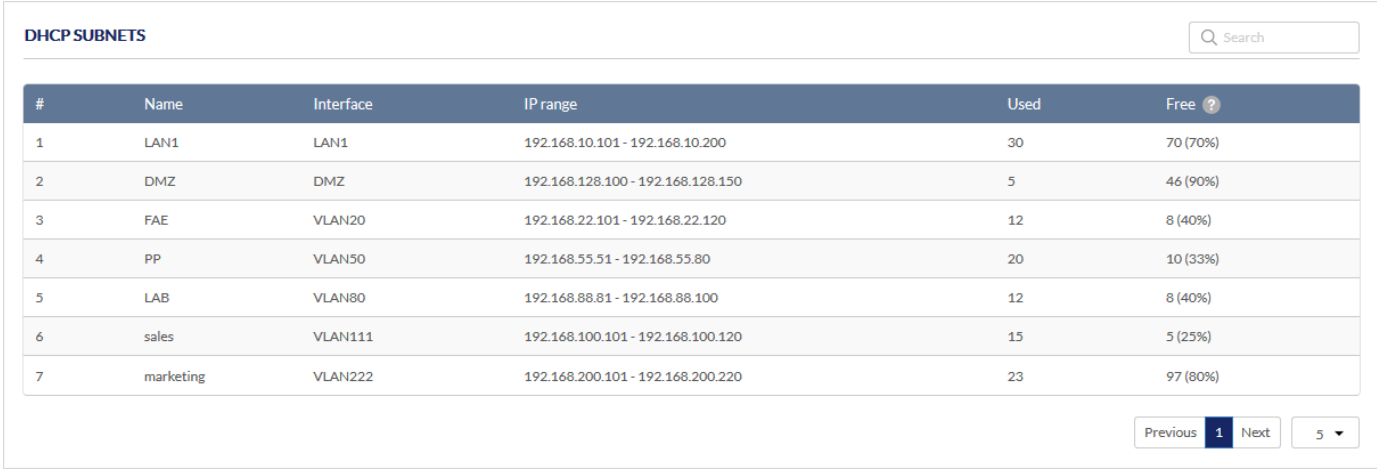
DHCP

The **Dynamic Host Configuration Protocol** (DHCP) simplifies the configuration and management of the IP address of the devices like printers, laptops, desktops, etc., present on the network. This is done by assigning a pool of IP addresses for the devices, and this pool is called the DHCP pool. When a device is added to a network and is asked to get its IP address from the DHCP server dynamically, then one of the IP addresses from the configured DHCP pool, along with the subnet mask and the default gateway, is assigned to the device. These IP addresses are assigned to the clients only for a limited amount of time, and this process is called a **DHCP lease**. The DHCP lease gets renewed on its own after the lease time is expired.

This page of the cloud gateway details the *DHCP subnets* and *DHCP leases* configured on your gateway.

DHCP Subnets

This section provides a list of DHCP subnets specifying their IP address range, the interface on which they have been configured, and the number of free and used IP addresses.



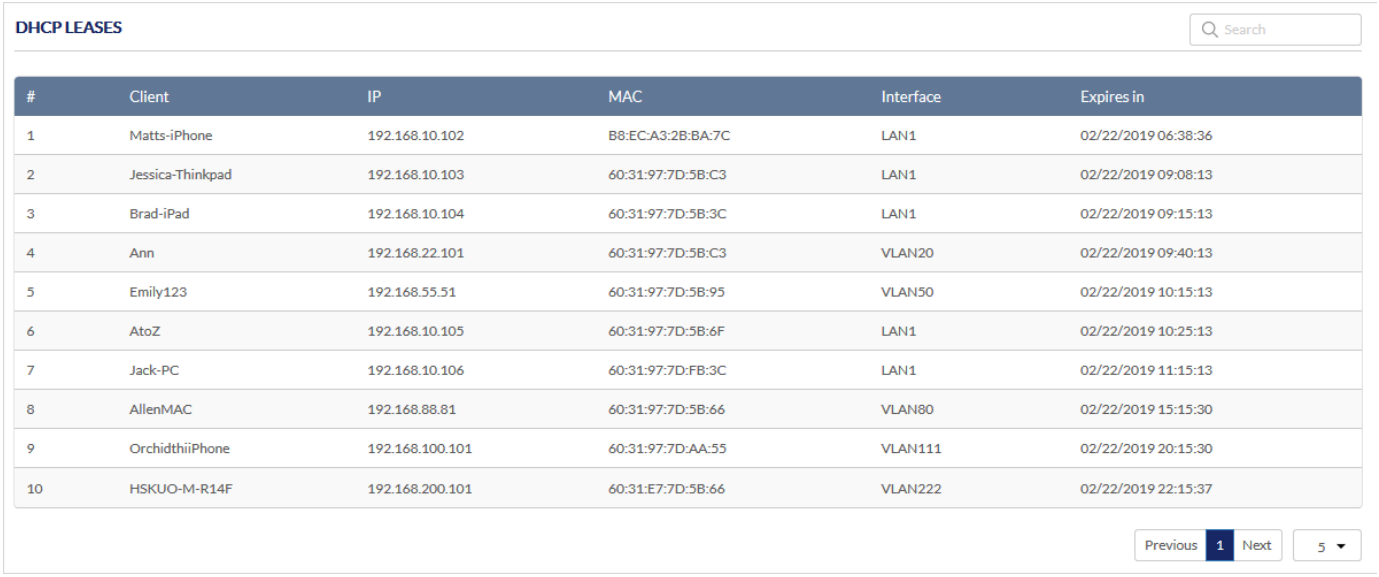
The fields displayed in the *DHCP Subnets* table are as follows:

Field	Description
Name	It displays the name of the DHCP subnet.

Interface	It displays the interface on which the DHCP subnet has been configured.
IP range	It displays the range of IP addresses that can be assigned for lease.
Used	It displays the number of IP addresses being used.
Free	It displays the number of IP addresses that are not assigned to anyone.

DHCP Leases

The *DHCP lease time* refers to the amount of time for which an IP address is assigned to the client by the DHCP server. This section lists all the DHCP leases provided to the clients on the network. It also provides an overview of the interface used and the expiry of each DHCP lease.

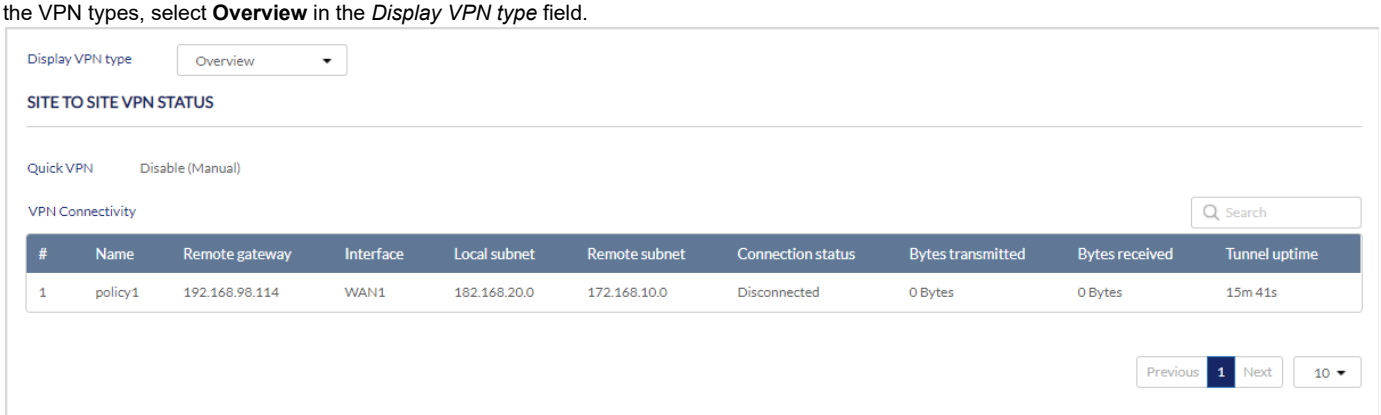


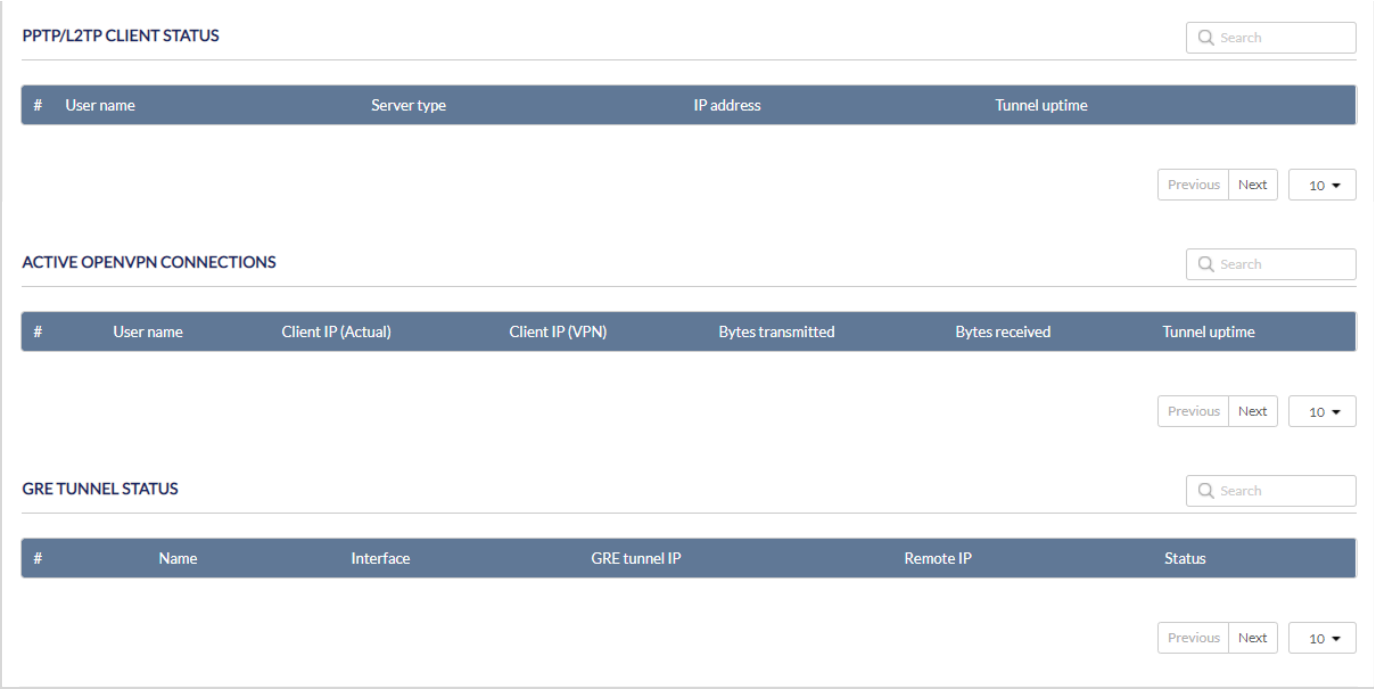
The fields displayed in the *DHCP Leases* table are as follows:

Field	Description
Client	It displays the name of the client to whom the IP address is assigned.
IP	It displays the IP address that has been assigned to the client.
MAC	It displays the MAC address of the client for which an IP address is reserved.
Interface	It displays the interface through which the client is connected.
Expires in	It displays the date and time when the DHCP lease will expire.

VPN Status

You can view the status (connect or disconnect) of the gateway's VPN associations/connections. The page lists the active VPN association or connections, the traffic details, and the tunnel state. The traffic is a cumulative measure of transmitted or received packets since the tunnel was established. You can get an overview of all the VPN types at once and can also view each VPN separately. If you want to display the status of all the VPN types, select **Overview** in the *Display VPN type* field.

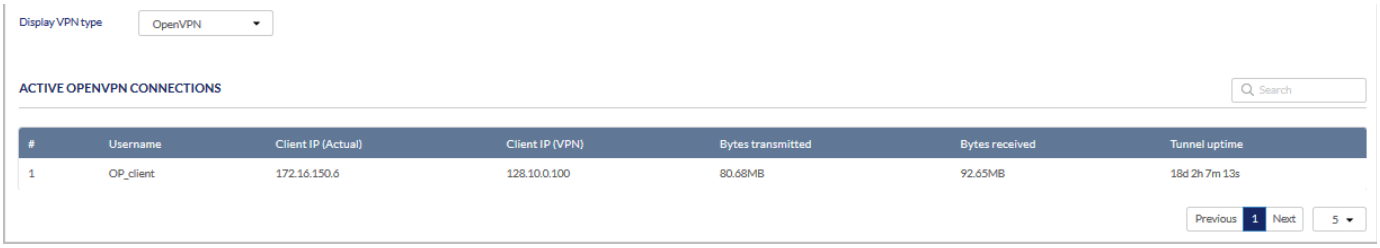




Field	Description
Display VPN type	Select the type of VPN you want to display. The options are given below: • *Overview*: It displays an overview of all the VPN types. • *Quick VPN (Manual)*: It displays only Manual Site-to-Site VPN details. • *Quick VPN (Site-to-Site)*: It displays details of Site-to-Site VPN. • *Quick VPN (Hub-and-Spoke)*: It displays details of Hub-and-Spoke VPN. • *PPTP/L2TP*: It displays PPTP/L2TP Client status details only. • *OpenVPN*: It displays OpenVPN client status only. • *GRE Tunnel*: It displays GRE Tunnel client details only. ***Note:*** *The Manual, Site-to-Site, and Hub-and-Spoke VPNs are available only when any of them are configured on the Site-to-Site VPN page by selecting the VPN type in the "Quick VPN" field.*
Site-to-Site VPN Status	
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 *Disable (Manual)* is selected, set up VPN manually at Manual VPN Configuration to establish VPN connection with other partners.
Disable (Manual)	
Name	It displays the name of the VPN.
Remote gateway	It displays the IP address or the domain name of the remote peer.
Interface	It displays the interface on which the VPN tunnel is established.
Local subnet	It displays the local subnet being used by this VPN connection.
Remote subnet	It displays the remote subnet being used by this VPN connection.
Connection status	It displays if the VPN connection is connected or disconnected.
Bytes transmitted	It displays the number of bytes transmitted through the tunnel.
Bytes received	It displays the number of bytes received through the tunnel.
Tunnel uptime	It displays the time duration when the tunnel is up.

Site-to-Site VPN Status (Site-to-Site)	
Quick VPN	If *Site-to-site* is selected, site-to-site connections between DBG2000 devices of the same organization and their VPN policies are configured by the Nuclias cloud.
Description	It displays the description of the local networks on which the IPSec VPN tunnel has been configured.
Contact point (IP address)	It displays the public IP address through which the device is connected.
Device name	It displays the remote device name of the Site-to-Site tunnel.
IP address	It displays the client's IP (actual) address.
Site	It displays the site name of the remote peer.
Subnet(s)	It displays the remote peer subnets for which the site-to-site VPN tunnel is established.
Connection Status	It displays if the tunnel is connected or disconnected.
Bytes transmitted	It displays the number of bytes transmitted from the tunnel.
Bytes received	It displays the number of bytes received by the tunnel.
Tunnel uptime	It displays the active duration of the tunnel.
Site-to-Site VPN Status (Hub-and-Spoke)	
Quick VPN	Hub-and-Spoke is used when there are multiple gateways sourcing (Spokes) with a central gateway called Hub.
Description	It displays the description of the local networks on which the IPSec VPN tunnel has been configured.
Contact point (IP address)	It displays the public IP address through which the device is connected.
Device name	It displays the device name of the remote peer.
IP address	It displays the IP address of the remote peer with which the tunnel is established.
Site	It displays the site name of the remote peer.
Subnet(s)	It displays the remote peer subnets for which the tunnel will be established.
Role	It displays if the connected client is acting as a hub or a spoke.
Connection Status	It displays if the tunnel is connected or disconnected.
Bytes transmitted	It displays the number of bytes transmitted from the tunnel.
Bytes received	It displays the number of bytes received by the tunnel.
Tunnel uptime	It displays the duration when the tunnel is up.

Field	Description
Username	It displays the PPTP/L2TP user name.
Server type	It displays the server type (PPTP or L2TP) to which the tunnel is established.
IP address	It displays the IP address of the connected PPTP/L2TP client.
Tunnel uptime	It displays the time duration when the tunnel is up.



Field	Description
Active OpenVPN Connections	
User name	It displays the name of the clients connected to the server.
Client IP (Actual)	It displays the IP address through which the client is connected.
Client IP (VPN)	It displays the virtual IP address of the connected client.
Bytes transmitted	It displays the number of bytes transmitted from the tunnel.
Bytes received	It displays the number of bytes received by the tunnel.
Tunnel uptime	It displays the duration when the tunnel is up.

Field	Description
GRE Tunnel Status	
Name	It displays the name of the tunnel.
Interface	It displays the interface where the tunnel is created.
GRE tunnel IP	It displays the IP address of the GRE tunnel.
Remote IP	It displays the IP address of the remote endpoint gateway.
Status	It indicates whether the GRE tunnel is connected or not.

Chapter 3 Network

Click the **Network** tab to edit or configure the network (LAN, WAN, or DMZ). This chapter discusses the various settings required to configure a network. This section's auto-rollover and load-balancing settings allow you to configure an easy and continuous traffic flow in the network. Similarly, the gateway's routing protocols help select an optimum path for traffic to flow from the source to its destination, and the various supported services provide a secure network to its end-users. Traffic management is another important configuration for a network that regulates the traffic flow from LAN to WAN ports. So, this chapter helps you in configuring the network's key elements like ports of the device, routing protocols, services, traffic management, and high availability features.

This chapter covers the following topics:

Ethernet

This section provides an overview of the port status diagrammatically. It indicates the device ports with different colors based on the port connectivity. You can configure WAN, LAN, and DMZ ports on this page. The Nuclias cloud gateway, DBG-2000, supports multiple WAN ports, and hence it allows you to use failover and load-balancing techniques for prioritizing Internet services during an unstable WAN connection.

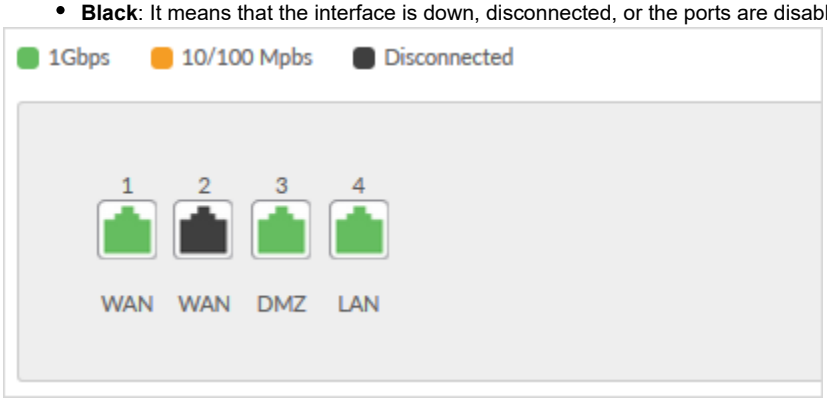
Another feature that the cloud gateway supports is Dynamic DNS (DDNS), i.e., an Internet service that allows routers with varying public IP addresses to be located using Internet domain names. You may also configure the *IP aliasing* feature to associate another IP address with the interface.

The *Ethernet* section includes the following topics:

Port Status

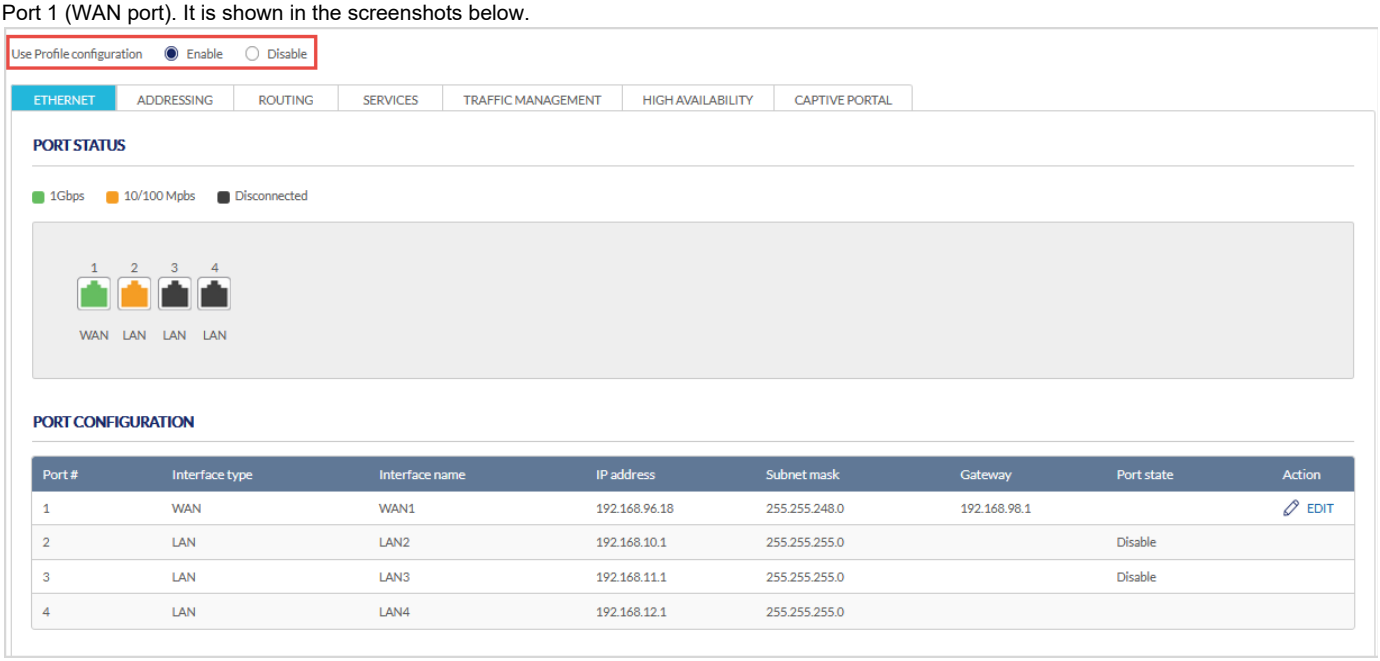
The Ethernet ports, available on the cloud gateway, support 10/100/1000 Mbps, and they use the highest common speed between the sending and the receiving devices. The *Port Status* section displays all the four ports of the device and indicates the connectivity of each port in the following three colors:

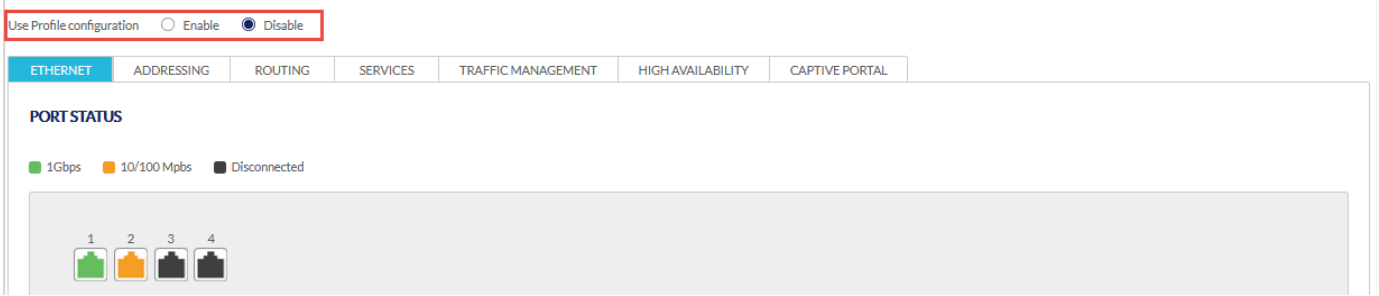
- **Green**: It means that the port transmits at 1Gbps.
- **Orange**: It means that the port transmits at 10/100Mbps.
- **Black**: It means that the interface is down, disconnected, or the ports are disabled.

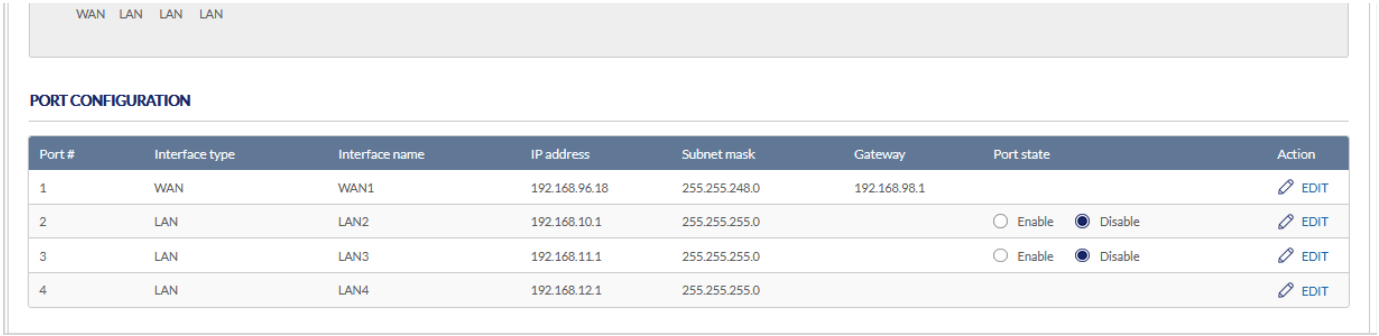


Port Configuration

To configure a port, you must disable the *Use profile configuration* field present above the **Port Status**. If this field is enabled, you can edit only Port 1 (WAN port). It is shown in the screenshots below.







The fields available in the *Port Configuration* table are as follows:

Field	Description
Port	It displays the port number.
Interface type	It displays the type of interface. The options are WAN, DMZ, and LAN.
Interface name	It displays the name of the interface.
IP address	It displays the IP address of the selected port.
Subnet mask	It displays the subnet mask for the IP address.
Gateway	It displays the gateway IP address.
Port state	You can enable or disable the port state only when the *Use profile configuration* field is disabled.
Actions	You can edit all the ports only when the *Use Profile configuration* field is disabled; otherwise, you can edit only Port 1.

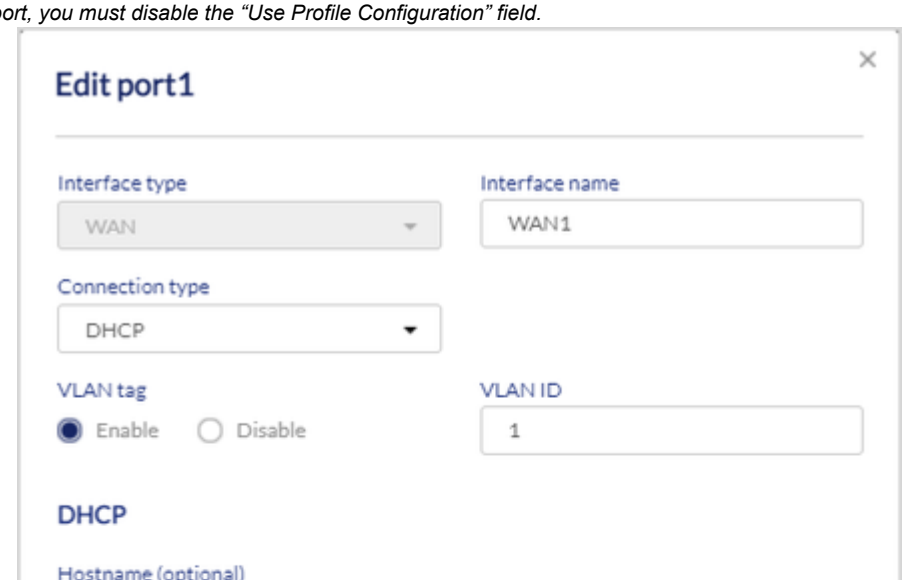
The *Port Configuration* section explains how to configure the following ports:

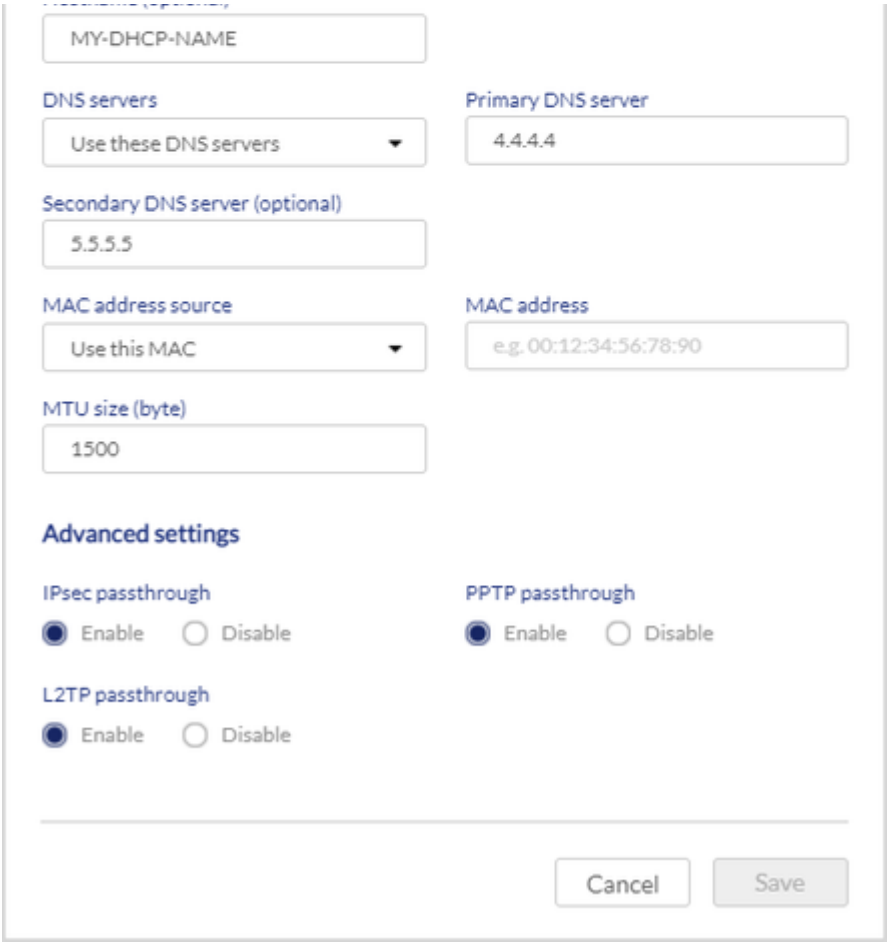
- WAN Port
- DMZ Port
- LAN Port

WAN Port

The gateway has a total of four ports, out of which Port 1, Port 2, and Port 3 can be used as WAN ports to establish a connection to the Internet. Port 1 can only be configured as a WAN port, while Port 2 and Port 3 can be configured as LAN, WAN, or DMZ port. It is assumed that you have arranged for Internet service with your Internet Service Provider (ISP). Please contact your ISP or network administrator for the configuration information required to set up the Nuclias cloud gateway.

You can configure the WAN port in the *Port Configuration* section. Click **Edit** to open the respective port configuration page.
***Note**: To configure the port, you must disable the "Use Profile Configuration" field.*





The fields available on this page are as follows:

Field	Description
Interface type	Select the type of interface. The options are WAN, DMZ, and LAN. ***Note:*** *You can not edit this field for Port 1 and Port 4 interfaces. Port1 can only be configured as a WAN port and Port 4 as a LAN port.*
Interface name	Enter a name for the interface.
Connection type	Select a connection type from the following options: DHCP, Static IP, PPPoE, PPTP, and L2TP.
VLAN tag	Enable or disable the VLAN tag on the configured WAN port.
VLAN ID	If the VLAN tag is enabled, enter the **VLAN ID**.
DHCP	
Hostname (optional)	Enter the hostname if required by your ISP.
DNS Servers	Select either **Get dynamically from ISP** or **Use these DNS servers** to enter DNS servers manually.
Primary DNS server	If you select **Use these DNS servers**, enter the primary DNS server IP address.
Secondary DNS server (optional)	If you select **Use these DNS servers**, enter the secondary DNS server IP address. It is an optional field.
MAC address source	Select **Use default MAC** to use the MAC address from the configured WAN port to associate with your modem/ISP, or **Use this MAC** to enter a MAC address manually.
MAC address	If you select **Use this MAC**, enter the MAC address you want to associate with your ISP.
MTU size (byte)	

	The MTU (Maximum Transmit Unit) is the largest packet that can be sent over the network. The standard MTU value for Ethernet networks is usually 1500 Bytes, and for PPPoE/ PPTP connections, it is 1492 Bytes. For all L2TP connections, it is 1460 Bytes.
Static IP	
IP address	Enter the static address that your ISP assigned to you.
IP subnet mask	Enter the IP subnet mask.
Gateway IP address	Enter the default gateway IP address.
PPPoE configuration	
Address mode	Select either **Dynamic IP** or **Static IP**.
IP address	If you select **Static IP**, enter the IP address supplied to you by your ISP.
IP subnet mask	If you select **Static IP**, enter the subnet mask supplied to you by your ISP.
User name	Enter your PPPoE user name.
Password	Enter your PPPoE password.
Service (Optional)	If your ISP supports the service name, enter it here.
Authentication type	Select the type of Authentication to use (Auto-Negotiate, PAP, CHAP, MS-CHAP, or MS-CHAPv2).
Reconnect mode	Select one of the following options: • **Always on:** The connection is always on. • **On-demand:** The connection is automatically ended if it is idle for a specified number of minutes.
Maximum idle time (minutes)	Enter the number of minutes in the *Maximum idle time* field. This feature is useful if your ISP charges you based on the time you are connected. This field is available only when **On-demand** is selected.
PPTP	
Address mode	Select **Dynamic IP** or **Static IP** (IP settings supplied by your ISP).
Server name	Enter your PPTP server IP address or the domain name.
User name	Enter your PPTP user name.
Password	Enter your PPTP password.
IP address	If you select **Static IP** as the address mode, enter the IP address supplied by your ISP.
IP subnet mask	If you select **Static IP** as the address mode, enter the subnet mask supplied by your ISP.
Gateway IP address	If you select **Static IP** as the address mode, enter the gateway IP address supplied by your ISP.
Static DNS IP	If you select **Static IP** as the address mode, enter the static DNS IP address in the respective subnet.
MPPE encryption	Enable it if the PPTP server supports this feature.
Reconnect mode	Some ISPs may require you to pay for usage time. Select **On-Demand** if this is the case. This will have the gateway connect to the Internet only when you initiate an Internet connection. Select **Always On** to have the gateway stay connected to the Internet.
Maximum idle time (minutes)	Enter the number of minutes in the *Maximum Idle Time* field. This feature is useful if your ISP charges you based on the time that you are connected. This field is available only when **On-demand** is selected.
L2TP	
Address mode	Select **Dynamic IP** or **Static IP** (IP settings supplied by your ISP).
Server name	Enter your L2TP server IP address or the domain name.

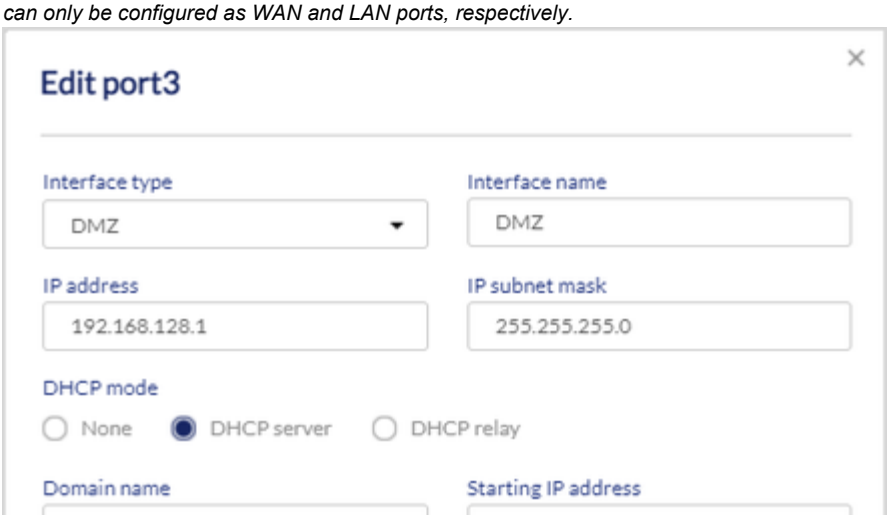
IP address	If you select **Static IP** as the address mode, enter the IP address supplied by your ISP.
IP subnet mask	If you select **Static IP** as the address mode, enter the subnet mask supplied by your ISP.
Gateway IP address	If you select **Static IP** as the address mode, enter the gateway IP address supplied by your ISP.
Static DNS IP	If you select **Static IP** as the address mode, enter the static DNS IP address in the respective subnet.
User name	Enter your L2TP user name.
Password	Enter your L2TP password.
Secret (Optional)	Enter a shared secret if your ISP supports it.
Reconnect mode	Some ISPs may require you to pay for usage time. Select **On-Demand** if this is the case. This will have the gateway connect to the Internet only when you initiate an Internet connection. Select **Always On** to have the gateway stay connected to the Internet.
Maximum idle time (minutes)	Enter the number of minutes in the *Maximum Idle Time* field. This feature is useful if your ISP charges you based on the time that you are connected. This field is available only when **On-demand** is selected.
Advanced settings	
IPSec passthrough	Enable this feature to allow encrypted VPN traffic for IPSec VPN tunnel connections through the device.
PPTP passthrough	Enable this feature to allow encrypted VPN traffic for PPTP VPN tunnel connections through the device.
L2TP passthrough	Enable this feature to allow encrypted VPN traffic for L2TP VPN tunnel connections through the device.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

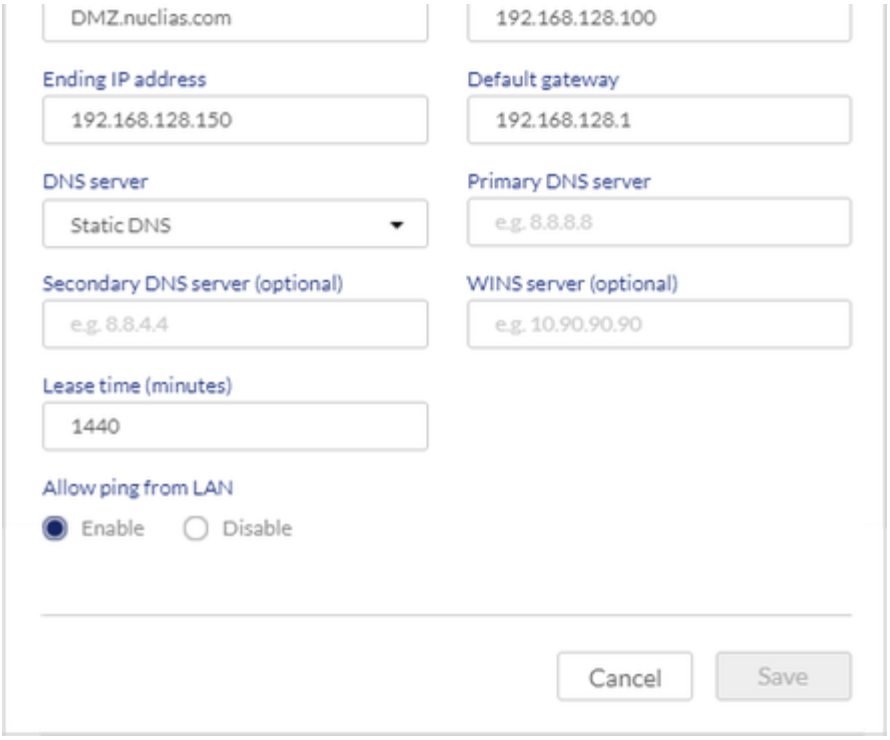
DMZ Port

The gateway supports one of the physical ports to be configured as a dedicated DMZ port. A DMZ is a sub-network that is open to the public but behind the firewall. The DMZ provides security to the network, as specific services/ports exposed to the Internet on the DMZ do not get exposed to the Intranet. Therefore, it is recommended that hosts exposed to the Internet (such as web or email servers) be placed in the DMZ network. Firewall rules can permit access to specific services/ports to the DMZ from LAN or WAN. In an attack on any of the DMZ nodes, the LAN is not necessarily vulnerable. DMZ configuration is identical to the LAN configuration. There are no restrictions on the IP address or subnet assigned to the DMZ port, other than the fact that it cannot be identical to the IP address given to the LAN interface of this gateway.
You can configure Port 2 or Port 3 as DMZ ports in the *Port Configuration* section. Click **Edit** to open the respective port configuration page.

***Note**:*

- *To configure the port, you must disable the "Use profile configuration" field.*
- *Port 1 and Port 4 can only be configured as WAN and LAN ports, respectively.*





The fields available on this page are as follows:

Field	Description
Interface type	Select **DMZ** to configure the port as the DMZ port.
Interface name	Specify the name for your DMZ interface.
IP address	Enter a new IP address for the device.
IP subnet mask	Enter the subnet mask for your network.
DHCP mode	Select one of the following modes: • **None** - Select **None** to turns off DHCP. • **DHCP server** - If this is selected, the gateway will act as the DHCP server on your network. By default, the “DHCP server” is selected as the DHCP mode. • **DHCP relay** - If this is selected, DHCP clients on your network will receive IP address leases from a DHCP server on a different subnet.
Domain name	Enter a domain name for DMZ configuration.
Starting IP address	Enter the starting IP address.
Ending IP address	Enter the ending IP address.
Default gateway	If you select **DHCP Server** as the DHCP mode, enter the default gateway for the DHCP server mode.
DNS server	Select one of the following options for DNS servers for the DHCP clients: • **DNS Proxy**: Enable or disable DNS Proxy. When the DNS Proxy field is selected, the device acts as a proxy for all DNS requests and communicates with the ISP’s DNS servers. • **DNS from ISP**: This option sends all DNS requests to the ISP’s DNS Servers. • **Static DNS**: This option sends all DNS requests to the configured static DNS servers.
Primary DNS server	Enter the primary DNS Server IP address.
Secondary DNS server (optional)	Enter the secondary DNS Server IP address. It is an optional field.
WINS server (optional)	

	Enter the WINS IP address in the DHCP configuration. A WINS (Windows Internet Naming Service Server) is the equivalent of a DNS server but uses the NetBIOS protocol to resolve hostnames. It is an optional field.
Lease time (minutes)	Enter the duration (in minutes) for which IP addresses will be leased to clients.
Relay gateway	Enter the relay gateway IP address. This field is available when you select *DHCP mode* as **DHCP relay**.
Allow ping from LAN	If this option is disabled, the ping requests to the LAN interface are blocked.
DNS Proxy	When the DNS Proxy field is enabled, the device acts as a proxy for all DNS requests and communicates with the ISP's DNS servers. This field is available when you select **DHCP relay** or **None** as the DHCP mode.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

LAN Port

By default, the gateway functions as a Dynamic Host Configuration Protocol (DHCP) server to the hosts present on the LAN network. With DHCP, PCs and other LAN devices can be assigned IP addresses and addresses for DNS servers, Windows Internet Name Service (WINS) servers, and the default gateway. The gateway's IP address serves as the gateway address for LAN clients, with the DHCP server enabled. The PCs in the LAN are assigned IP addresses from a pool of addresses if the DHCP server is configured.

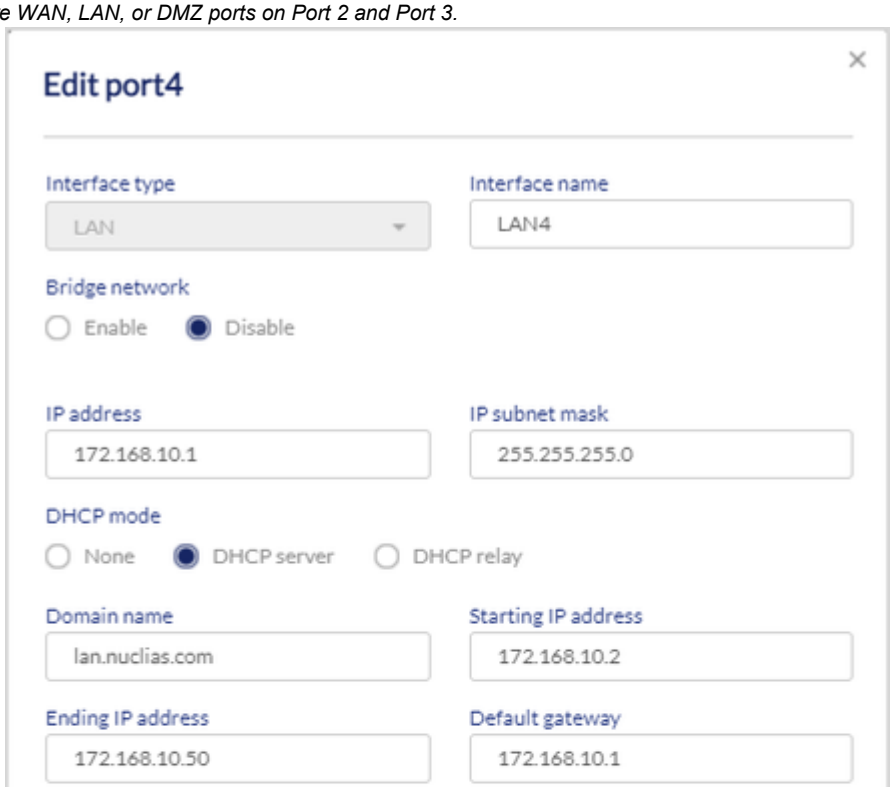
For most applications, the default DHCP and TCP/IP settings are satisfactory. If you want another PC on your network to be the DHCP server or if you are manually configuring the network settings of all of your PCs, set the DHCP mode to "none." DHCP relay can forward DHCP packets to get the DHCP lease information from another DHCP server on the network.

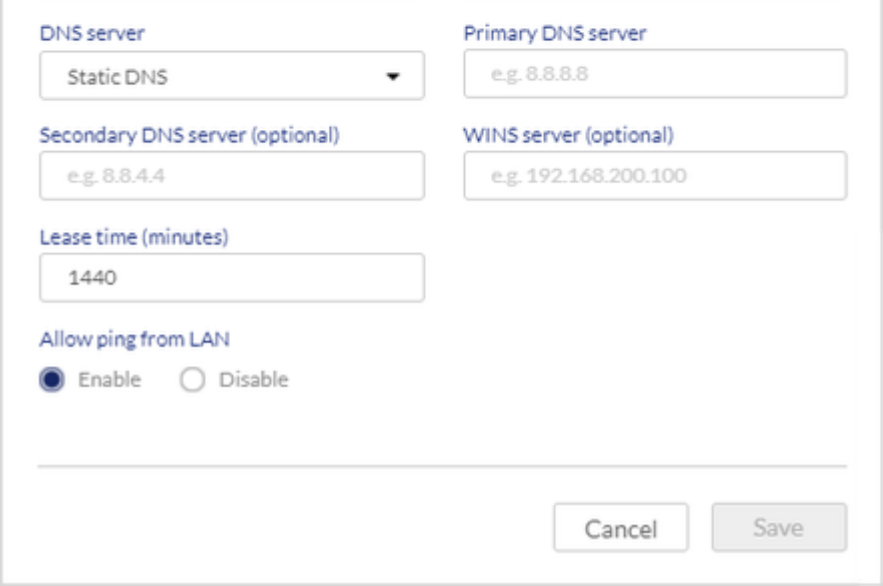
Along with a DNS server, you can also use a Windows Internet Naming Service (WINS) server. A WINS server is the equivalent of a DNS server but uses the NetBIOS protocol to resolve hostnames. The gateway includes the WINS server IP address in the DHCP configuration when acknowledging a DHCP request from a DHCP client.

You can configure the LAN port in the *Port configuration* section. Click **Edit** to open the respective port configuration page.

***Note**:*

- *To configure the port, you must disable the "Use profile configuration" field.*
- *Port 1 and Port 4 are WAN and LAN ports, respectively.*
- *You can configure WAN, LAN, or DMZ ports on Port 2 and Port 3.*





The fields available on this page are as follows:

Field	Description
Interface type	Select **LAN** to configure the port as the LAN port. ***Note:*** *You can not edit this field for Port 1 and Port 4 interfaces. Port1 can only be configured as a WAN port and Port 4 as a LAN port.*
Interface name	Specify the name for your LAN interface.
Bridge network	Enable this field to bridge this LAN to another VLAN.
Network	Select the network from the drop-down list. This field is available when you enable the *Bridge network* field.
IP address	Enter a new IP address for the gateway.
IP subnet mask	Enter the subnet mask for your network.
DHCP mode	Select one of the following modes: • **None** - Select **None** to turns off DHCP. • **DHCP server** - If this is selected, the gateway will act as the DHCP server on your network. By default, the “DHCP server” is selected as the DHCP mode. • **DHCP relay** - If this is selected, DHCP clients on your network will receive IP address leases from a DHCP server on a different subnet.
Domain name	Enter a domain name for LAN configuration.
Starting IP address	Enter the starting IP address.
Ending IP address	Enter the ending IP address.
Default gateway	If DHCP mode is **DHCP server**, enter the default gateway for the DHCP server mode.
DNS server	Select one of the following options for DNS servers for the DHCP clients: • **DNS Proxy**: Enable or disable DNS Proxy on this VLAN. When the DNS Proxy field is selected, the gateway acts as a proxy for all DNS requests and communicates with the ISP’s DNS servers. • **DNS from ISP**: This option sends all DNS requests to the ISP’s DNS Servers. • **Static DNS:** This option sends all DNS requests to the configured static DNS servers.
Primary DNS server	Enter the primary DNS Server IP address.
Secondary DNS server (optional)	Enter the secondary DNS Server IP address. It is an optional field.

WINS server (optional)	Enter the WINS IP address in the DHCP configuration. A WINS (Windows Internet Naming Service Server) is the equivalent of a DNS server but uses the NetBIOS protocol to resolve hostnames. It is an optional field.
Lease time (minutes)	Enter the duration (in minutes) for which IP addresses will be leased to clients.
Relay gateway	Enter the relay gateway IP address. This field is available when you select *DHCP mode* as **DHCP relay**.
Allow ping from LAN	If this option is disabled, the ping requests to the LAN interface are blocked.
DNS Proxy	When the DNS Proxy field is enabled, the gateway acts as a proxy for all DNS requests and communicates with the ISP's DNS servers. This field is available when you select **DHCP relay** or **None** as the DHCP mode.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

WAN Mode Configuration

The Nuclias cloud gateway supports multiple WAN links. This allows you to take advantage of rollover and load balancing features to ensure that certain Internet-dependent services are prioritized in the event of unstable WAN connectivity on one of the ports.
To use Auto-rollover or Load Balancing, you must configure WAN link failure detection. This involves accessing DNS servers on the Internet or ping to an Internet address (user-defined). In load balancing, you can also select *None* to disable the failure detection feature. When the failure detection is enabled, specify the retry interval and the number of attempts it has to connect to the configured server. If all the attempts are failed, the WAN port is considered to be down.

This section discusses the following WAN modes:

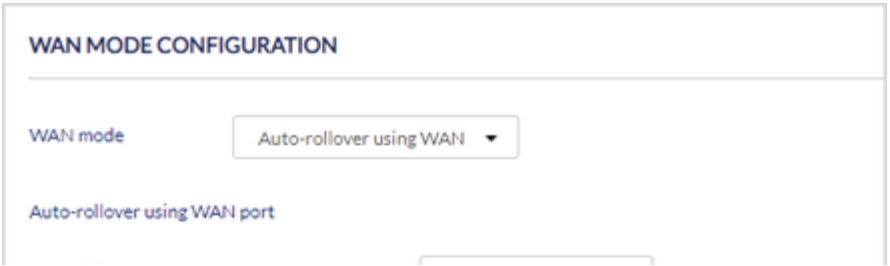
- Primary WAN
- Auto-rollover using WAN
- Load Balancing
  - Round Robin
  - Spillover mode

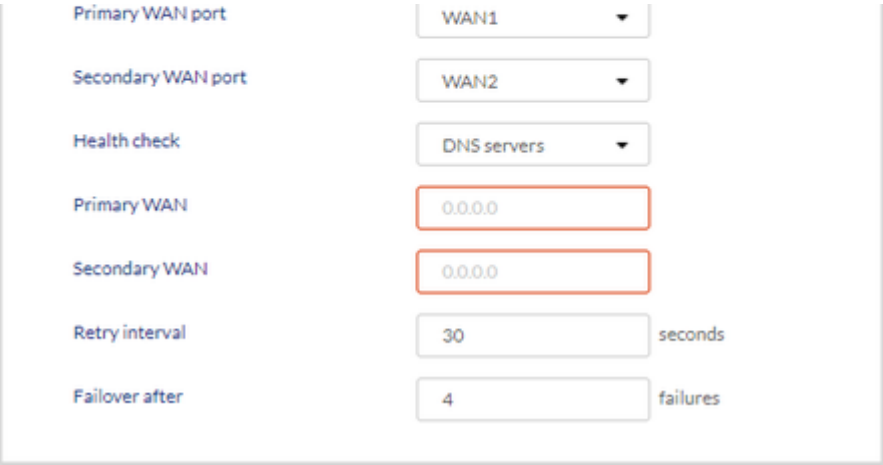
Primary WAN

If you do not want to use Auto-rollover or Load balancing, select **Primary WAN** as the WAN mode and select the WAN port you want to set as the primary WAN port.

Auto-rollover using WAN

In the Auto-rollover using WAN mode, one of the WAN ports is assigned as the primary Internet link for all the Internet traffic; the secondary WAN port is used for redundancy if the primary link goes down for any reason. Both WAN ports (primary and secondary) must be configured to connect to the respective ISP's before enabling this feature. The secondary WAN port will remain unconnected until a failure is detected on the primary link (either port can be assigned as the primary). If a failure occurs on the primary port, the Internet traffic will roll over to the backup port. When configured in Auto-rollover mode, the link status of the primary WAN port is checked at regular intervals as defined by the failure detection settings.





If you want to use Auto-rollover, select *Auto-rollover using WAN* as the WAN mode and enter the following details.

Field	Description
WAN mode	Select *Auto-rollover using WAN*.
Primary WAN port	Select the primary WAN port.
Secondary WAN port	Select the secondary WAN port.
Health check	Select one of the following options for the health check: • **WAN DNS Servers**: If you select this option, it detects the health of a WAN link using the WAN DNS servers configured in the WAN Settings pages. • **DNS Servers**: If you select this option, it detects WAN health by using a specific DNS server. Select DNS Servers and enter the IP addresses of custom DNS servers for the primary and secondary WANs. • **Ping IP address**: If you select this option, ping to an IP address to detect WAN health. Select this option and enter the IP addresses in the fields to ping from the primary and secondary WANs. Ensure that this destination host is reliable.
Primary WAN	Enter the IP address whose health could be checked using the primary WAN port.
Secondary WAN	Enter the IP address whose health could be checked using the secondary WAN port.
Retry interval	Enter the retry time duration in seconds to check the WAN health. By default, it is every 30 seconds.
Failover after	Enter the number of failures after which the port is considered to be down.

Load Balancing

The load balancing feature allows you to simultaneously use multiple WAN links (presumably multiple ISP's). After configuring more than one WAN port, the load balancing option can carry traffic over more than one link. Protocol bindings are used to segregate and assign services over one WAN port to manage Internet flow. The configured failure detection method is used regularly on all the configured WAN ports when in Load Balancing mode.

Load balancing is beneficial when the connection speed of one WAN port greatly differs from another. In this case, you can define protocol bindings to route low-latency services (such as VOIP) over the higher-speed link and let low-volume background traffic (such as SMTP) go over the lower-speed link.
The gateway currently supports two algorithms for Load Balancing:

- **Round Robin**: This algorithm works in a recurring process where the packets are routed to the available WAN ports in a sequence irrespective of the connection speed of any WAN ports. If one packet is forwarded to one WAN port, the next packet will automatically go to the next WAN port. This ensures that the traffic load is distributed among all the active WAN ports.
- **Spillover**: If the Spillover method is selected, one WAN acts as a dedicated link until a defined bandwidth threshold is reached. After this, the next WAN will be used for new connections. Inbound connections on WAN are permitted with this mode, as the spillover logic governs outbound connections moving from one WAN to the other WAN.

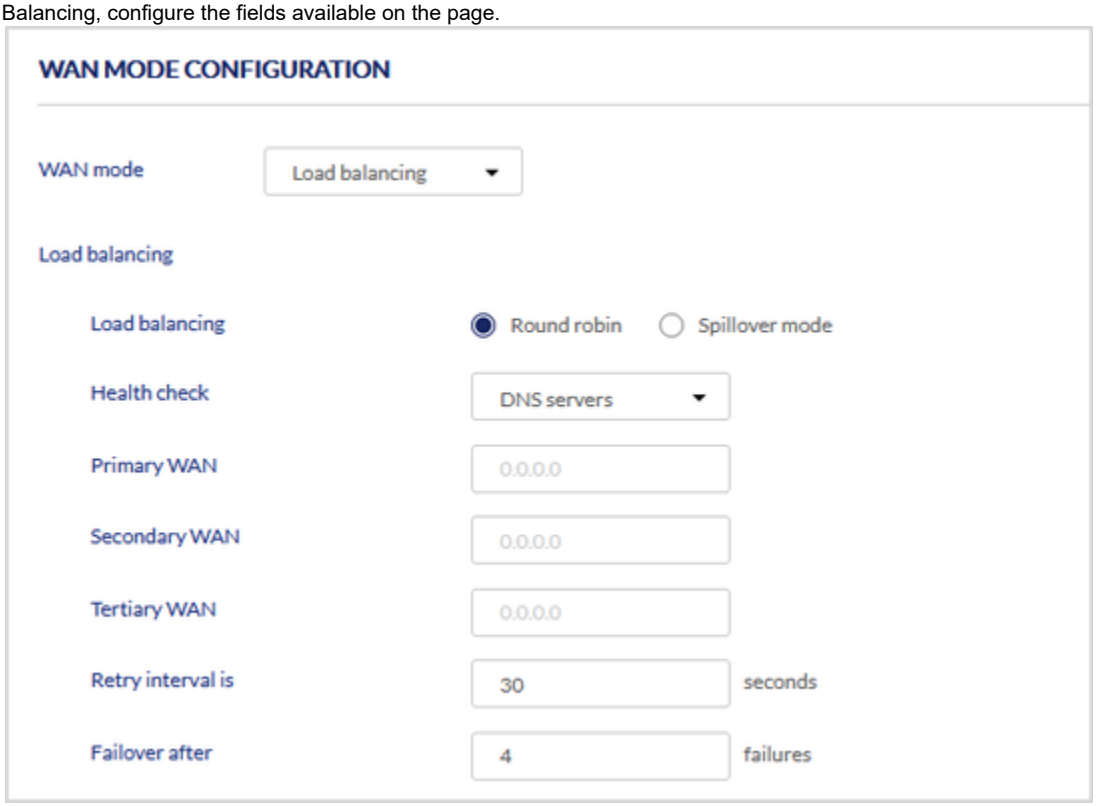
You can configure spillover mode by using the following options:

- **Load Tolerance**: It is the percentage of bandwidth after which the gateway switches to secondary WAN.
- **Max Bandwidth**: This sets the maximum bandwidth tolerable by the primary WAN for outbound traffic.
  If the link bandwidth of outbound traffic goes above the max bandwidth load tolerance value, the gateway will spill over the next connections to the next WAN.

For example, if the maximum bandwidth of a WAN is 1Kbps and the load tolerance is set to 70. Now, every time a new connection is established, the bandwidth increases. After a certain number of connections, say bandwidth reached 70% of 1Kbps, the gateway will spill over new outbound connections to the next WAN. The maximum value of load tolerance is 80%, and the minimum is 20%.

Round Robin

Round robin is an algorithm for load-balancing and is useful when the traffic load is distributed among all the WAN ports. When you select **Round-robin** as Load Balancing, configure the fields available on the page.

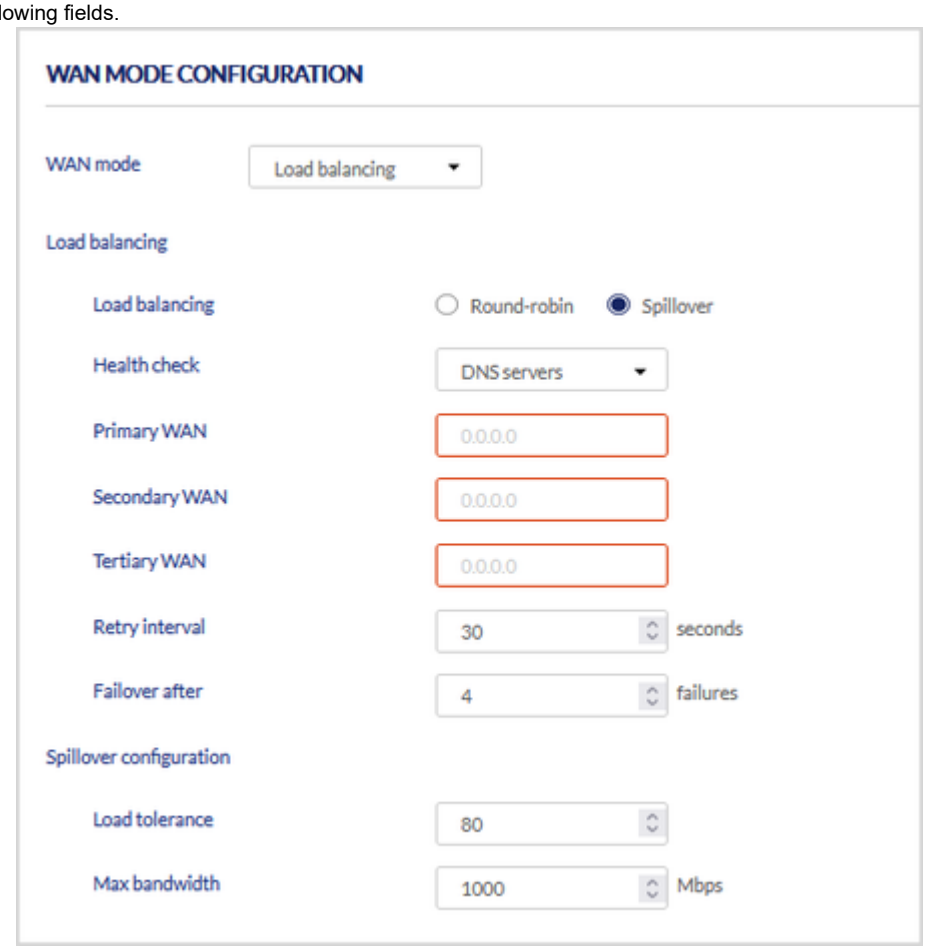


Field	Description
Load balancing	Select **Round robin**.
Health check	Select any one of the following options: • **None**: Select this option if you do not want to check the WAN health. • **WAN DNS Servers**: Select this option to detect the health of a WAN link using the WAN DNS servers configured in the WAN Settings page. • **DNS Servers**: Select this option to use a specific DNS server for detecting WAN health, select DNS Servers, and enter the IP addresses of custom DNS servers for the primary, secondary, and tertiary WAN ports. • **Ping IP address**: Select this option to detect WAN health by pinging to an IP address, select this option, and enter the IP addresses in the fields to ping from the primary, secondary, and tertiary WAN ports.
Primary WAN	Enter the primary DNS server or primary IP address to ping.
Secondary WAN	Enter the secondary DNS server or secondary IP address to ping.
Tertiary WAN	Enter the tertiary DNS server or tertiary IP address to ping. This field is available only when all three WANs are configured.
Retry interval is	Enter the retry time duration in seconds to check the WAN health. By default, it is every 30 seconds.

Failover after	Enter the number of failures after which the port is considered to be down.

Spillover mode

Select **Spillover mode** when you want a specific WAN to act as a dedicated link until a defined bandwidth threshold is reached. After this, the next WAN is used for new connections. When you select Spillover mode, configure the following fields.



Field	Description
Load balancing	Select **Spillover mode**.
Health check	Select any one of the following options: • **None**: Select this option if you do not want to check the WAN health. • **WAN DNS Servers**: Select this option to detect the health of a WAN link using the WAN DNS servers configured in the WAN Settings page. • **DNS Servers**: Select this option to use a specific DNS server for detecting WAN health. Select DNS Servers and enter the IP addresses of custom DNS servers for the primary, secondary, and tertiary WAN ports. • **Ping IP address**: Select this option to detect WAN health by pinging to an IP address. Enter the IP addresses in the fields to ping from the primary, secondary, and tertiary WAN ports.
Primary WAN	Enter the primary DNS server or primary IP address to ping.
Secondary WAN	Enter the secondary DNS server or secondary IP address to ping.
Tertiary WAN	Enter the tertiary DNS server or tertiary IP address to ping. This field is available only when all three WANs are configured.
Retry interval is	Enter the retry time duration in seconds to check the WAN health. By default, it is every 30 seconds.

Failover after	Enter the number of failures after which the port is considered to be down.
Spillover Configuration	
Load tolerance	Enter the percentage of bandwidth, after which the gateway switches to the next WAN. The range is from 20 to 80.
Max bandwidth	This sets the maximum bandwidth tolerable by WAN for outbound traffic. The range of maximum bandwidth is from 1 to 1000 Mbps.

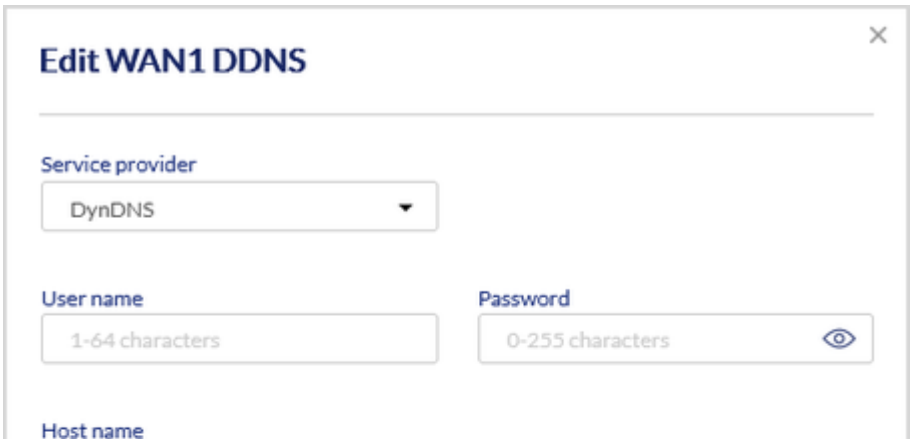
Dynamic DNS

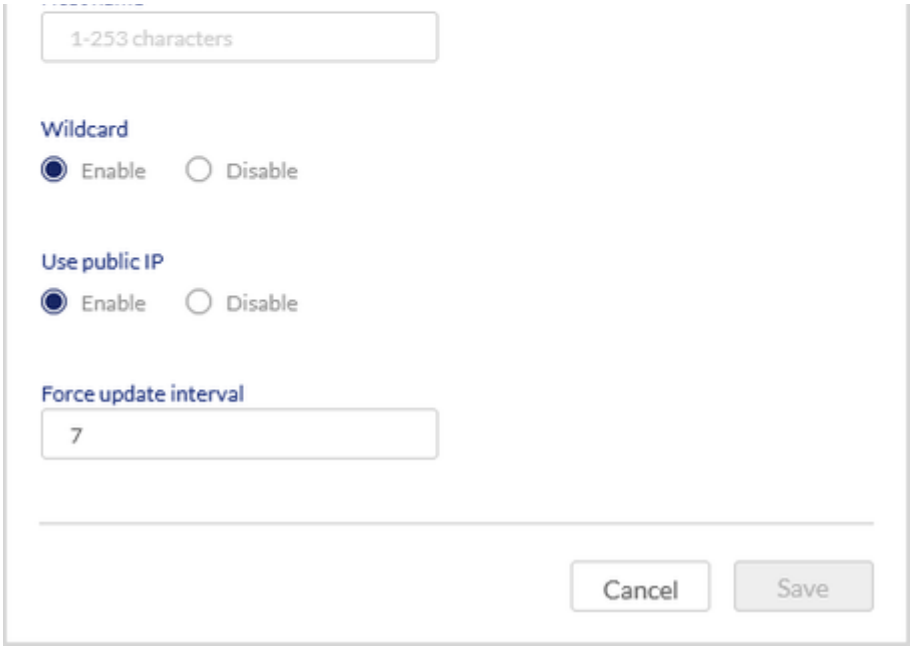
Dynamic DNS (DDNS) is an Internet service that allows routers with varying public IP addresses to be located using Internet domain names. To use DDNS, you must set up an account with a DDNS provider such as DynDNS, FreeDNS, NO-IP, or 3322.org.

Each configured WAN can have a different DDNS service if required. Once configured, the gateway will update DDNS services changes in the WAN IP address. It will direct the features dependent on accessing the gateway's WAN via FQDN to the correct IP address. When you set up an account with a DDNS service, the host and domain name, user name, password, and wildcard support will be provided by the account provider.

When the DDNS feature is enabled, it is applied to the WAN IP, which is up, and the following fields are displayed in the table:

Field	Description
Index	It displays the serial number of the entries.
WAN interface	It displays the WAN interface on which the DDNS is applied.
Service provider	It displays the service types that this WAN port is using.
Hostname	It displays the hostname to be mapped with the WAN interface IP in the selected DDNS service.
Wildcard	It indicates if the Wildcard feature is enabled or disabled.
Use public IP	It displays if this option is enabled or disabled. Enabling this option would use an external (NAT router's) IP address instead of the device's WAN IP address.
Force update interval	It specifies the periodic update interval to automate the gateway to update the host information on the selected DDNS Service.
DDNS status	It displays the DDNS status of the WAN port.
Actions	Click **Edit** to edit the configuration. This opens the *Edit WAN1/WAN2/WAN3 DDNS* page.



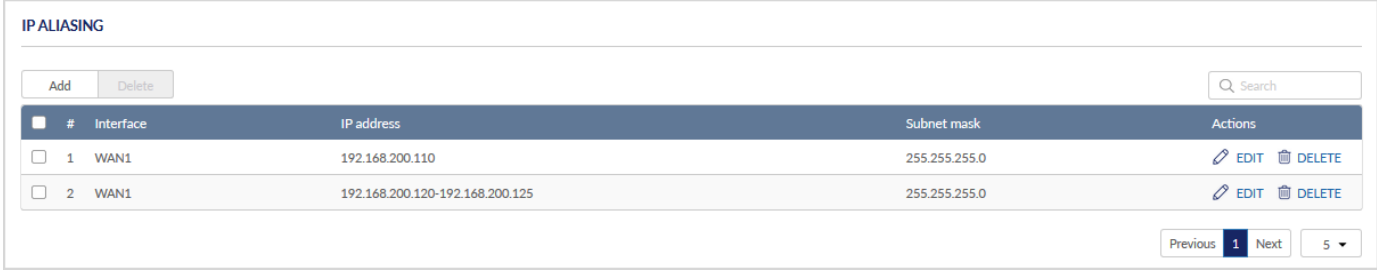


The fields available on this page are as follows:

Field	Description
Service provider	Select one of the following service types that this WAN port should use: DynDNS, FreeDNS, NO-IP, 3322.org, and Disable.
User name	Enter the account user name for the following service providers: DynDNS, FreeDNS, NO-IP, and 3322.org.
Password	Enter the password for the above service providers' accounts.
Hostname	Specify the complete hostname which is to be mapped with the WAN interface IP in the selected DDNS service.
Wildcard	The wildcard feature allows all sub-domains of your DynDNS or 3322.org Hostname to share the same public IP as the hostname. This option can be enabled here if not done on the DynDNS website. This field is available when you select **DynDNS** or **3322.org** as the Service provider.
Use public IP	Enabling this option would use an external (NAT router's) IP address instead of the device's WAN IP address.
Force update interval	Specify the periodic update interval to automate the gateway to update the host information on the selected DDNS Service.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

IP Aliasing

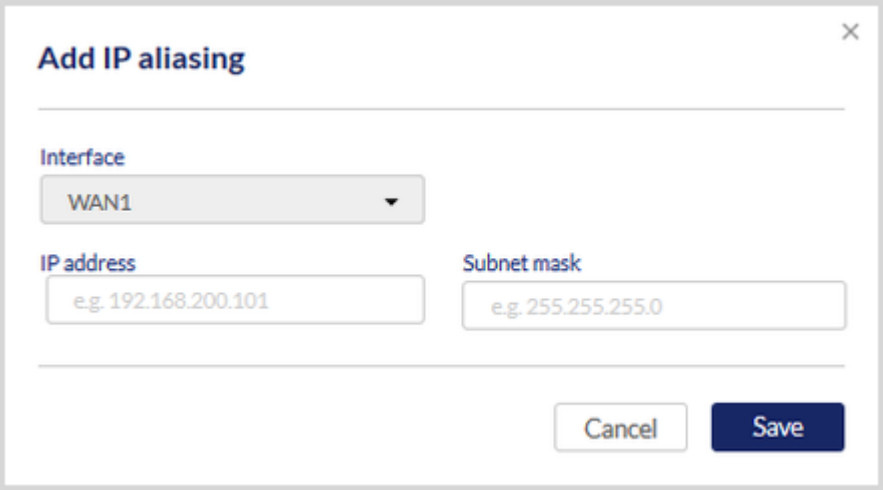
A single WAN Ethernet port can be accessed via multiple IP addresses by adding an alias to the port. This is done by configuring an IP Alias address. The IP aliasing section lists the configured IP aliases on the WAN interfaces. You can add a new IP alias and edit or delete the configured IP alias.



The fields displayed on the *IP aliasing* table are as follows:

Field	Description
Interface	It displays the WAN port on which the IP alias is configured.
IP address	It displays an alias IP address for the WAN interface you selected.
Subnet mask	It displays the subnet mask for the WAN interface you selected.
Actions	You can edit or delete that entry. *Note: This column is available only when you disable the "Use profile configuration" field.*

To delete multiple entries at once, select the checkboxes of the *IP aliasing* you want to delete, and click **Delete**. Click **Add** to add a new IP alias. This opens the *Add IP aliasing* page.



The fields available on this page are as follows:

Field	Description
Interface	Select the WAN port.
IP address	Enter an alias IP address for the WAN interface you selected.
Subnet mask	Enter a subnet mask for the WAN interface you selected.
Save	Click **Save** to save your settings.
Close	Click **Close** to revert to the previous settings.

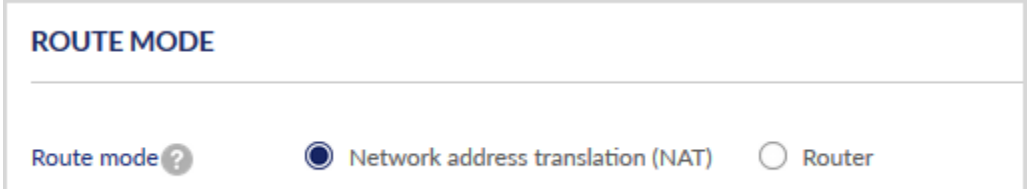
Addressing

The *Addressing* section introduces various features that the Nuclias cloud gateway uses to handle traffic flow between the Internet and the secure LAN. To limit broadcast packets of a device in a large network, the gateway supports Virtual LANs. These virtual LANs assign VLAN IDs to the LAN ports to isolate that port's traffic from the general LAN. You will learn about all these topics in detail in this section.

The *Addressing* section covers the following topics:

Route mode

Routing between the LAN and WAN will impact how this gateway handles traffic received on any of its physical interfaces. The routing mode of the gateway is core to the traffic flow behavior between the secure LAN and the Internet.



With Router (classical routing), devices on the LAN can be directly accessed from the Internet with their public IP addresses (assuming appropriate firewall settings are configured). If your ISP has assigned an IP address for each of the computers/devices you use, select **Router**.

Network address translation (NAT) is a technique that allows several computers and devices on your local network to share an Internet connection. The computers on the LAN use a “private” IP address range, while the WAN port on the gateway is configured with a single “public” IP address. Along with connection sharing, NAT also hides internal IP addresses from the computers on the Internet. NAT is required if your ISP has assigned only one IP address to you. The computers/devices that connect through the gateway will need to be assigned IP addresses from a private subnet.

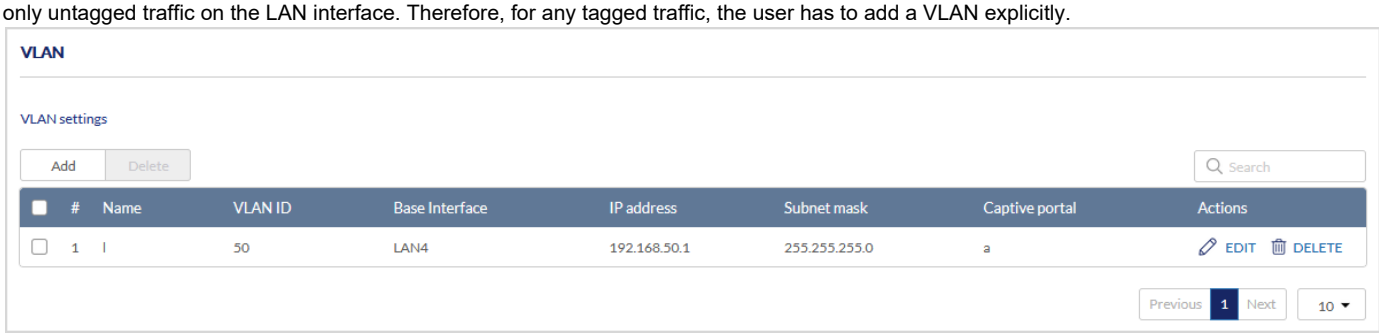
VLAN

The gateway supports virtual network isolation on the LAN by using VLANs. You can configure LAN devices to communicate in a sub-network defined by VLAN identifiers. A unique VLAN ID can be assigned for each LAN port so that traffic to and from the physical port can be isolated from the general LAN.

VLAN filtering is advantageous to limit broadcast packets of a device in a large network. In the *Add VLAN profile* page, define the virtual network.

VLAN Settings

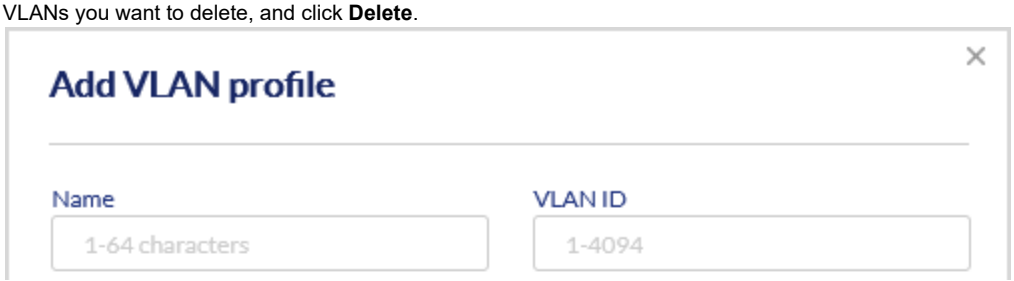
The *VLAN settings* section displays a list of configured VLANs by name and VLAN ID. A VLAN membership can be created by clicking the **Add** button present above the list.
The cloud gateway supports LAN ports with different subnets for each LAN, i.e., for port 4, the assigned IP address is 192.168.10.1, for port 3, it is 192.168.11.1, and for port 2, it is 192.168.12.1. The VLAN ID value can be any number from 1 to 4094. By default, the cloud gateway accepts only untagged traffic on the LAN interface. Therefore, for any tagged traffic, the user has to add a VLAN explicitly.

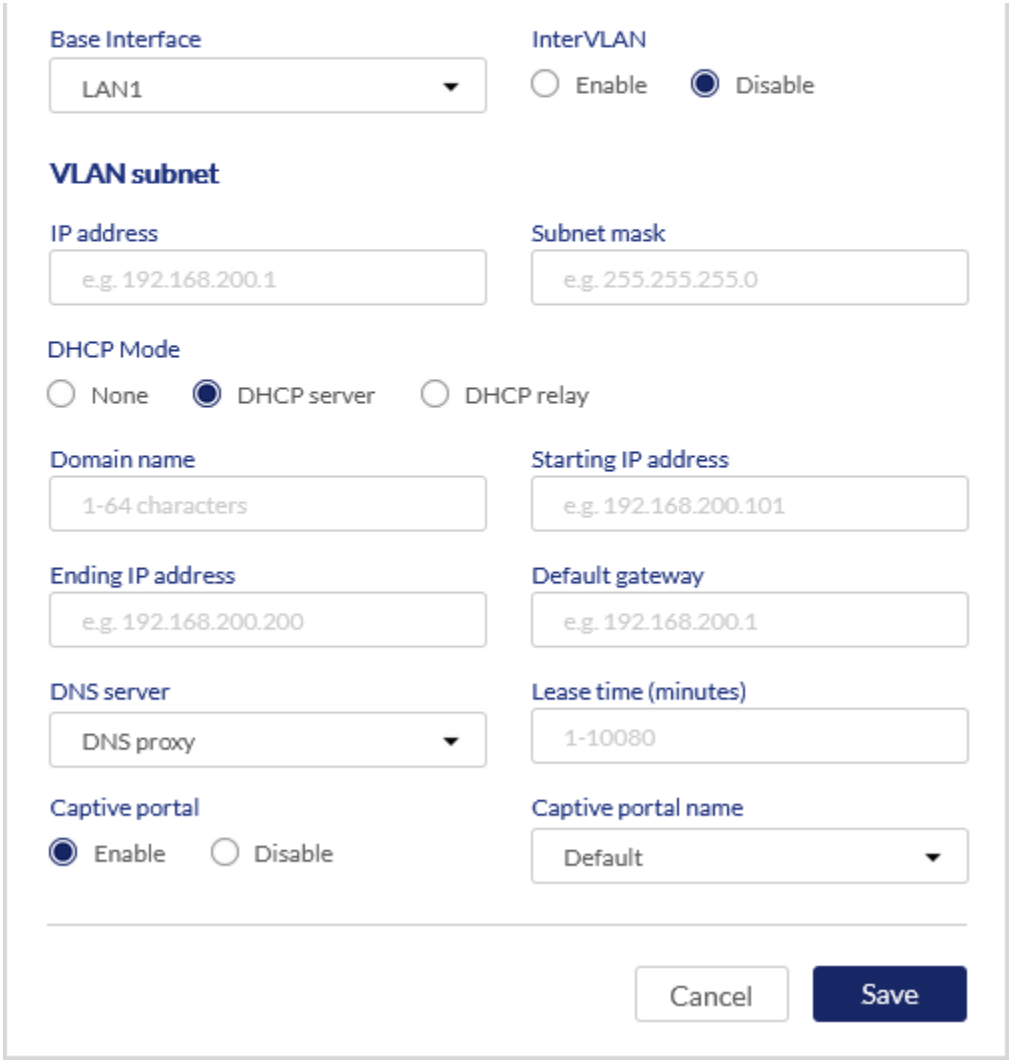


The fields available on the *VLAN settings* table are as follows:

Field	Description
Name	It displays the name of the VLAN.
VLAN ID	It displays the numeric value associated with the VLAN.
Base Interface	It displays the physical interface on which the VLAN is created.
IP address	It displays the IP address for the VLAN.
Subnet mask	It displays the subnet mask for the VLAN.
Captive portal	If the captive portal is enabled on the VLAN, this field displays the name of the captive portal.
Actions	You can edit or delete the respective VLAN. *Note: This field is available only when the “Use profile configuration” field is disabled.*

Click **Add** to add a new VLAN. This opens the *Add VLAN profile* page. To delete multiple entries at once, select the checkboxes of the configured VLANs you want to delete, and click **Delete**.





The fields available on the *Add VLAN profile* page are as follows:

Field	Description
Name	Enter a unique name for this VLAN.
VLAN ID	Enter a unique ID to this VLAN (1 - 4094).
Base Interface	Select the physical interface on which VLAN is to be created.
InterVLAN	It allows or denies communication between VLAN networks.
VLAN subnet	
IP address	Enter an IP address for the VLAN subnet.
Subnet mask	Enter the subnet mask for the VLAN subnet.
DHCP mode	Select one of the following modes: • **None:** Select **None** to turns off DHCP. • **DHCP Server:** If this is selected, the device will act as the DHCP server on your network. • **DHCP Relay:** If this is selected, DHCP clients on your network will receive IP address leases from a DHCP server on a different subnet.
Domain name	Specify the domain name. This field is available only when **DHCP Server** is the *DHCP Mode*.
Starting IP address	Enter the starting IP address.

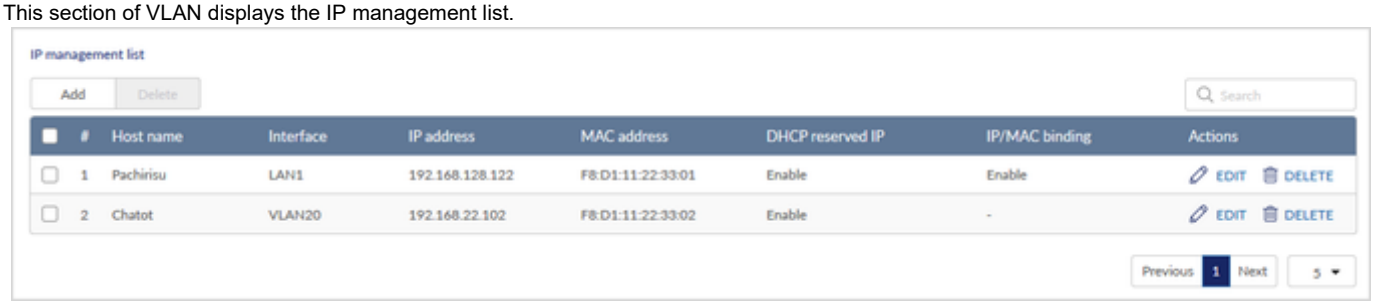
Ending IP address	Enter the ending IP address.
Default gateway	If *DHCP mode* is **DHCP Server**, enter the default gateway for the DHCP server mode.
DNS server	Select one of the following options for DNS servers for the DHCP clients: • **DNS Proxy**: Enable or disable DNS Proxy on this VLAN. If enabled, the gateway acts as a proxy for all DNS requests and communicates with the ISP's DNS servers. • **DNS from ISP**: This option sends all DNS requests to the ISP's DNS Servers. • **Static DNS:** This option sends all DNS requests to the configured static DNS servers.
Primary DNS server	Enter the primary DNS Server IP address.
Secondary DNS server	Enter the secondary DNS Server IP address.
WINS server (optional)	Enter the WINS IP address in the DHCP configuration. A WINS (Windows Internet Naming Service Server) is the equivalent of a DNS server but uses the NetBIOS protocol to resolve hostnames. It is an optional field.
Lease time (minutes)	Enter the duration (in minutes) for which IP addresses will be leased to DHCP clients.
Relay gateway	Enter the relay gateway IP address.
Captive portal	You can enable or disable the captive portal feature over the VLAN.
Captive portal name	Select the configured captive portal name from the drop-down list.
DNS Proxy	When the DNS Proxy field is enabled, the gateway acts as a proxy for all DNS requests and communicates with the ISP's DNS servers. This field is available when you select **DHC P Relay** or **None** as the DHCP mode.
Save	Click **Save** to save your settings.
Close	Click **Close** to revert to the previous settings.

IP management list

The gateway's DHCP server can assign IP settings to your clients on your network by adding a client's MAC address and the IP address to the DHCP server's database. Whenever the gateway receives a request from a client, the MAC address of that client is compared with the MAC address list present in the database, and the corresponding IP address is assigned to the client.

Another available security measure is to allow outbound traffic (from LAN to WAN) when the LAN node has an IP address matching the MAC address bound to it. This is IP/MAC Binding. By enforcing the gateway to validate the source traffic's IP address with the unique MAC Address of the configured LAN node, the administrator can ensure traffic from that IP address is not spoofed. If a violation (i.e., the traffic's source IP address does not match up with the expected source MAC address) occurs, the packets will be dropped.

This section of VLAN displays the IP management list.

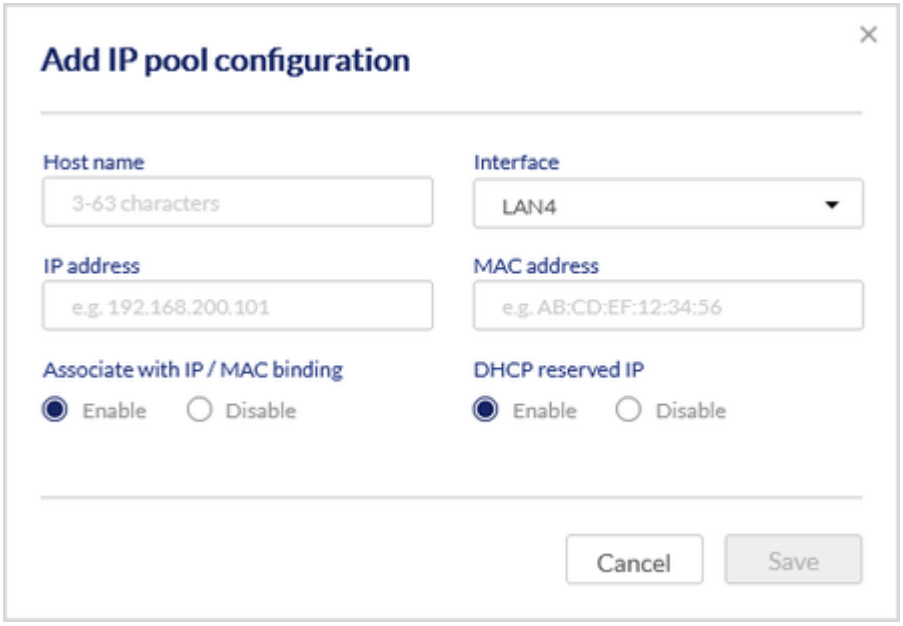


The fields displayed in the *IP management list* table are as follows:

Field	Description
Hostname	It displays the hostname for the pair of IP and MAC addresses.
Interface	It displays the interface to which the client is connected, and the DHCP lease is provided. It can include custom VLAN interface names.
IP address	It displays the IP address you have assigned to the device.
MAC address	

	It displays the MAC address of the host that can connect on the configured interface and for which an IP address is reserved.
DHCP reserved IP	It displays if the DHCP reserved IP is enabled or disabled.
IP/MAC binding	It displays if the IP/MAC binding feature is enabled or disabled.
Actions	You can edit or delete the selected entry. *Note: This field is available only when the "Use profile configuration" field is disabled.*

Click **Add** to add a new entry. This opens the *Add IP pool configuration* page. To delete multiple entries at once, select the checkboxes of the IP management that you want to delete, and click **Delete**.



The fields available on the *Add IP pool configuration* page are as follows:

Field	Description
Hostname	Enter the hostname for the pair of IP and MAC addresses.
Network	Select the network from the drop-down list.
IP address	Enter the IP address you want to assign to this device. *Note: This IP address must be in the same range as the starting/ending IP address under DHCP Settings for that interface.*
MAC address	Enter the MAC address (xx:xx:xx:xx:xx:xx format) of the host that can be connected on LAN, for which an IP address has to be reserved.
Associate with IP/MAC binding	You can enable or disable the IP/MAC binding feature. If enabled, it associates the host's information with IP/MAC Binding.
DHCP reserved IP	You can enable or disable the DHCP reserved IP feature.
Save	Click **Save** to save your settings.
Close	Click **Close** to revert to the previous settings.

Routing

Routing refers to the path that the packets follow from the source to the destination in the most optimum manner. This section of the Network provides you with the configuration fields required to manage the routing process in the network. Various methods are supported by the Nuclias cloud gateway like the Static Route, Policy Route, RIP, and OSPFv2. Static routing is a conventional method where the gateway uses the manually configured route path, and if any changes occur, the static route is to be reconfigured manually. Policy route allows you to configure routing policy based on certain parameters like the source address, destination address, source port, or destination port. Another protocol that the cloud gateway supports is the Routing Information Protocol (RIP). It is a protocol that keeps a check on the number of hops a packet can

make from its source to destination. Similarly, you will also learn to configure OSPFv2 in this section. OSPFv2 is a dynamic protocol that routes Internet Protocol (IP) packets solely within a single routing domain.

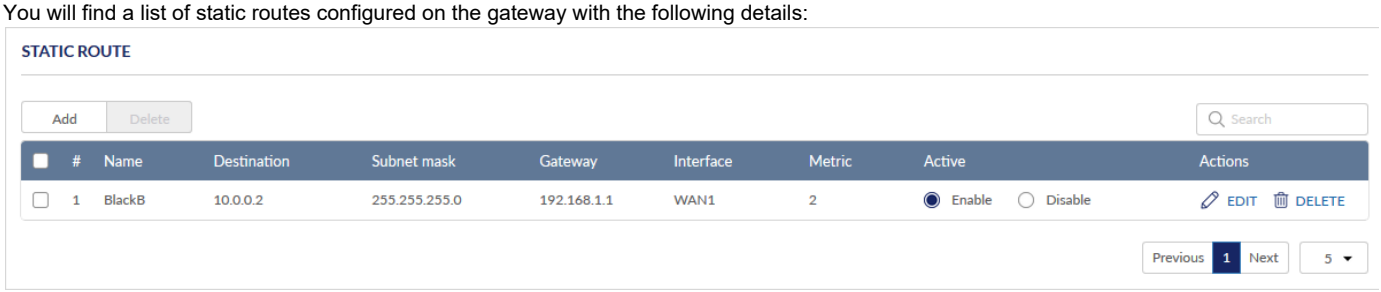
This section covers the following topics:

Static Route

Routing between the LAN and WAN will impact how this gateway handles traffic received on any of its physical interfaces. The routing mode of the gateway is core to the traffic flow behavior between the secure LAN and the Internet.

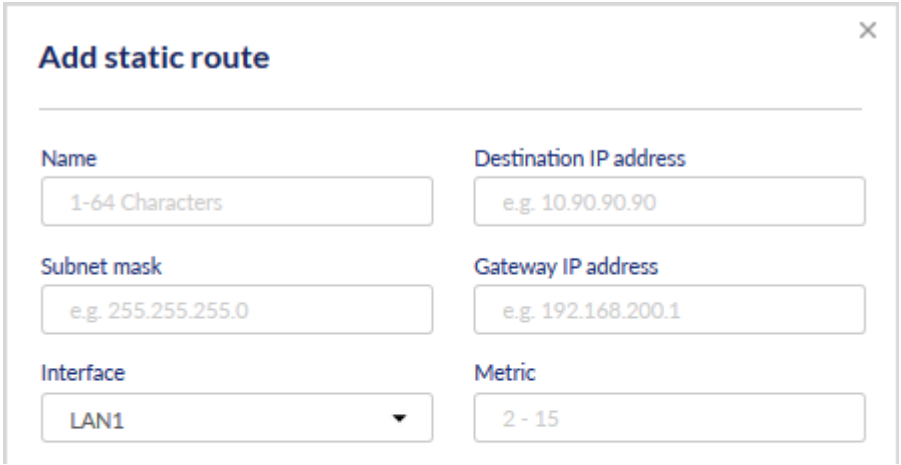
Manually adding static routes to this device allows you to define the traffic path selection from one interface to another. There is no communication between this gateway and other devices to account for changes in the path; once configured, the static route will be active and effective until the network changes.
The Static Route page displays all routes added manually by an administrator and allows several operations on the static routes.

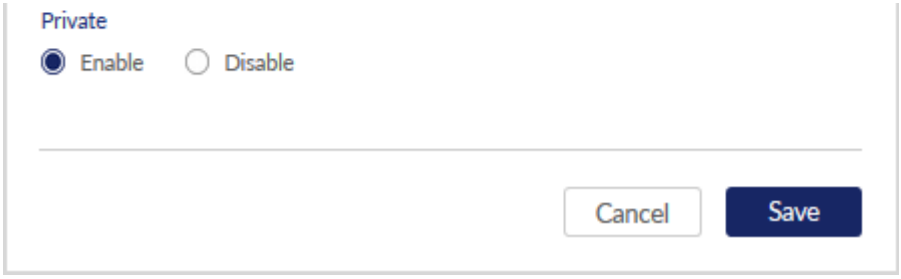
You will find a list of static routes configured on the gateway with the following details:



Field	Description
Name	It displays the name of the route.
Destination	It displays the IP address of the static route's destination.
Subnet mask	It displays the subnet mask of the static route.
Gateway	It displays the IP address of the gateway through which the destination host or network can be reached.
Interface	It displays the physical network interface (WAN, DMZ, VLAN, or LAN) through which this route is accessible.
Metric	It displays a value between 2 and 15.
Active	Select enable or disable to activate or deactivate this route. ***Note**: The enable and disable options are available only if the "Use profile configuration" field is disabled.*
Actions	You can edit or delete the route. ***Note**: This field is available only if the "Use profile configuration" field is disabled.*

Click **Add** to add a new entry. This opens the *Add static route* page. To delete multiple entries at once, select the checkboxes of the configured static route you want to delete, and click **Delete**.





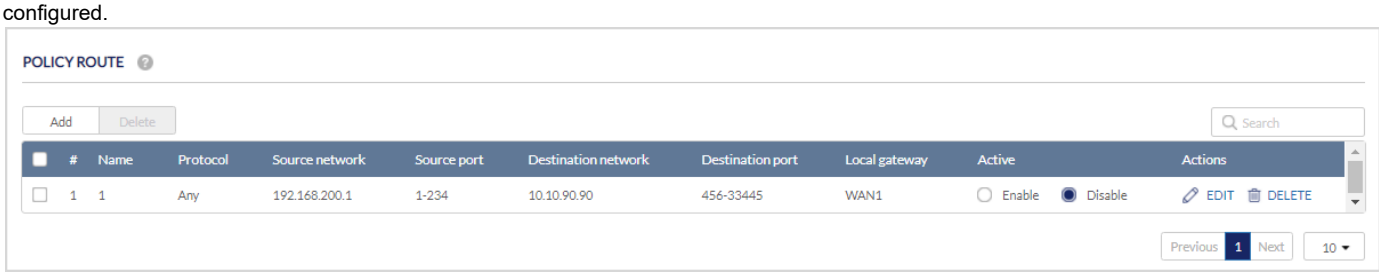
The fields available on this page are as follows:

Field	Description
Name	Enter the name of the route.
Destination IP address	Enter the IP address of the static route's destination.
Subnet mask	Enter the subnet mask of the static route.
Gateway IP address	Enter the IP address of the gateway through which the destination host or network can be reached.
Interface	Select a physical network interface (WAN, DMZ, VLAN, or LAN) through which this route is accessible.
Metric	Enter a value between 2 and 15. It determines the priority of the route. If multiple routes to the same destination exist, the route with the lowest metric is chosen.
Private	Enable this feature to make this route private. If the route is made private, the route will not be shared in a RIP.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

Policy Route

Policy routes are useful when the Load Balancing feature is in use. Selecting TCP/UDP, you can assign the type of traffic to go over the specified WAN ports. The source network, source address, the destination network, a destination address, service, or protocol can be associated with a particular WAN port for increased flexibility.

For example, the VoIP traffic for a set of LAN IP addresses can be assigned to one WAN, and any VoIP traffic from the remaining IP addresses can be assigned to the other WAN link. Policy routes are only applicable when load balancing mode is enabled and more than one WAN is configured.

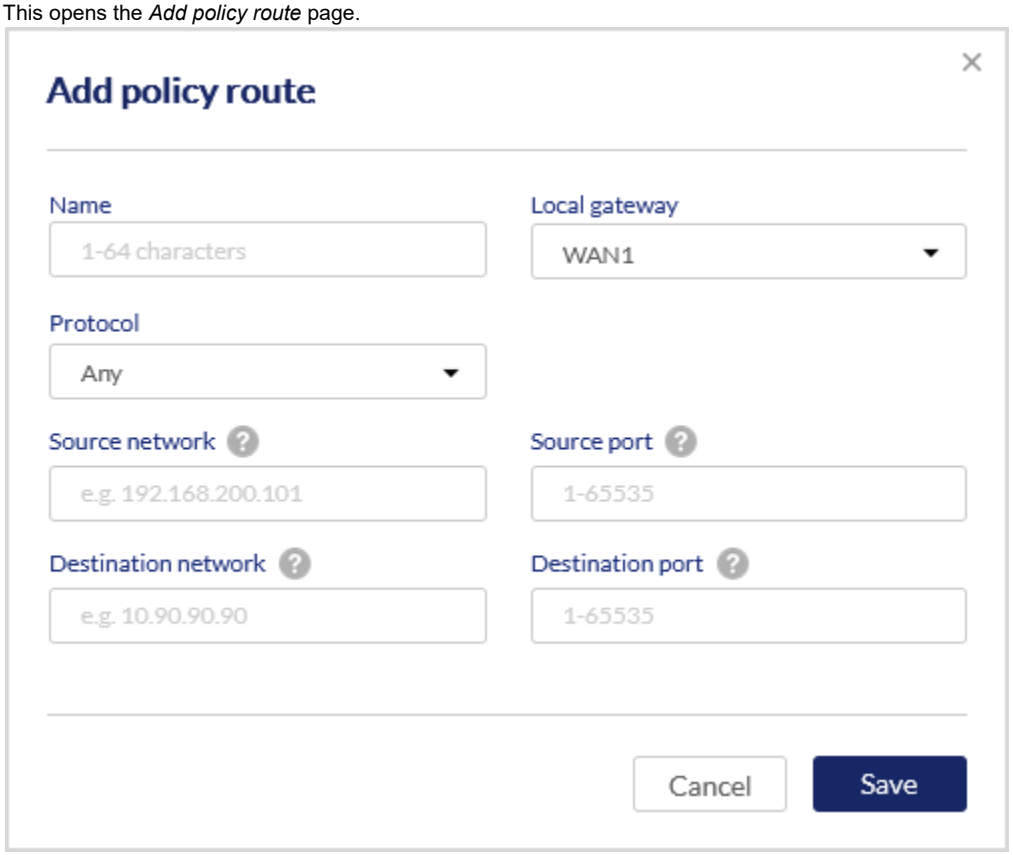


This section of the routing shows a list of configured policy routes on the gateway with the following details:

Field	Description
Name	It displays the name of the policy route.
Protocol	It displays the protocol placed in the transport layers of the Internet protocol suite.
Source network	It displays the source network. It options are Any, an IP address, and a range of IP address.
Source port	It displays a source port for which the policy route will be applicable.
Destination network	It displays the destination network. Its options are Any, an IP address, and a range of IP addresses.

Destination port	It displays a destination port for which the policy route will be applicable.
Local Gateway	It displays the WAN interface.
Active	You can enable or disable the selected policy route. ***Note**: The enable and disable options are available only if the "Use profile configuration" field is disabled.*
Actions	You can edit or delete the route. ***Note**: This field is available only if the "Use profile configuration" field is disabled.*

To delete multiple entries at once, select the checkboxes of the policy route you want to delete, and click **Delete**. Click **Add** to add more entries. This opens the *Add policy route* page.



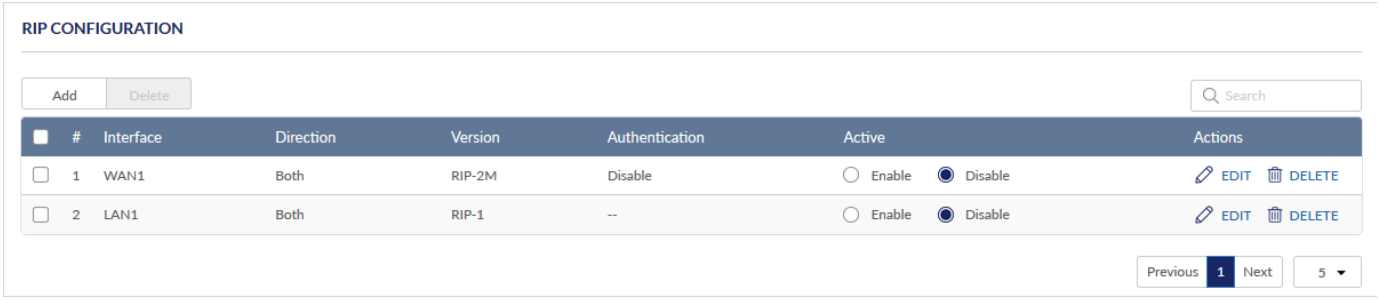
The fields available on the *Add policy route* page are as follows:

Field	Description
Name	Enter the name of the policy route.
Local gateway	Select the WAN interface.
Protocol	Select one of the protocols that are commonly placed in the transport layers of the Internet protocol suite.
Source network	Enter an IP address, a range of IP addresses, or Any as the source network.
Source port	A port is a communication endpoint. Ports are identified for each protocol and address combination by 16-bit unsigned numbers, commonly known as the port number. The most common protocols that use port numbers are the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). Here, the *Source port* is an integer in the range of 1-65535 initiated from a specific application on the source IP. Enter a source port number.
Destination network	Enter an IP address, a range of IP addresses, or Any as the destination network.
Destination port	Destination Port is an integer in the range of 1-65535 destined to a specific application on destination IP. Enter the destination port number.

Save	Click **Save** to save your settings.
Close	Click **Close** to revert to the previous settings.

RIP Configuration

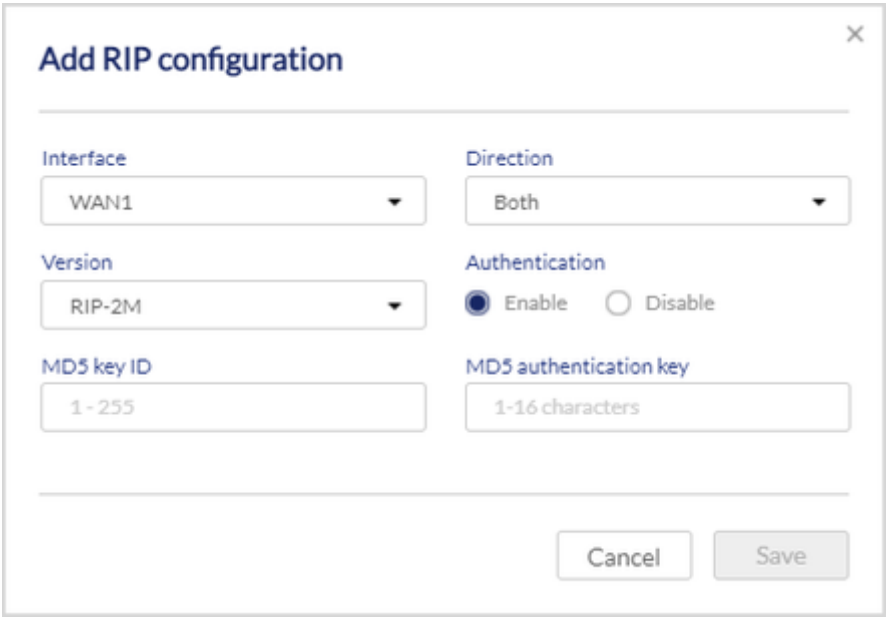
Dynamic routing using the Routing Information Protocol (RIP) is an Interior Gateway Protocol (IGP) common in LAN. With RIP, the cloud gateway can exchange routing information with other supported gateways in the LAN and allow for dynamic adjustment of routing tables to adapt to modifications in the LAN without interrupting traffic flow.



The fields displayed on the page are as follows:

Field	Description
Interface	It displays the interface on which the RIP is configured.
Direction	It displays in which direction the RIP packets need to be exchanged.
Version	It displays the RIP version supported by the routing devices in the selected interface.
Authentication	It displays whether the authentication is enabled or disabled for RIP-2M.
Active	You can enable or disable the configured RIP. ***Note**: The enable and disable fields are available only if the "Use profile configuration" field is disabled.*
Actions	You can edit or delete the configured RIP. ***Note**: This field is available only if the "Use profile configuration" field is disabled.*

Click **Add** to add a new entry to the list. This opens the *Add RIP configuration* page. To delete multiple entries, select the corresponding checkboxes present in the first column of the table, and click **Delete**.

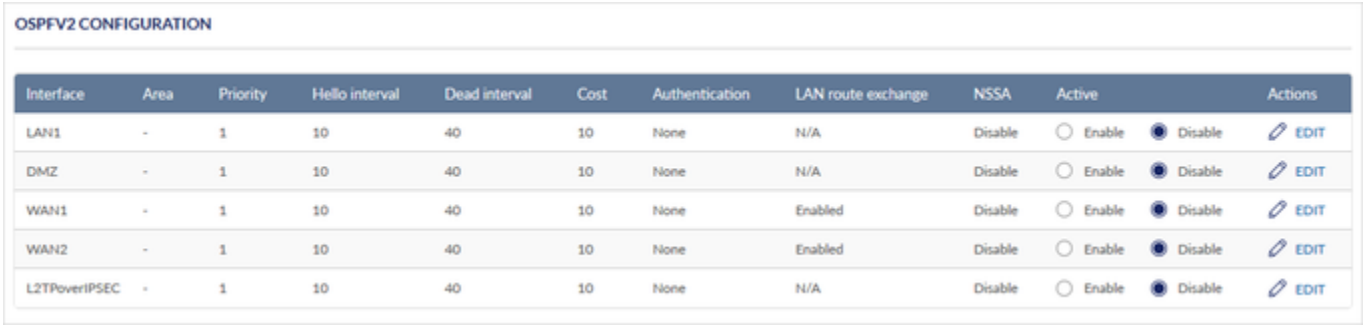


The fields available on the *Add RIP configuration* page are as follows:

Field	Description
Interface	Select the interface where you want to configure the RIP.
Direction	The RIP direction will define how this gateway sends and receives RIP packets. Select one of the following options: • **Both**: The gateway both broadcasts its routing table and also processes RIP information received from other routers. This is the recommended setting to utilize RIP capabilities fully. • **In Only**: The gateway accepts RIP information from other routers but does not broadcast its routing table.
Version	The RIP version is dependent on the RIP support of other routing devices in the LAN. • **RIP-1**: A class-based routing version that does not include subnet information. This is the most commonly supported version. • **RIP-2M**: It includes all the functionality of RIPv1, plus it supports subnet information. RIP-2M sends data to multicast addresses.
Authentication	Select **Enable** to activate the authentication for RIP-2M. By default, RIP authentication is disabled.
MD5 Key ID	Enter the unique MD5 key ID.
MD5 Authentication Key	Enter the authentication key for this MD5 key.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to your previous settings.

OSPFv2 Configuration

OSPF is an interior gateway protocol that routes Internet Protocol (IP) packets solely within a single routing domain. It gathers link state information from available routers and constructs a topology map of the network. OSPF version 2 is a routing protocol which is described in RFC2328 - OSPF Version 2. OSPF is IGP (Interior Gateway Protocols) and is widely used in large networks such as ISP backbone and enterprise networks.

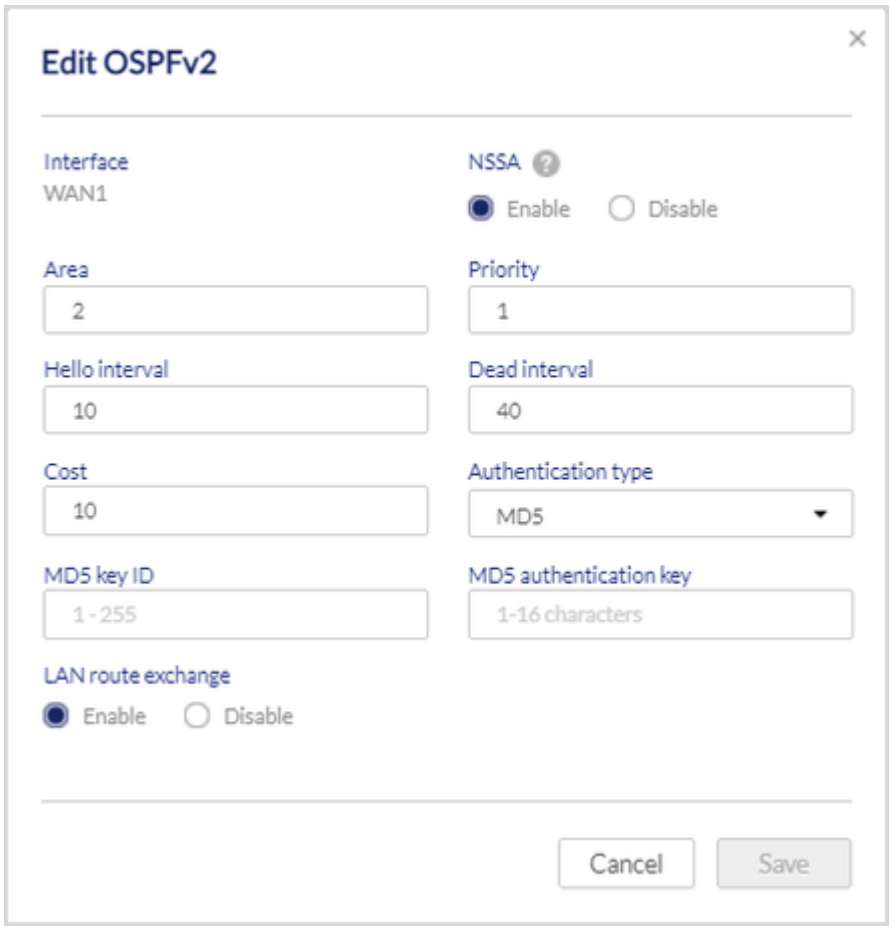


The fields displayed on the *OSPFV2 Configuration* table are as follows:

Field	Description
Interface	It displays the physical network interface on which OSPFv2 is enabled or disabled. *Note:* • *For the "L2TP over IPsec" interface, follow the steps as follows:* 1. *In the cloud portal, goto VPN > PPTP/L2TP > Server mode/Client mode and click **Add**.* 2. *Select **L2TP** as the server/client type, and enable **L2TP over IPsec**. Configure L2TP over IPsec on the server-side/client-side.* 3. *Save the configuration. For more details, refer to PPTP/L2TP.* • *Similarly, for the "DMZ interface," you must configure DMZ on the Port configuration (Network > Ethernet> Port configuration) page. For more details, refer to Port configuration.*
Area	It displays the area to which the interface belongs.

Priority	It displays the priority of the router to become the designated router.
Hello interval	It displays the number of seconds that the hello packet is sent.
Dead interval	It displays the time (number of seconds) that a device's hello packets must not have seen before its neighbors declare the OSPF router down.
Cost	It displays the cost of sending a packet on an OSPFv2 interface.
Authentication	It displays the authentication type.
LAN route exchange	It displays the LAN Route Exchange status for a WAN interface.
NSSA	It displays whether NSSA is enabled or disabled.
Active	You can enable or disable the respective interface. ***Note**: The enable and disable options are available only if the "Use profile configuration" field is disabled.*
Actions	You can edit the configured interface. ***Note**: This field is available only if the "Use profile configuration" field is disabled.*

Click **Edit** to open the *Edit OSPFv2* page. To delete multiple entries at once, select the checkboxes of OSPFv2 you want to delete, and click **Delete**.



The fields available on the *Edit OSPFv2* page are as follows:

Field	Description
Interface	It displays the physical network interface on which OSPFv2 is enabled or disabled.
NSSA	Enable this option to allow OSPF stub areas to carry external routes.
Area	

	Enter the area to which the interface belongs. Two routers having a common segment; their interfaces have to belong to the same area on that segment. The interfaces should belong to the same subnet and should have a similar mask.
Priority	It helps to determine the OSPFv2 designated gateway for a network. The gateway with the highest priority will be more eligible to become Designated Router. Setting the value to 0 makes the router ineligible to become Designated Router. The default value is 1. Lower the value means higher priority.
Hello interval	Enter the number, in seconds, when the Hello packet is to be sent. This value must be the same for all gateways attached to a common network. The default value is 10 seconds.
Dead interval	Enter the number of seconds when a device's hello packets are not seen before its neighbors declare the OSPF router down. This value must be the same for all routers attached to a common network. The default value is 40 seconds. OSPF requires these intervals to be the same between two neighbors. If any of these intervals are different, these routers will not become neighbors on a particular segment.
Cost	Enter the cost of sending a packet on an OSPFv2 interface.
Authentication Type	Select one of the following authentication types: • **None**: The interface does not authenticate OSPF packets. • **Simple**: OSPF packets are authenticated using simple text keys. • **MD5**: The interface authenticates OSPF packets with MD5 authentication.
Authentication Key	Enter the authentication key. This field is available when you select **Simple** as the *Authentic ation Type*.
MD5 Key ID	If you select **MD5** as the *Authentication Type*, enter the MD5 key ID.
MD5 Authentication Key	If you select **MD5** as the *Authentication Type*, enter the MD5 authentication key.
LAN route exchange	It displays the LAN Route Exchange status for a WAN interface.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

Services

The **Services** section of the Nuclias cloud gateway web UI discusses the multiple services to provide a secure and fast network to its users. Services like the Jumbo frame improve network performance by using an efficient maximum transmission unit (MTU). IGMP snooping filters the multicast traffic on the network, and the UPnP feature helps discover devices on the network that can communicate with the gateway and auto-configure. This section of the Network will also explain service management and Application layer gateways, supported by the Nuclias cloud gateway.

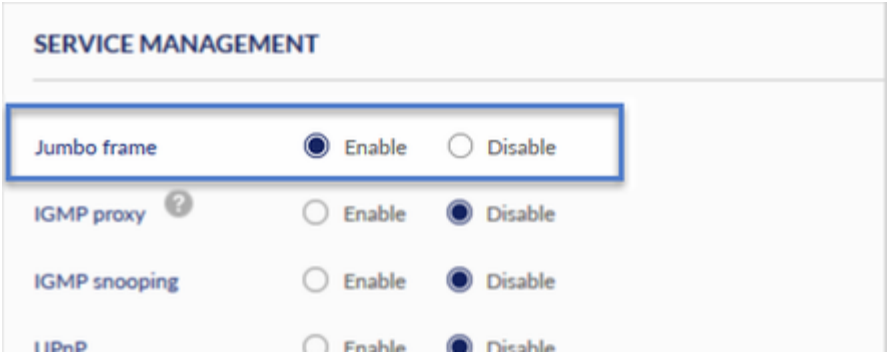
This section covers the following topics:

Service Management

This section of the web UI discusses the following services supported by the Nuclias cloud gateway:

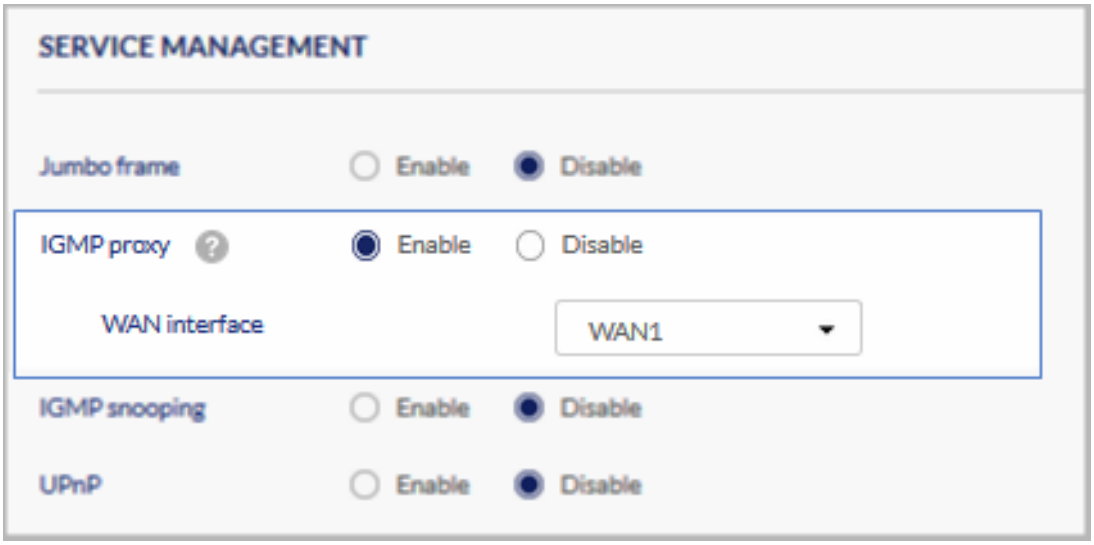
Jumbo frame

Jumbo frames are Ethernet frames with more than 1500 bytes of payload. When this feature is enabled, the LAN devices can exchange information at the Jumbo frames rate. You can enable or disable this feature.



IGMP Proxy

The Internet Group Management Protocol (IGMP) is used by hosts and routers on an IP network to create multicast group memberships. The IGMP can be used for web and support applications like the online streaming of videos and games. The IGMP proxy enables the gateway to issue IGMP messages on behalf of the clients behind it. If the IGMP proxy feature is enabled, select the WAN interface on which it is to be applied.



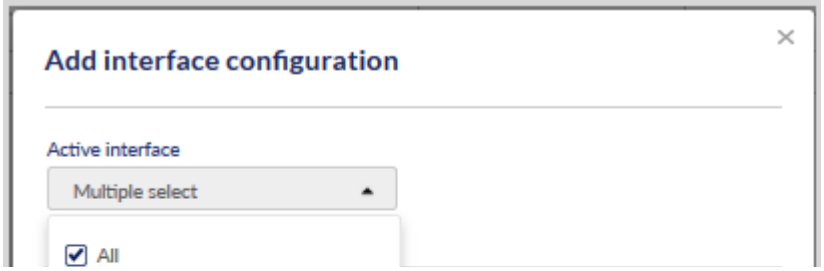
IGMP Snooping

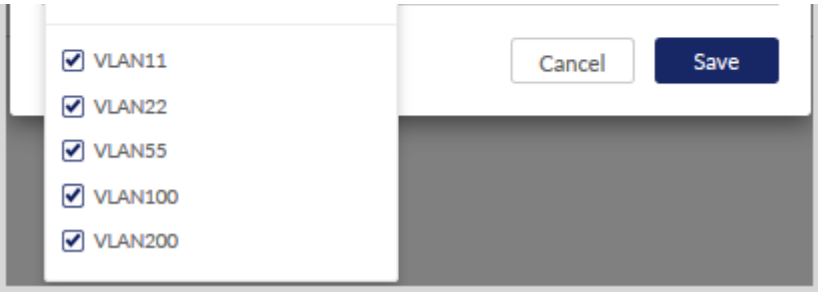
IGMP snooping allows the gateway to 'listen' in on IGMP network traffic through the gateway. This allows the gateway to filter multicast traffic and direct it only to hosts that need this stream. This is helpful when there is a lot of multicast traffic on the network where all LAN hosts do not need to receive this multicast traffic.

The fields available in the *Configuration* table are as follows:

Field	Description
Interface	It displays the interface on which the IGMP snooping is configured.
IGMP snooping	It displays if the IGMP snooping is enabled or disabled.
Actions	It allows you to delete the configured IGMP snooping one at a time.

Click **Add** to add a new interface. This opens the *Add interface configuration* page. To delete more than one configured IGMP snooping, select the checkbox of the corresponding configured interface, and click **Delete**.





The fields available on the *Add interface configuration* page are as follows:

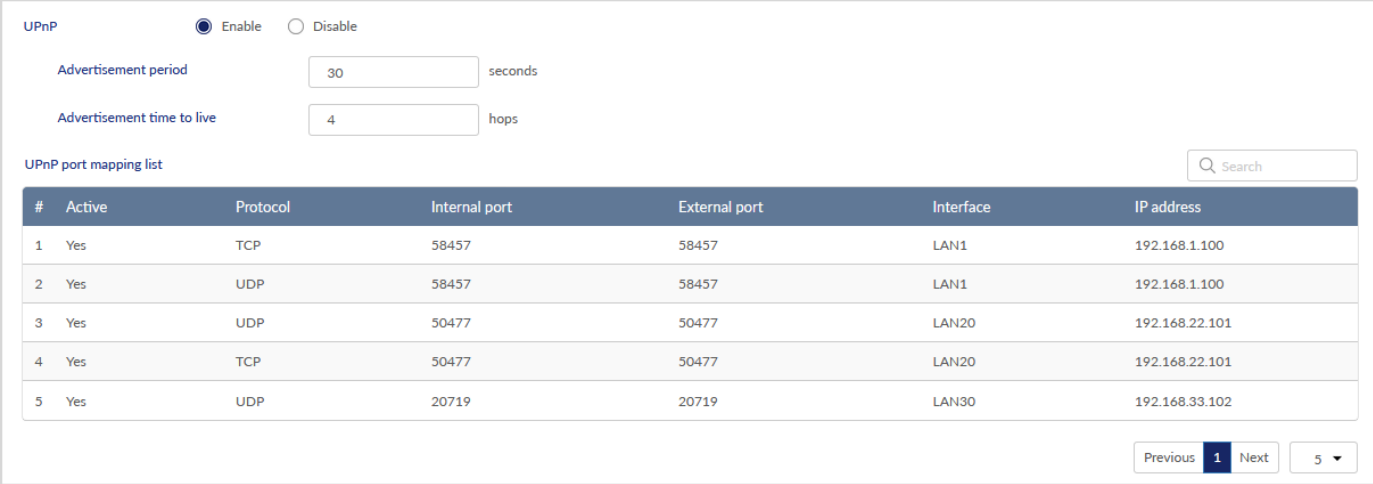
Field	Description
Active interface	Select the active interface. ***Note**: IGMP snooping supports VLAN only.*
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to your previous settings.

UPnP

Universal Plug and Play (UPnP) is a feature that allows the cloud gateway to find the devices on the network that can communicate with the gateway and allow for auto-configuration. If UPnP detects a network device, the gateway can open internal or external ports for the traffic protocol required by that network device. If the UPnP feature is disabled, the gateway can not configure an automatic device, and you may have to manually open/forward ports to allow applications to work.

Select **Enable** to configure UPnP and display the UPnP port mapping list.

***Note**: You can edit the UPnP feature only if the "Use profile configuration" field is disabled.*



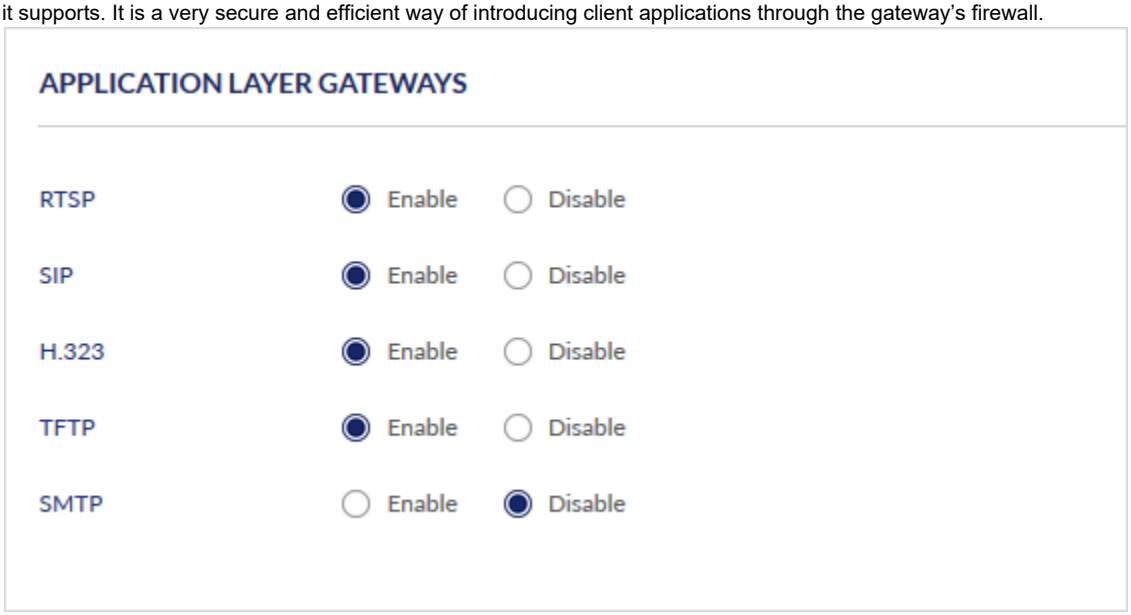
The *UPnP port mapping list* has the details of UPnP devices that respond to the gateway's advertisements. The following information is displayed for each detected device:

Field	Description
UPnP	You can enable or disable the UPnP feature.
Advertisement period	Enter a value for the Advertisement period. This is the frequency that the gateway broadcasts UPnP information over the network. A large value will minimize the network traffic but cause delays in identifying new UPnP devices to the network.
Advertisement time to live	Enter a value for Advertisement time to live. This is the number of hops a packet is allowed to propagate before being discarded. Small values will limit the UPnP broadcast range. A default of 4 is typical for networks with a few numbers of switches.
UPnP port mapping list	

Active	It indicates if the UPnP port is still open in the device or not.
Protocol	It displays the network protocol used by the gateway.
Internal port	It displays the internal ports opened by UPnP (if any).
External port	It displays the external ports opened by UPnP (if any).
Interface	It refers to the LAN/VLAN segment on which the UPnP option is enabled.
IP address	It displays the IP address of the UPnP device detected by the gateway.

Application Layer Gateways (ALGs)

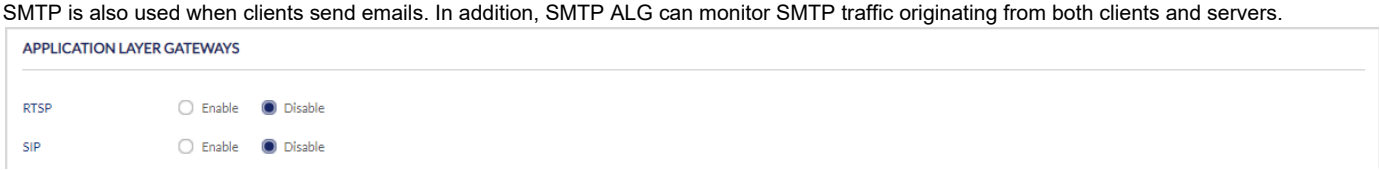
Application Level Gateways (ALGs) are security components that enhance the firewall and NAT support of the gateway to seamlessly support application layer protocols. In some cases enabling the ALG will allow the firewall to use dynamic, ephemeral TCP/ UDP ports to communicate with the known ports a particular client application (such as H.323 or RTSP) requires; otherwise, the admin would have to open a large number of ports to accomplish the same support. ALG understands the protocol used by the specific application that it supports. It is a very secure and efficient way of introducing client applications through the gateway's firewall.

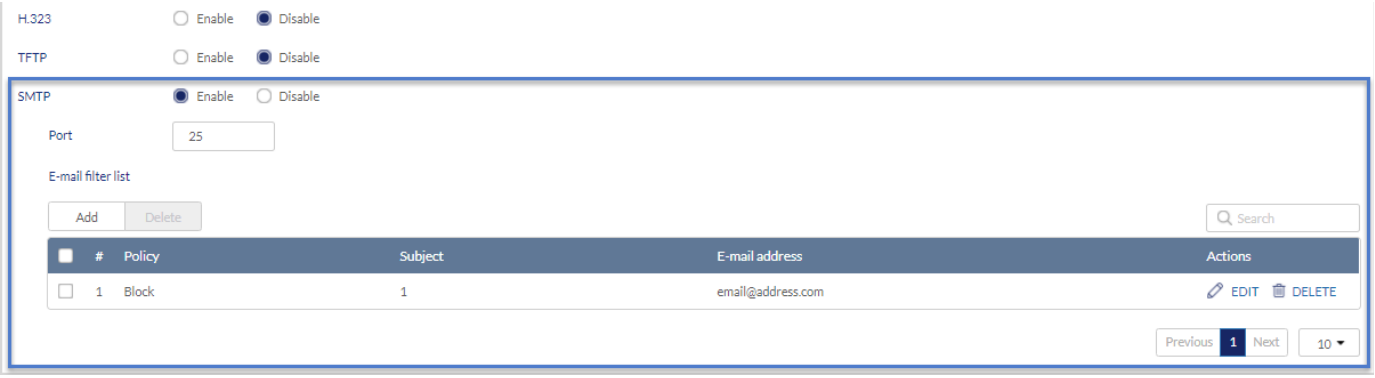


Field	Description
RTSP	Enable it to allow applications that use Real Time Streaming Protocol to receive streaming media from the Internet. QuickTime and Real Player are some of the common applications using this protocol.
SIP	Enable it to allow devices and applications using VoIP (Voice over IP) to communicate across NAT.
H.323	Enable it to allow H.323 (specifically Microsoft Netmeeting) clients to communicate across NAT.
TFTP	Enable it to allow Trivial FTP (TFTP) clients and servers to transfer data across NAT.
SMTP	Enable it to transfer email between mail servers over the Internet and enter the **port** at which the SMTP packets are inspected.

E-mail filter list

The *E-mail filter list* appears only when the SMTP is enabled. Simple Mail Transfer Protocol (SMTP) is a text-based protocol used for transferring emails between mail servers over the Internet. Typically, the local SMTP server is located on a DMZ so that mail sent by remote SMTP servers traverses the gateway to reach the local server. Local users then use email client software to retrieve their email from the local SMTP server. SMTP is also used when clients send emails. In addition, SMTP ALG can monitor SMTP traffic originating from both clients and servers.

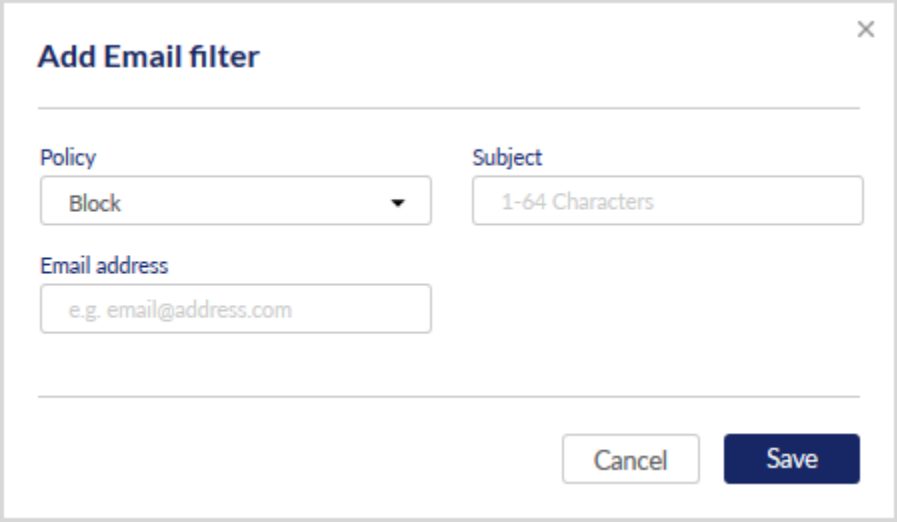




The table lists all the subjects along with email addresses that are blocked or allowed.

Field	Description
Policy	It displays the policy to allow or block the email address.
Subject	It displays the subject.
Email address	It displays the email address.
Actions	You can click **Edit** to modify the entry and click **Delete** to delete the entire entry.

Click **Add** to open the *Add Email filter* page to add a new entry. To delete multiple entries at once, select the checkboxes of the entries you want to delete, and click **Delete**.



The fields available on the *Add Email filter* page are as follows:

Field	Description
Policy	Select a policy. It can be either **Allow** or **Block**.
Subject	Enter the subject. The range is from 1 to 64 characters.
Email address	Enter an email address.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

Traffic Management

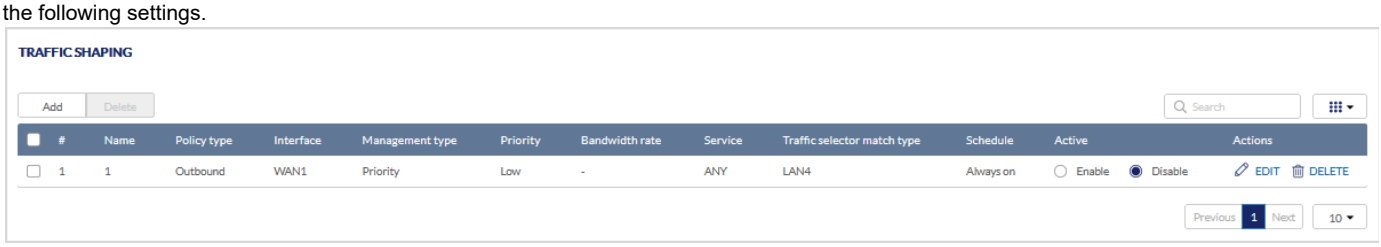
The traffic management feature allows you to regulate the traffic flow from the LAN to WAN. This is useful to ensure that low priority LAN users (like guests or HTTP service) do not monopolize the available WAN's bandwidth for cost-savings or bandwidth-priority-allocation purposes.

This section will help you understand and configure the bandwidth control feature from the web user interface and add a profile that defines the control parameters. You can then associate the profile with a traffic selector to apply the bandwidth profile to the traffic, matching the selectors. Selectors are elements like IP addresses or services that would trigger the configured bandwidth regulation.

The *traffic management* section covers the following topics:

Traffic Shaping

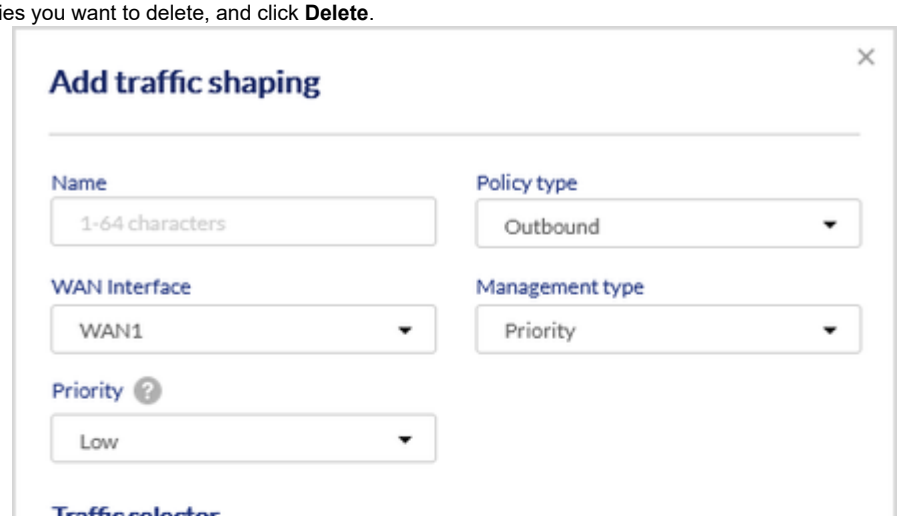
Traffic selector is a service-based rule to which the user can attach traffic management profiles. Once a profile has been created, it can then be associated with traffic flow from the LAN to WAN. Traffic selector configuration binds a bandwidth profile to a type or source of LAN traffic with the following settings.

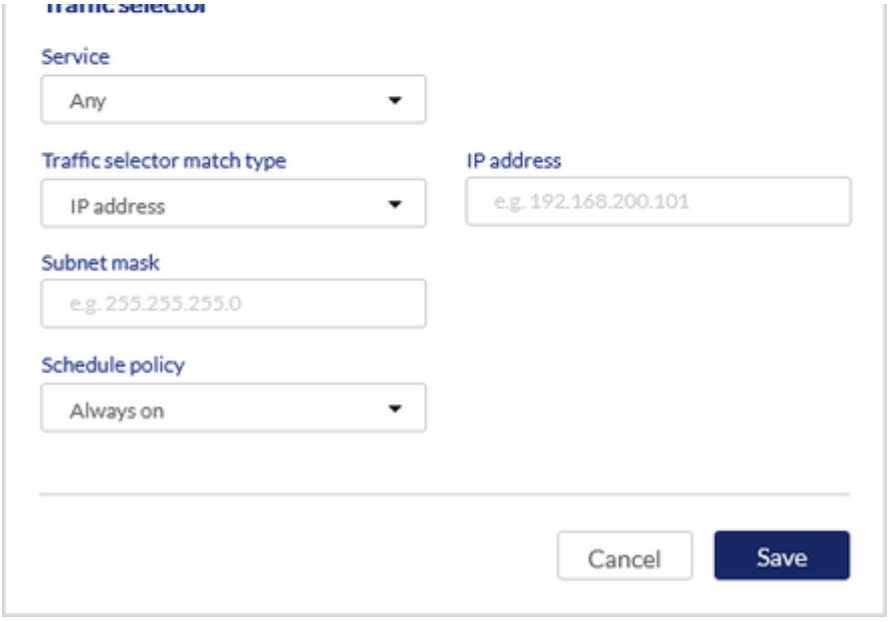


The fields displayed in the *Traffic Shaping* table are as follows:

Field	Description
Name	It displays the name of your profile.
Policy type	It displays the policy type (**Inbound** or **Outbound**).
Interface	It displays the interface with which the profile is associated.
Management type	It displays as **Priority** or **Rate**.
Priority	It displays the priority level, i.e., low, medium, or high.
Bandwidth rate	It displays the range of bandwidth rates.
Service	It displays the service.
Traffic selector match type	It displays the traffic selector match type.
Schedule	It displays the schedule of the selected traffic shaping.
Active	You can enable or disable the respective Traffic management policy. ***Note**: This field is available only if the "Use profile configuration" field is disabled.*
Actions	You can edit or delete the selected traffic management policy. ***Note**: This field is available only if the "Use profile configuration" field is disabled.*

Click **Add** to add a new entry to the table. This opens the *Add traffic shaping* page. To delete more than one entry, select the checkbox of the traffic management policies you want to delete, and click **Delete**.





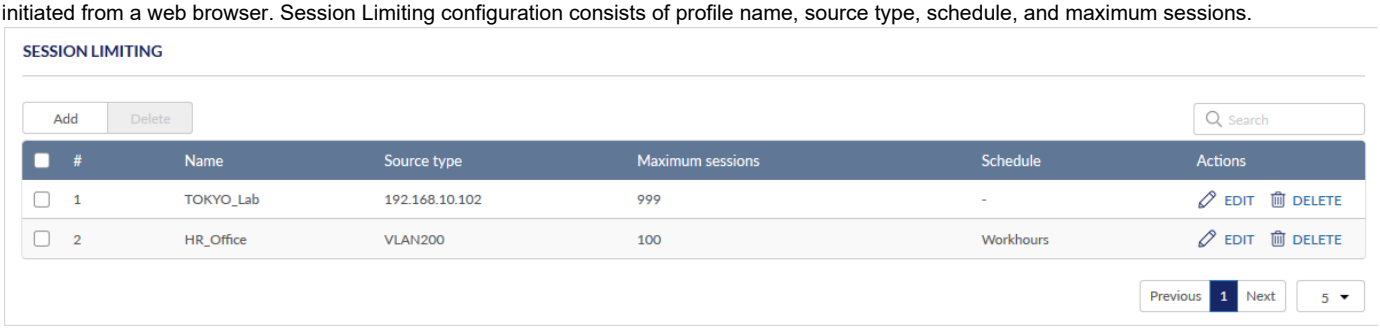
The fields available on the *Add traffic shaping* page are as follows:

Field	Description
Name	Enter a name for your profile. This identifier is used to associate the configured profile to the traffic selector.
Policy type	Select the policy type (**Inbound** or **Outbound**).
WAN Interface	Select which of the available WAN interfaces you want to associate this profile with. This field appears when **Outbound** is selected as the *Policy type*.
Interface	Select which of the available interfaces you want to associate this profile with. This field appears when **Inbound** is selected as the *Policy type*.
Management type	Select either **Priority** or **Rate**.
Priority	If you select **Priority**, specify the priority. It could be *Low*, *Medium*, or *High*.
Max. bandwidth rate (Kbps)	If you select **Rate**, enter the maximum bandwidth rate.
Min. bandwidth rate (Kbps)	If you select **Rate**, enter the minimum bandwidth rate.
Traffic selector	
Service	Select a service from the drop-down list.
Traffic selector match type	This field is available when you select **Outbound** as the *Policy type*. Select any one of the following match types: • **IP address**: Select this option to associate this traffic selector with an IP Address of a LAN device. Once selected, enter the IP address of the LAN device. • **MAC address**: Select this option to associate this traffic selector with a specific MAC address on the LAN. Once selected, enter a valid MAC Address. • **Interface**: If this option is selected, select the interface.
Interface	If you select **Interface**, select an interface from the drop-down list.
IP address	Enter the IP address of the source associated with this profile.
Subnet mask	Enter the subnet mask.
MAC address	If you select **MAC address**, enter the MAC address of the source associated with this profile.
Schedule policy	It allows you to define the time and day when the traffic shaping rule is to be applied.
Save	Click **Save** to save your settings.

Close	Click **Close** to revert to the previous settings.

Session Limiting

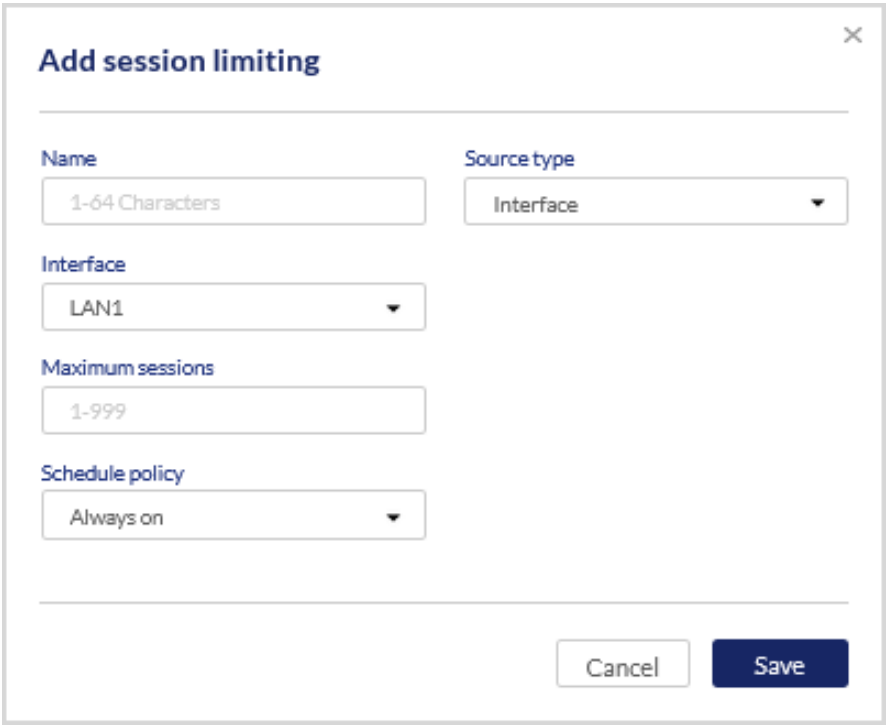
The *Session Limiting* section displays a list of configured session limiting profiles. It allows a user to limit the number of sessions per IP address, range of IP addresses, or interface through the device. When the session limit is reached, a warning message is displayed to users for a session initiated from a web browser. Session Limiting configuration consists of profile name, source type, schedule, and maximum sessions.



The fields displayed in the *Session Limiting* table are as follows:

Field	Description
Name	It displays the name of the profile configured for a particular source type.
Source type	It displays the source type selected for the profile.
Maximum sessions	It displays the maximum number of sessions allowed on the selected source type to limit sessions.
Schedule	It displays the schedule for the configured session limit profile.
Actions	You can edit or delete an entry.

Click **Add** to add a new entry to the list. This opens the *Add session limiting* page. To delete more than one entry, select the check-boxes of the entries you want to delete, and click **Delete**.



The fields available on the *Add session limiting* page are as follows:

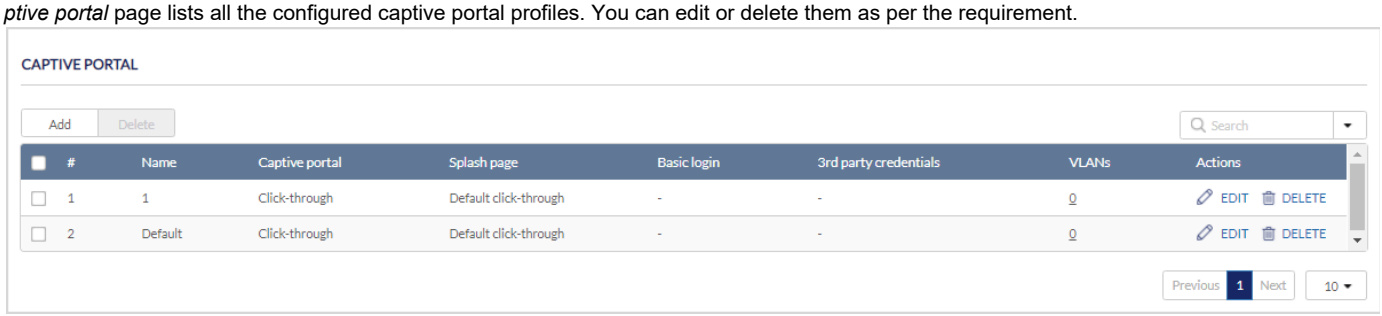
Field	Description

Name	Enter the name of the profile to be configured for a particular Source type.
Source type	Select a source type for the profile. The options are IP address, IP range, and Interface.
IP address	Enter the IP Address of the client/Host to be controlled in the Session Limit profile when the selected source type is **IP address**.
Starting IP address	Enter the starting IP address of the clients to be controlled in the Session Limit profile when the selected source type is **IP Range**.
Ending IP address	Enter the ending IP Address of the clients to be controlled in the Session Limit profile when the selected source type is **IP Range**.
Interface	Select the Interface from the drop-down list to select the complete network controlled in the Session Limit profile when the selected source type is **Interface**.
Maximum sessions	Enter the maximum number of sessions allowed on the source type to limit sessions.
Schedule policy	It allows you to define the time and day when the session limiting profile is to be used. Select any one of the configured schedules from the drop-down list.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

Captive Portal

A *captive portal* (also known as a “splash page”) is a web page that appears when an unauthenticated user tries to access the Internet. When the captive portal is configured, the user has to be verified and authenticated, and then only Internet access is granted. It is done either by entering the login credentials or by accepting the terms and conditions of service. This helps the gateway monitor and control Internet usage.

The Nuclias cloud gateway, DBG-2000, allows its users to configure the captive portal page and provides various authentication methods. The *Captive portal* page lists all the configured captive portal profiles. You can edit or delete them as per the requirement.

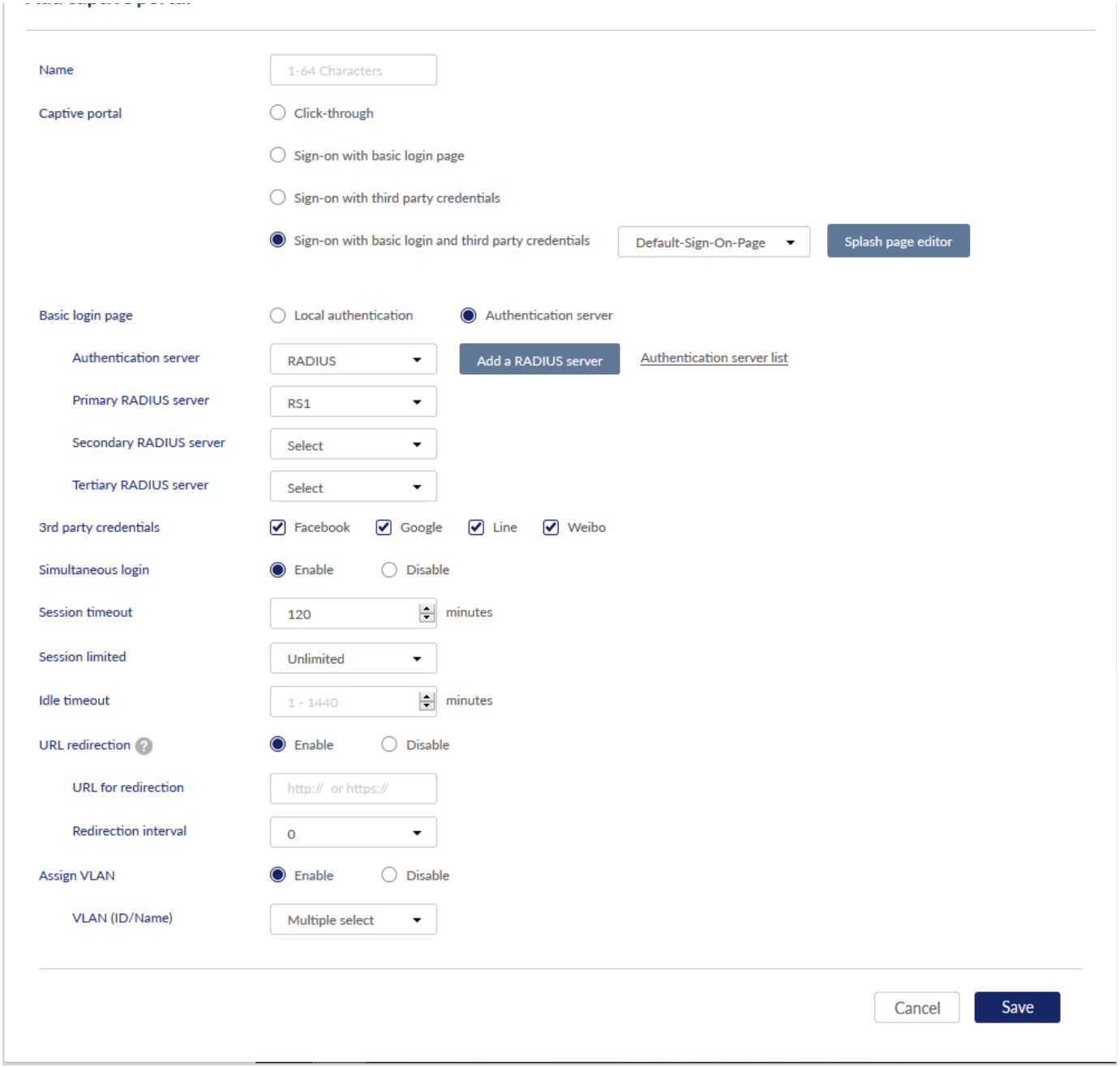


The fields displayed in the *Captive portal* table are as follows:

Field	Description
Name	It indicates the name of the configured captive portal profiles.
Captive portal	It displays the authentication type used for the configured captive portal.
Splash page	It displays the name of the splash page created.
Basic login	It indicates the authentication server which is being used for the basic login.
3rd party credentials	It displays the 3rd parties whose credentials will be used for the login.
VLANs	It displays the VLAN ID on which the captive portal is configured.
Actions	You can edit or delete the selected Captive portal profile. When you click **Edit**, it opens the *Edit captive portal* page. *Note: This column is available only when you disable the “Use profile configuration” field.*

Click **Add** to add a new captive portal profile. This opens the *Add captive portal* page. If you want to delete multiple entries at once, select the corresponding checkboxes, and click **Delete**.

*Note: The **Add** and **Delete** buttons located above the table are available only when the “Use profile configuration” field is disabled.*



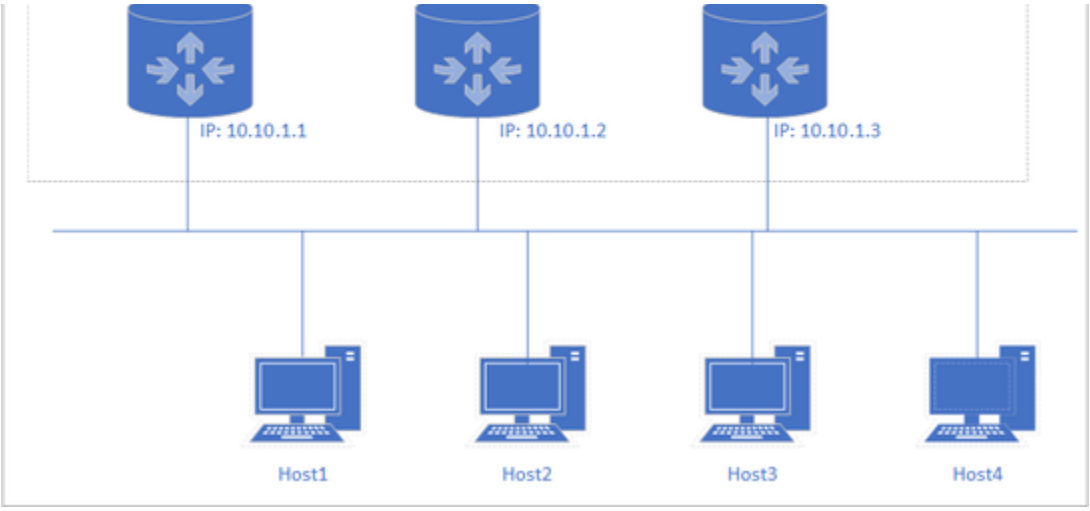
The fields available on the *Add captive portal* page are as follows:

Field	Description
Name	Enter a descriptive name for the captive portal profile.
Captive portal	Select one of the following authentication types to be used for the captive portal: • **Click-through**: Click-through authentication is an alternative sign-in method that does not require the end-user to create an account to access the service. The end-user clicks a button and then can access the Internet. • **Sign-on with basic login page**: This authentication type provides Internet access after successfully entering the user name and password. • **Sign-on with third-party credentials**: If you select this authentication type, it uses the third-party credentials hosted on an external server. The users need to provide login credentials to access the network. • **Sign-on with basic login and third-party credentials:** The user can log in either by using a basic login page or through third-party credentials.

Splash page editor	Click this button to edit the existing splash page or add a new splash page for the corresponding authentication type. For details, please refer to the Splash page editor page.
Basic login page	Select any one of the authentication methods. The credentials entered on the login page are validated against one of the following authentication servers: • **Local Authentication:** Local authentication is a method where the end-user is redirected to a page that provides options to enter username and password validated against the configured user database of the device. • **Authentication Server:** If this is selected, the end-user is redirected to a page that provides options to enter username and password validated against the configured external authentication server. The list of servers includes RADIUS, LDAP, POP3, Active Directory, and NT domain.
Local authentication	Select a local authentication server from the drop-down list. This field is available when you select **Local authentication** as the *Basic login page*.
Authentication server	Select one of the external authentication servers from the drop-down list and then select the **Primary**, **Secondary**, and **Tertiary** servers for the selected external authentication server. If you want to add an external authentication server, click the **Add a Server** button. This opens the *Add server* page of the selected server type. For details, please refer to the Authentication servers page. If you want to see a list of configured authentication servers, click the **Authentication server** list. You will be redirected to the Authentication servers page.
3rd party credentials	Select the checkbox of the external third-party server where the users provide credentials to gain access to the Internet.
Simultaneous login	It allows multiple clients to log in with the same credentials.
Session timeout	Session timeout is the time configured for the clients connected to the gateway to re-authenticate to continue using the Internet services. Enter or select the session timeout in minutes. The range is from 1 to 1440.
Session limited	You may restrict the number of active user sessions for each account. For example, if you select "*Unlimited*," it means an unlimited number of users can use the same account.
Idle timeout	Idle timeout refers to the end of the session when no data traffic is observed for the given amount of time. The client connected to the gateway has to re-authenticate once the idle timeout is observed to access the Internet. This value is per gateway and applicable to all the clients connected to the gateway. The range of idle timeout is between 1-1440 minutes.
URL redirection	If enabled, the user is redirected to the configured URL after the successful authentication.
URL for redirection	Enter the URL where you want the user to be redirected after a successful login.
Redirection interval	Select the periodic time interval when the user will be redirected to the URL mentioned in the above field.
Assign VLAN	Enable this feature if you want to assign the captive portal to any VLANs.
VLAN (ID/Name)	Select the VLAN ID or name on which the captive portal is to be enabled.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

High Availability

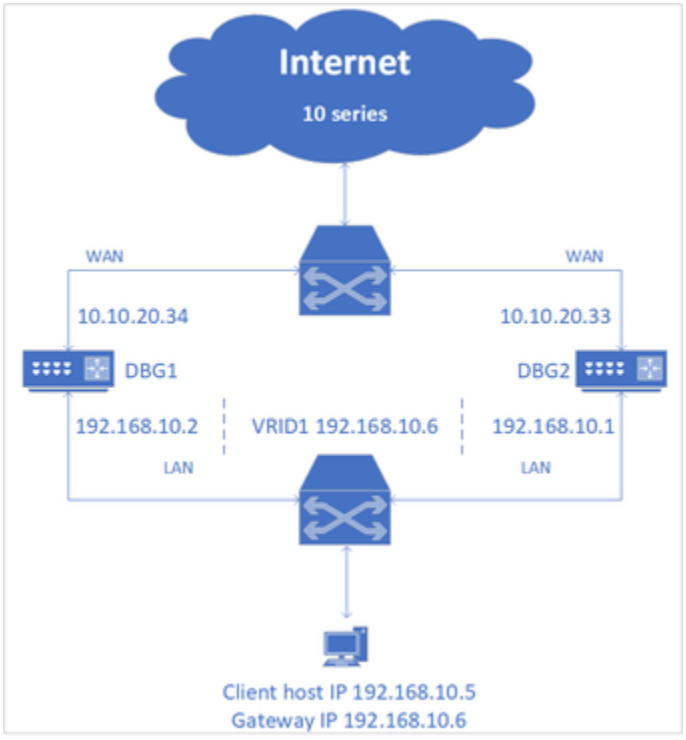
High availability refers to the availability of the default path without configuring dynamic routing or router discovery protocols on each host. The feature that is used to provide a default path is **Virtual Router Redundancy Protocol (VRRP)**. VRRP is an election protocol that dynamically assigns a virtual router to one of the VRRP routers on a LAN. A virtual router is a router that acts as a default router for hosts on the shared LAN. A VRRP router is configured to run the protocol with one or more virtual routers on the IP address of the physical Ethernet.



In VRRP, instead of having only one router, a group of virtual routers is provided; If one fails, the other will take over the failed router and its IP addresses and provides uninterrupted service to the hosts. In the above configuration, the end-hosts install a default route to the IP address of the virtual router A, and all the three routers run VRRP. Router A becomes the Master Virtual router, and the other two routers become the backup routers. If the master virtual router A fails, it passes the packets to the backup virtual router, selected based on the priority given to the backup routers. The backup router (let's say 'Virtual router B') becomes the master immediately and maintains the connectivity between the hosts. Once the failed master virtual router becomes functional, the backup router (Virtual router B) forwards the packets through the recovered Virtual router A.

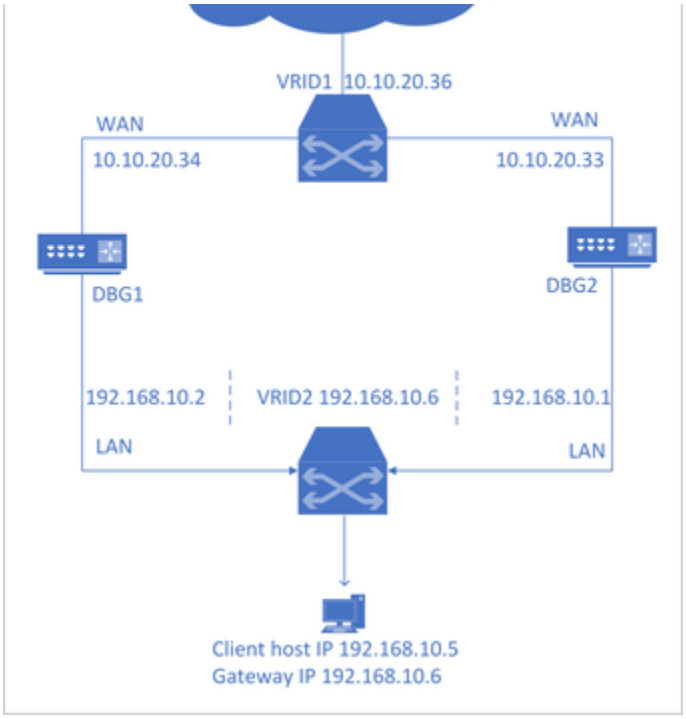
DBG-2000 supports the VRRP feature, and it has been described in detail using the following two test cases and their topologies:

1. Test case 1



The routers (DBG1 and DBG2) have been configured with the VRRP feature for the LAN interface and are given priority numbers. For example, let's say the priority of DBG1 is 200 and DBG2 is 100. Then, when the client tries to connect to the Internet, it follows the DBG with a higher priority number. Here, it follows DBG1. But, if DBG1 gets disconnected or not reachable, it connects with the second router DBG2, and when DBG1 regains its functionality, it switches to DBG1.

2. Test case 2

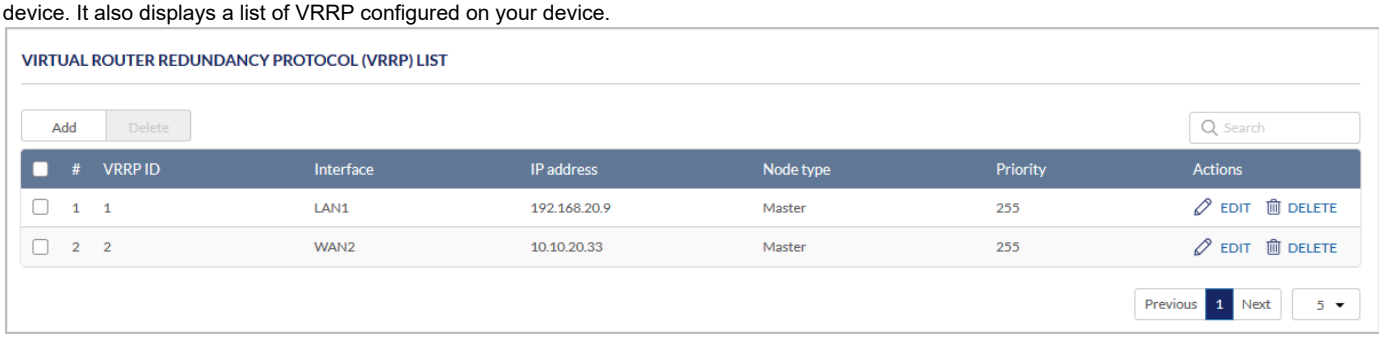


The routers (DBG1 and DBG2) have been configured with the VRRP feature for both the interfaces (LAN and WAN) and are given priority numbers. Then, when the client tries to connect to the Internet, it follows the router with a higher priority number (say DBG1). When the DBG1 WAN is not reachable or disconnected from the topology, it connects to the DBG2 WAN, and when DBG1 WAN gets connected or becomes functional, it again switches to DBG1.

To configure your DBG-2000, refer to VRRP List & Configuration.

VRRP List & Configuration

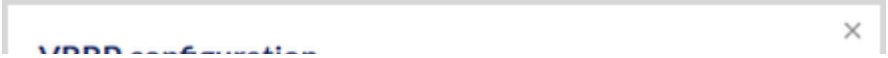
This page of the Nuclias cloud gateway's user interface allows you to configure the VRRP, i.e., Virtual Router Redundancy Protocol, on your device. It also displays a list of VRRP configured on your device.

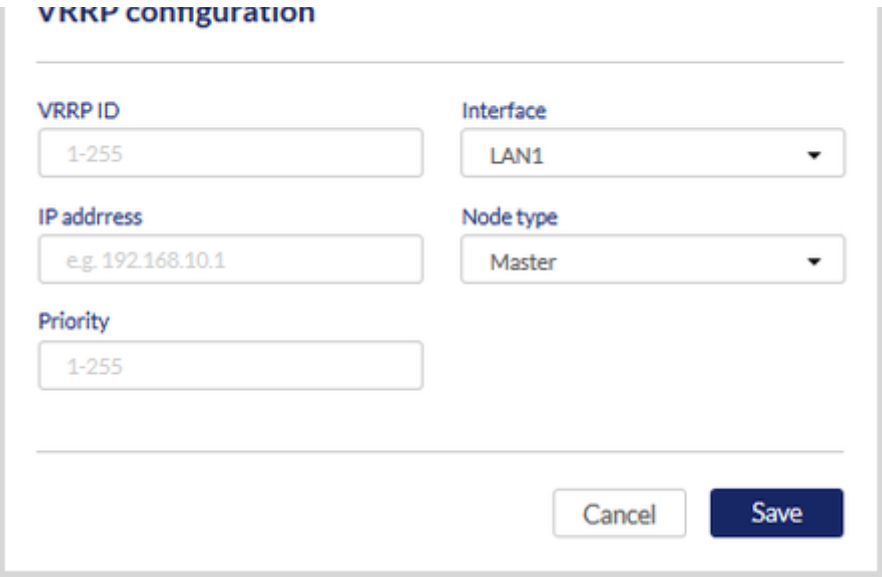


The fields displayed in the *Virtual Router Redundancy Protocol (VRRP) List* are as follows:

Field	Description
VRRP ID	It displays the ID given to the VRRP routers.
Interface	It displays the interface on which the VRRP has been configured.
IP address	It displays the IP address of the VRRP router.
Node type	It indicates if the selected VRRP router is working as a **Master** router or a **Backup** router.
Priority	It indicates the priority given to the configured VRRP router.
Actions	You can edit or delete the selected VRRP.

Click **Add** to add a new entry to the list. This opens the *VRRP configuration* page. If you want to delete multiple entries at once, select the corresponding checkboxes, and click **Delete**.





The fields available on the *VRRP configuration* page are as follows:

Field	Description
VRRP ID	Specify an ID to the VRRP router.
Interface	Select the interface on which you want to configure VRRP.
IP address	Enter the IP address of the VRRP router.
Node type	Select the node type for the VRRP router. Select **Master** if you want the VRRP router to work as a master, and select **Backup** if you want it to be the backup router.
Priority	It indicates the priority given to the respective router. If the master is unavailable, then the highest priority Backup will transit to Master, providing a controlled transition of the virtual router responsibility with minimal service interruption.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to previous settings.

Chapter 4 Security

This chapter introduces you to the security features supported by the Nuclias cloud gateway. These features include Firewall, IPS, Web content filtering, and Application control. These are the various techniques used to block any malicious attacks from the Internet to access your network. You can also configure your own Internet policies to allow only selected web-based information.

This chapter covers the following topics:

Firewall

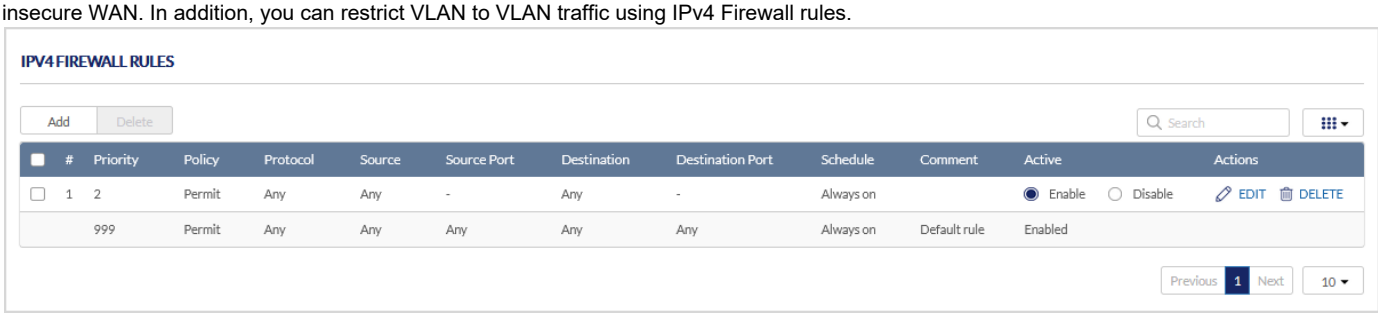
The *Firewall* section of the Security deals with the various methods adopted by the Nuclias cloud gateway to ensure a safe and secure network. In this section, you will learn about the Firewall rules configuration on the IPv4 networks. These are the rules defined to keep a check on the incoming and outgoing traffic of the network. You can state which traffic is to be allowed or blocked. Similarly, the Port Forwarding method can restrict access to traffic entering your network while allowing only specific outside users to access specific local resources. When you have multiple public IP addresses and multiple servers across the firewall, the 1:1 NAT method is used.

This section covers the following topics:

Expand all Collapse all

IPv4 Firewall Rules

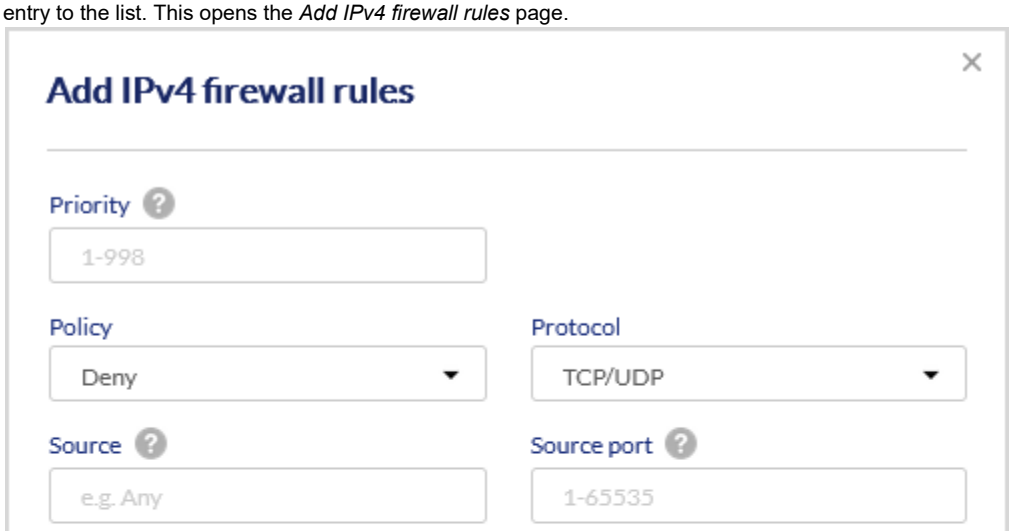
Outbound (LAN/DMZ to WAN) rules restrict access to traffic leaving your network, selectively allowing only specific local users to access specific outside resources. The default outbound rule allows access from the secure zone (LAN) to either the public DMZ or insecure WAN. On the other hand, the default outbound rule is to deny access from DMZ to insecure WAN. In addition, you can restrict VLAN to VLAN traffic using IPv4 Firewall rules.

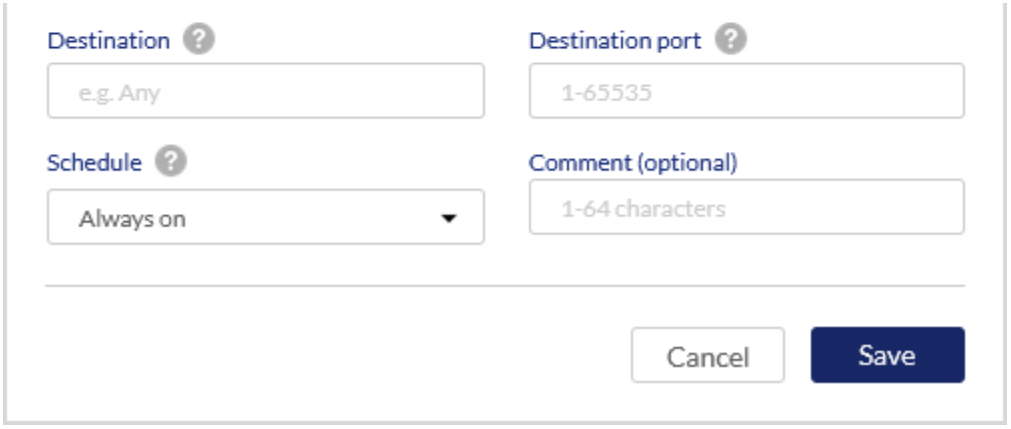


The fields displayed in the *IPv4 Firewall Rules* table are as follows:

Field	Description
Priority	It specifies the priority of the configured rule.
Policy	It displays the policy applied to the particular firewall rule. It is either **Deny** or **Permit**.
Protocol	It displays the protocol for which the firewall rule is defined.
Source	It displays the source IP address range, a specific IP address, or Any for all IP addresses on which the firewall rule is applied.
Source port	It displays a range of ports, specific ports, or Any for all source ports assigned for the configured protocol.
Destination	It displays the destination IP address range, a specific IP address, or Any for all IP addresses on which the firewall rule is applied.
Destination port	It displays a range of ports, specific ports, or Any for all destination ports assigned for the configured protocol.
Schedule	It displays the schedule when the firewall rule is applied.
Comment	It displays the comment added for the firewall rule.
Active	You can enable or disable the respective IPv4 firewall rule, except for the *Default rule*. ***Note**: You can edit this field only when the "Use profile configuration" field is disabled.*
Actions	You can edit or delete the configured firewall rule except for the *Default rule*. ***Note**: This field is available only when the "Use profile configuration" field is disabled.*

To delete multiple entries at once, select the checkboxes of the IPv4 firewall rules you want to delete, and click **Delete**. Click **Add** to add a new entry to the list. This opens the *Add IPv4 firewall rules* page.



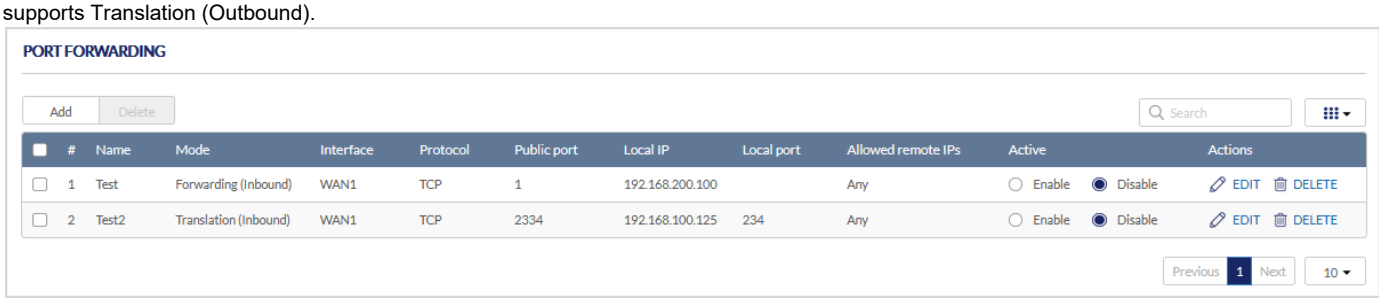


The fields displayed on this page are as follows:

Field	Description
Priority	Define the priority of the IPv4 firewall rule. The smaller the number, the higher the priority.
Policy	Select either **Deny** or **Permit**.
Protocol	Select the protocol on which you want to configure the firewall rule. The options are Any, TCP, UDP, TCP/UDP, and ICMP.
Source	Enter a specific IP address, a range of IP addresses, or any IP addresses from where the traffic is sent.
Source port	Specify a source port or multiple source ports where the traffic generates. This field appears only when you select TCP, UDP, or TCP/UDP protocols.
Destination	Enter a specific IP address, a range of IP addresses, or any IP addresses where the traffic is sent.
Destination port	Specify a destination port or multiple destination ports that will receive the traffic for this firewall rule. This field appears only when you select TCP, UDP, or TCP/UDP protocol.
Schedule	Select a schedule from the drop-down list. You can define the time and day when the IPv4 firewall rule is to be applied. To configure a schedule, refer to the Schedule policies section.
Comment (Optional)	Enter the comment. This field is optional.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

Port Forwarding

Port forwarding is a process to restrict access to traffic entering your network, selectively allowing only specific outside users to access specific local resources. By default, all access from the WAN side is blocked from accessing the secure LAN, except in response to the LAN or DMZ requests. To allow outside devices to access services on the secure LAN, you must create a port forwarding rule for each service. It also supports Translation (Outbound).

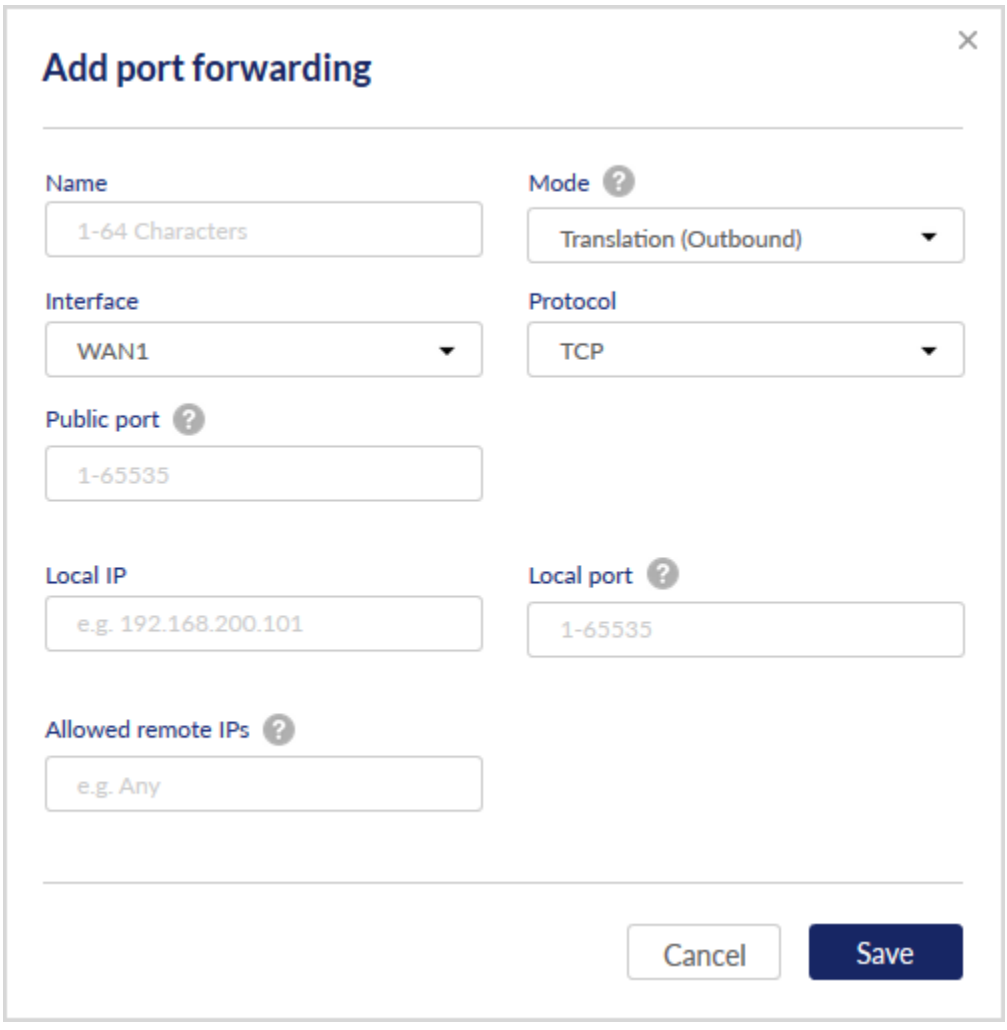


The fields displayed in the *Port forwarding* table are as follows:

Field	Description
Name	It displays the name of the rule.

Mode	It displays the mode configured for the selected rule.
Interface	It displays the interface on which the rule is configured.
Protocol	It displays the protocol followed for the configured rule.
Public port	It displays the public port number.
Local IP	It displays the LAN host IP address.
Local port	It displays the LAN host port numbers.
Allowed remote IPs	It displays the IP addresses that can accept to and from traffic.
Active	You can enable or disable the respective rule. ***Note**: You can edit this field only when the "Use profile configuration" field is disabled.*
Actions	Click **Edit** to make changes in the existing port forwarding rule. Click **Delete** to delete the rule. ***Note**: This column is available only when the "Use profile configuration" field is disabled.*

Click **Add** to add a new entry. This opens the *Add port forwarding* page. To delete multiple entries, select the checkboxes that you want to delete, and click **Delete**.



The fields available on the *Add port forwarding* page are as follows:

Field	Description
Name	Enter the name for your rule.

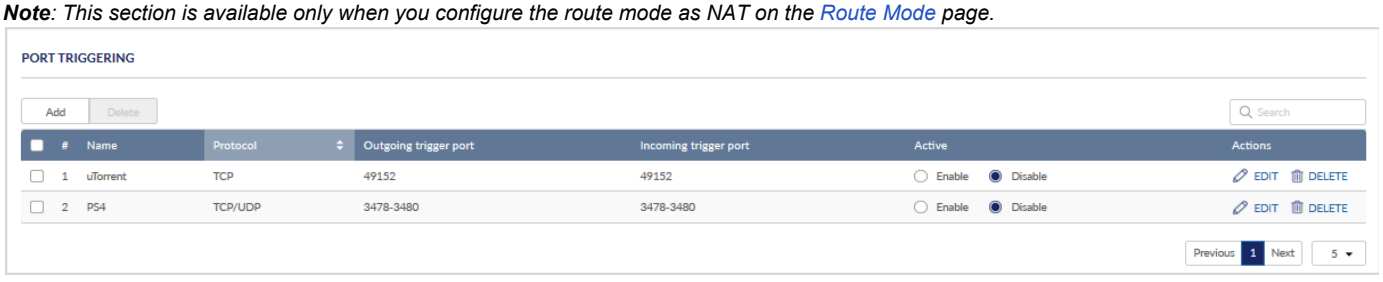
Mode	Select any one of the following modes: • **Forwarding (Inbound)**: If you select this mode, traffic passes from the WAN host to the LAN host for a public destination port. • **Translation (Outbound**): It translates the traffic from a local source port number to the configured public source port number for the LAN host to the WAN host traffic. • **Translation (Inbound)**: If you select this mode, traffic passes from the WAN host to the LAN host and translates to the destination local port when the traffic is sent on the public destination port. ***Note**: Translation (Inbound) and Translation (Outbound) options are available only when the route mode is configured as NAT on the Route mode page.*
Interface	Select the interface on which this rule will be applied.
Protocol	Select one of the following protocols: TCP, UDP, or TCP/UDP.
Public port	Enter the port number on which the applications are running on the WAN host.
Local IP	Enter the LAN host IP address. For Translation (Outbound), it refers to the IP address from where the traffic will be originating. For Translation (Inbound) or Forwarding (Inbound), it refers to the IP address to which the traffic will be sent. ***Note**: This field is not available only when you configure the route mode as Router on the Route mode page.*
Local port	Local port refers to the LAN host port numbers. For outbound, it means local source port, and for inbound, it means the destination local port for the LAN host. This field is available only when you select **Translation (Outbound)** or **Translation (Inbound)** mode. ***Note:*** • *Mapping a range of public ports to a range of local ports, the ranges must be the same length.* • *This field is not available only when you configure the route mode as Router on the Route mode page.*
Allowed remote IPs	Enter the allowed remote IPs. Allowed remote IPs are the IPs that accept to (for Translation Outbound) and from traffic (for Translation Inbound and Forwarding Inbound).
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

Port Triggering

Port triggering allows devices on the LAN or DMZ to request one or more ports to be forwarded to them. This feature waits for an outbound request from the LAN or DMZ on one of the defined outgoing ports and then opens an incoming port for that type of traffic. This can be a form of dynamic port forwarding while an application transmits data over the opened outgoing or incoming port(s).

Port triggering application rules are more flexible than static port forwarding, which is an option when configuring forwarding rules. This is because a port triggering rule does not reference a specific LAN IP or IP range. Also, ports are not left open when not in use, thereby providing a level of security that port forwarding does not offer.

***Note**: This section is available only when you configure the route mode as NAT on the Route Mode page.*

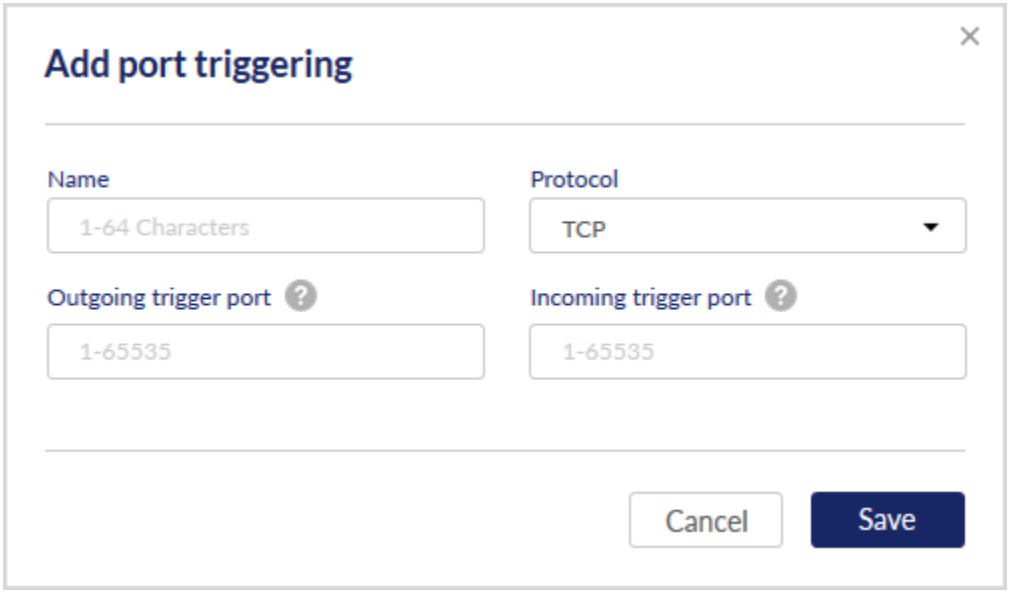


The fields displayed in the *Port Triggering* table are as follows:

Field	Description
Name	It displays the name of the port-triggering rule.

Protocol	It displays the protocol on which the rule is being configured. It is TCP, UDP, or TCP/UDP.
Outgoing trigger port	It displays the start and end trigger port range.
Incoming trigger port	It displays a port range that is open to receive the traffic.
Active	You can enable or disable the port-triggering rule. ***Note**: You can edit this field only when the "Use profile configuration" field is disabled.*
Actions	You can edit or delete the corresponding port-triggering rule. ***Note**: This field is available only when the "Use profile configuration" field is disabled.*

Click **Add** to add a new entry. This opens the *Add port triggering* page. To delete multiple entries, select the checkboxes you want to delete, and click **Delete**.



The fields available on this page are as follows:

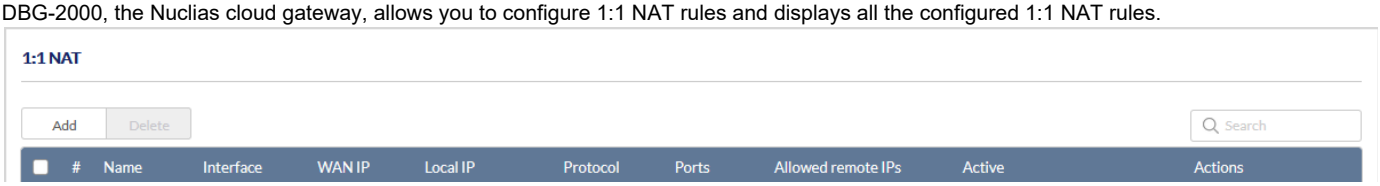
Field	Description
Name	Enter the name of the port-triggering rule.
Protocol	Select the protocol on which the rule is to be configured. It is TCP, UDP, or TCP/UDP.
Outgoing trigger port	Enter the start and end trigger port range.
Incoming trigger port	Enter the port range that is open to receive the traffic.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

1:1 NAT

1:1 NAT is a firewall technique when multiple public IP addresses and multiple servers are available across the firewall. As the name suggests, it maps one internal IP address to one external IP address. To carry out the whole process, first, it has to set up an external IP address alias, then map the inbound traffic and redirect it to the correct internal IP address. In addition, it also maps the outbound traffic from the internal IP address and directs it to the destined external IP address.

***Note**: This section is available only when you configure the route mode as NAT on the Route Mode page.*

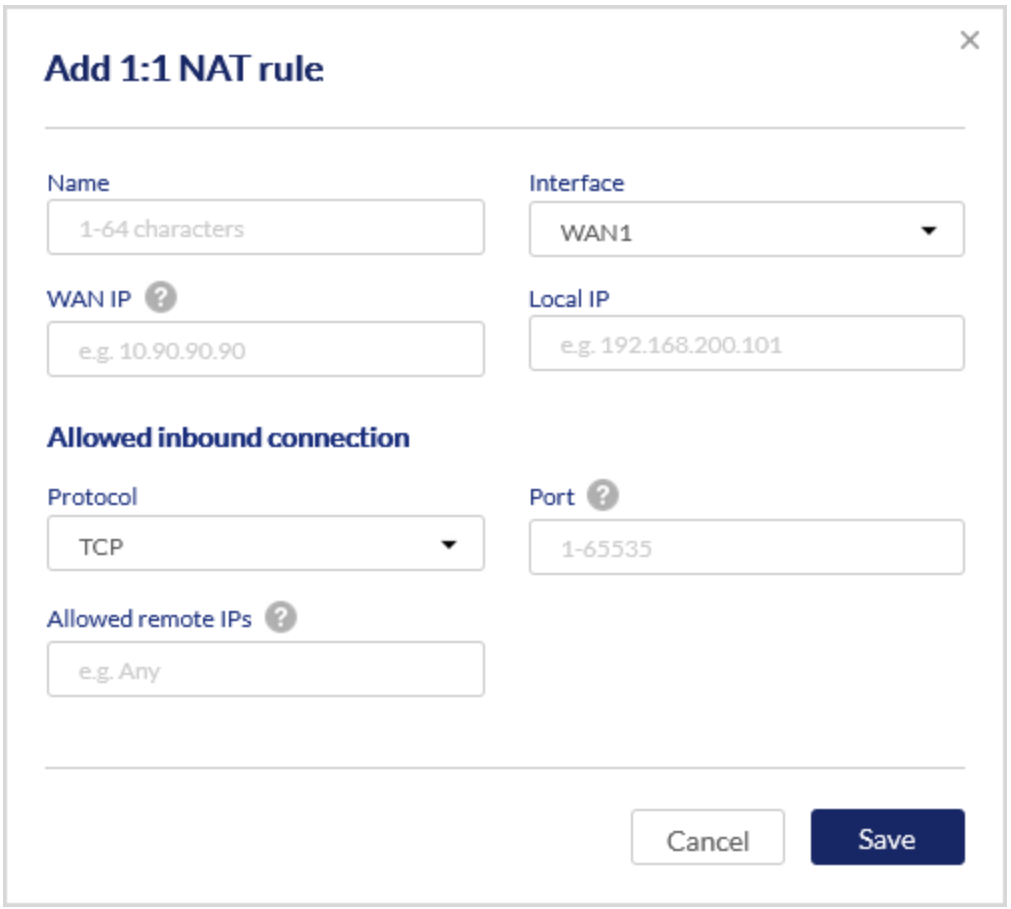
DBG-2000, the Nuclias cloud gateway, allows you to configure 1:1 NAT rules and displays all the configured 1:1 NAT rules.



The fields displayed in the *1:1 NAT* table are as follows:

Field	Description
Name	It displays the name of the rule.
Interface	It displays the WAN for which it is configured.
WAN IP	It displays the public IP address for which the local IP address is mapped.
Local IP	It displays the local IP address from which the WAN IP address is mapped.
Protocol	It displays the protocol on which the rule has been configured.
Ports	It displays the port number or a range of ports allowed to access the internal resource.
Allowed remote IPs	It displays the IP addresses from which the firewall accepts traffic.
Active	You can enable or disable the selected rule. ***Note**: You can edit this field only when the "Use profile configuration" field is disabled.*
Actions	You can edit or delete the configured 1:1 NAT rule. ***Note**: This column is available only when the "Use profile configuration" field is disabled.*

Click **Add** to add a new entry. This opens the *Add 1:1 NAT rule* page. To delete multiple entries, select the checkboxes you want to delete, and click **Delete**.



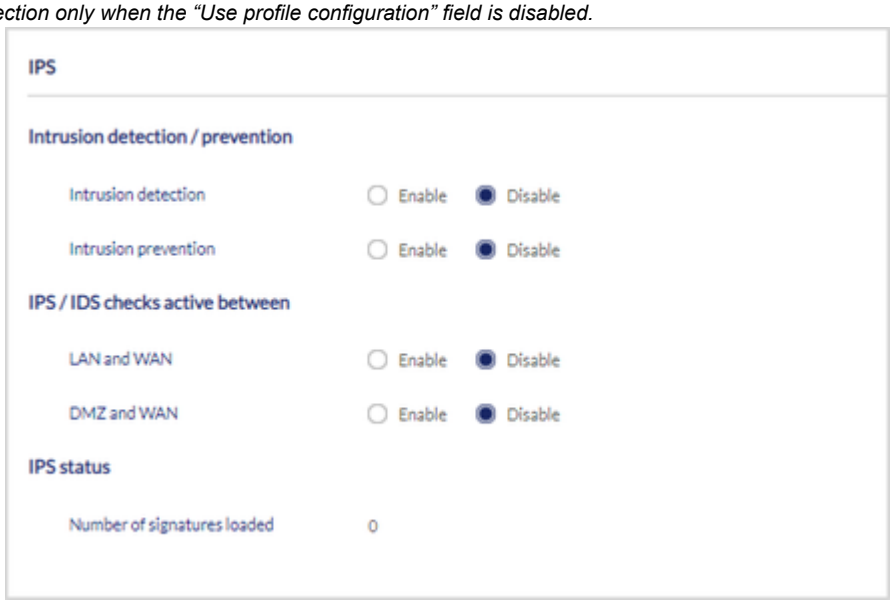
The fields available on the *Add 1:1 NAT rule* page are as follows:

Field	Description
Name	Enter a descriptive name of the rule.
Interface	Select the WAN interface on which the rule will be applied.
WAN IP	Enter the public IP address for which the local IP address is mapped.
Local IP	Enter the local IP address from which the WAN IP address is mapped.
Allowed inbound connection	
Protocol	Select a protocol to be used while allowing the inbound connection. The options are TCP, UDP, and TCP/UDP.
Port	Select the port or a range of ports to be used for the connection.
Allowed remote IPs	Enter the remote IP addresses that will be allowed to establish the inbound connections.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

IPS

The gateway's Intrusion Prevention System (IPS) prevents malicious attacks from the Internet from accessing the private network. Static attack signatures loaded to the gateway allow common attacks to be detected and prevented. In addition, you can enable checks between the WAN and DMZ or LAN.

***Note**: You can edit this section only when the "Use profile configuration" field is disabled.*



The fields available on this page are as follows:

Field	Description
Intrusion detection/prevention	
Intrusion detection	Enable or disable intrusion detection.
Intrusion prevention	Enable or disable intrusion prevention.
IPS/IDS checks active between	
LAN and WAN	Enable it to detect intrusions between LAN and WAN interfaces.
DMZ and WAN	Enable it to detect intrusions between DMZ and WAN interfaces.
IPS status	

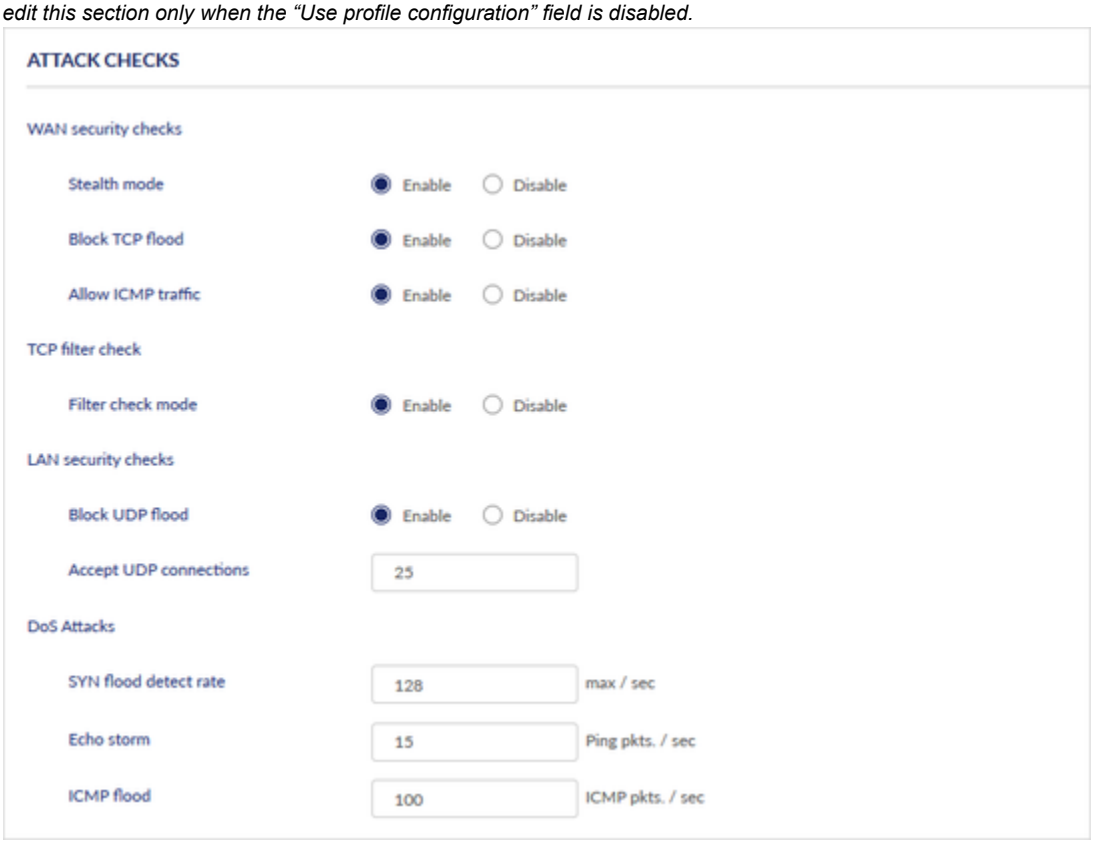
Number of signatures loaded	It displays the number of signatures loaded.

Attack Checks

Attacks can be malicious security breaches or unintentional network issues that render the gateway unusable. Attack checks allow you to manage WAN security threats, such as continual ping requests and discovery via ARP scans. You can enable TCP and UDP flood attack checks to manage extreme usage of WAN resources.

Additionally, you can block certain Denial-of-Service (DoS) attacks. These attacks, if uninhibited, can use up processing power and bandwidth and can prevent normal regular network services. You can also configure ICMP packet flooding, SYN traffic flooding, and Echo storm thresholds to suspect traffic from the offending source temporarily.

***Note**: You can edit this section only when the "Use profile configuration" field is disabled.*



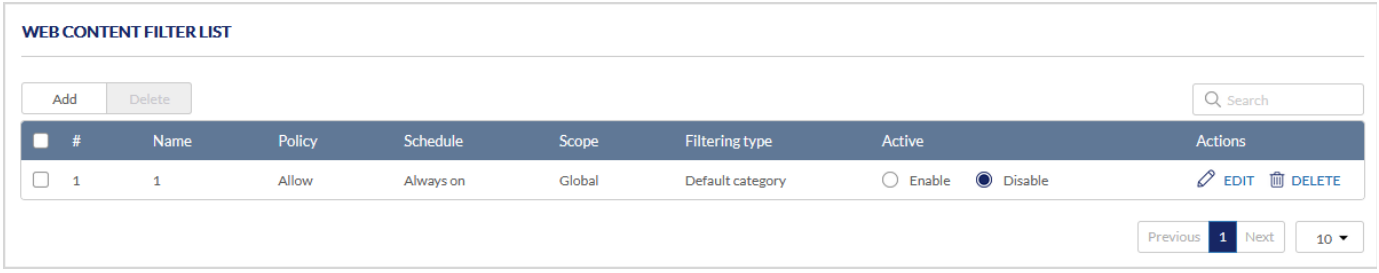
The fields available on this page are as follows:

Field	Description
WAN security checks	
Stealth mode	If this option is enabled, the gateway will not respond to port scans from the WAN. This makes it less susceptible to discovery and attacks.
Block TCP flood	If this option is enabled, the gateway drops all invalid TCP packets and gets protected from the TCP flood attack.
Allow ICMP traffic	If this option is enabled, the WAN host can ping traffic to the WAN interface.
TCP filter check	
Filter check mode	If this option is enabled, the gateway drops invalid TCP packets (FIN, RST, and ACK) going with SNAT while the connection is closed. Some of the other packets, like TCP OUT-OF-WINDOW, are also considered to be invalid. Disable this option while taking performance, as enabling this option will affect the throughput.
LAN security checks	
Block UDP flood	If this option is enabled, the gateway will not accept more than the configured value in *Acce pt UDP connections*, indicating simultaneous, active UDP connections from a single computer on the LAN.

Accept UDP connections	Enter the number of UDP connections simultaneously accepted by the gateway from a single computer on the LAN. You can select any number between 25 to 500. This field is available when you enable *Block UDP flood*.
DoS Attacks	
SYN flood detect rate	Enter the rate at which the SYN flood can be detected.
Echo storm	Enter the number of ping packets per second at which the gateway detects an Echo storm attack from the WAN and prevents further ping traffic from that external address.
ICMP flood	Enter the number of ICMP packets per second at which the gateway detects an ICMP flood attack from the WAN and prevents further ICMP traffic from that external address.

Web Content Filter

The gateway offers standard web filtering options to filter out the web page displayed by the domain names. It allows you to create Internet access policies between LAN and WAN. Instead of creating policies based on the type of traffic (as is the case when using firewall rules), web-based content itself can be used to determine if the traffic is allowed or dropped.

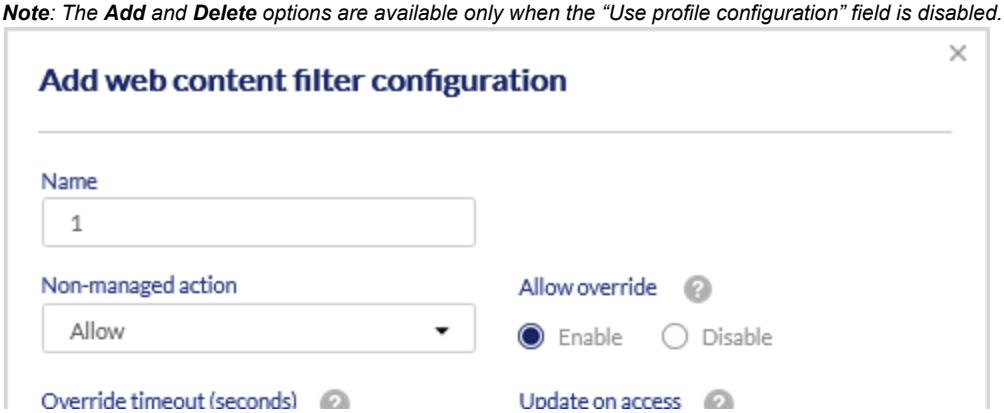


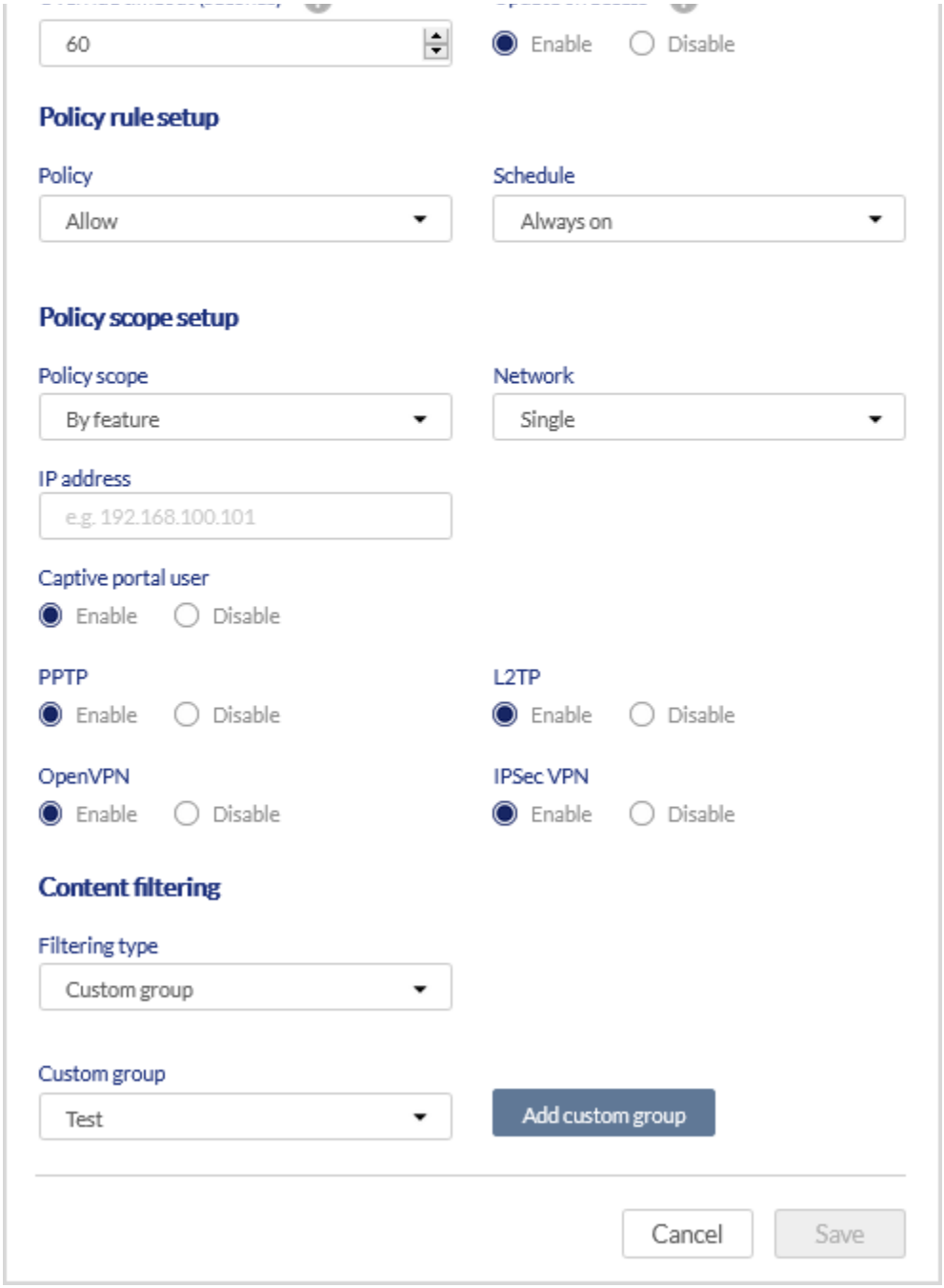
The fields displayed in the *Web content filter list* are as follows:

Field	Description
Name	It displays the name of the policy.
Policy	It displays the policy rule.
Schedule	It displays the schedule selected for the policy.
Scope	It displays the scope. It is either Global or Feature.
Filtering type	It displays the type of information you want to filter with this policy.
Active	You can enable or disable the policy. ***Note**: You can edit this field only when the "Use profile configuration" field is disabled.*
Actions	You can edit or delete the selected web content filter policy. ***Note**: This field is available only when the "Use profile configuration" field is disabled.*

Click **Add** to add a new entry. This opens the *Add web content filter configuration* page. To delete multiple entries, select the checkboxes of the web content filter you want to delete, and click **Delete**.

***Note**: The **Add** and **Delete** options are available only when the "Use profile configuration" field is disabled.*





The fields available on the *Add web content filter configuration* page are as follows:

Field	Description
Name	Enter the name of the policy.
Non-managed action	This is an action to be taken for the Non-Managed Site. You can Allow or Block. By default, it is Allow.
Allow override	If enabled, it allows the sites categorized under Blocked categories.
Override timeout (seconds)	Enter the time (in seconds) for which all the disallowed categories will be allowed.
Update on access	Enable the field to restart the override timer on each new access to disallowed categories.
Policy rule setup	
Policy	Select the policy rule. The options are *Allow* and *Block*.

Schedule	Select the schedule when the policy rule is to be applied. To configure a schedule, refer to the Schedule policies page.
Policy scope setup	
Policy scope	Select either *Global* or *By Feature* as the policy scope. The global policy affects all types of traffic matching the selected application(s). If you select *By Feature*, the following additional fields will be available.
Network	Select one of the configured network profiles. You can select *None, Single*, *Range*, or *Interface*.
IP address	If you select a **Single** as the *Network*, enter the IP address.
Starting IP address	If you select **Range** as the *Network*, enter the starting IP address of the IP range.
Ending IP address	If you select **Range** as the *Network*, enter the ending IP address of the IP range.
Interface	If you select **Interface** as the *Network*, select the configured interface from the drop-down list.
Captive portal user	Enable or disable the *Captive Portal user* option. Enabling this option allows all Captive Portal clients to follow this policy.
PPTP	Enable or disable the PPTP VPN. Enabling this option allows PPTP traffic to follow this policy.
L2TP	Enable or disable the L2TP VPN. Enabling this option allows L2TP traffic to follow this policy.
OpenVPN	Enable or disable the OpenVPN. Enabling this option allows OpenVPN traffic to follow this policy.
IPSec VPN	Enable or disable the IPSec VPN. Enabling this option allows IPSec traffic to follow this policy.
Content filtering	
Filtering type	This field allows you to select the type of information you want to filter. Select any one of the following options: • **Default category**: Select the default categories that you want to filter. • **URL**: The URL filtering section is available on the next page. Click the **Next** button located in the lower-right corner of the page to add URLs or keywords. • **Default category+URL**: Select a default category from the drop-down list, and add URLs/keywords in the URL filtering section available on the next page. • **Custom group**: Select one of the configured custom groups or create a new group.
URL filtering	To add a URL (HTTP or HTTPS), domain name, or a keyword, select **Add URL/keyword**. Click **+Add** to add more than one entry. If you want to add URLs or keywords at once, select **Bulk import**. Click **Browse** and select the file (in CSV format) whose information you want to import into the database. You can download the sample template file here. *Note that the number of entries is limited to a maximum of 512 URLs.*
Default category	This field is available when you select the *Default category* or *Default category+URL* as the filtering type. Select the type of categories to be filtered from the drop-down list.
Custom group	Select any one of the configured custom groups from the drop-down list. To create a new group, click **Add custom group**. This opens the *Add group configuration* page. For details, refer to Custom Group List.
Previous	Click **Previous** to go back to the previous configuration page.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

Custom Group List

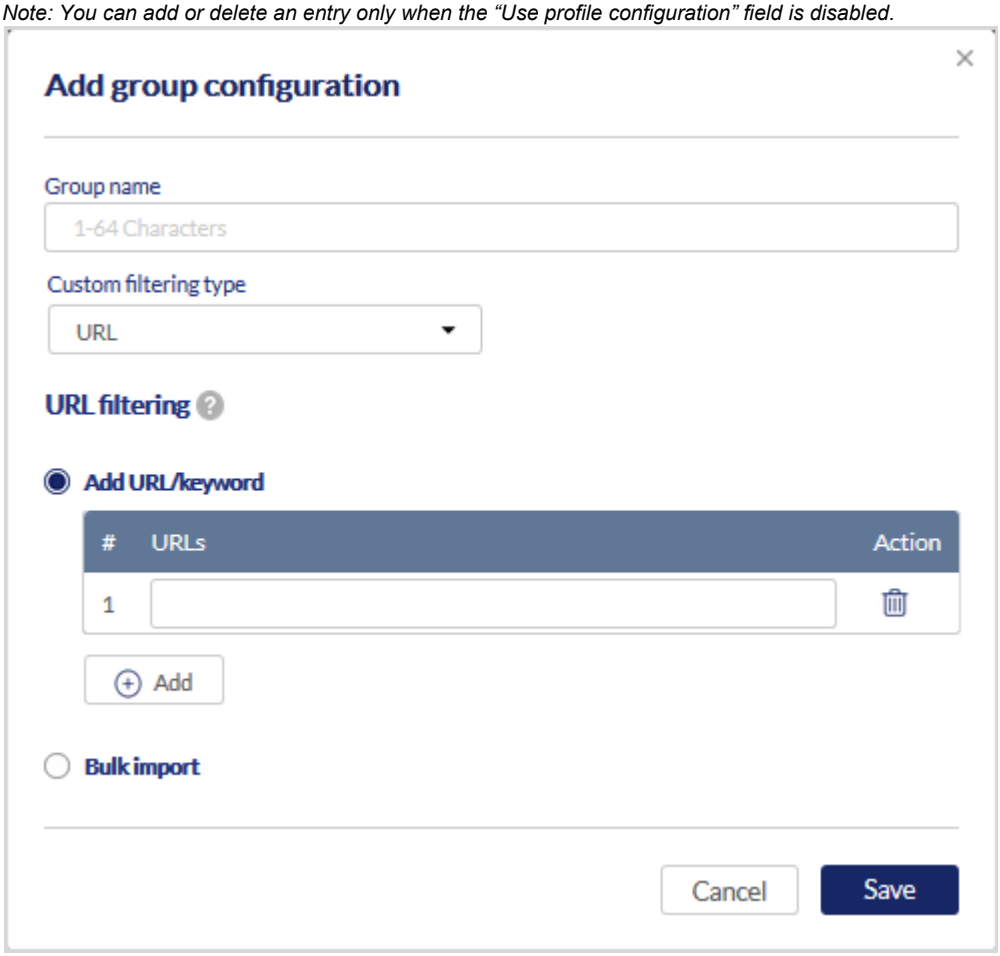
Users can select a particular URL or select a group to manage URLs associated with that group. This section displays groups and URLs associated with them.

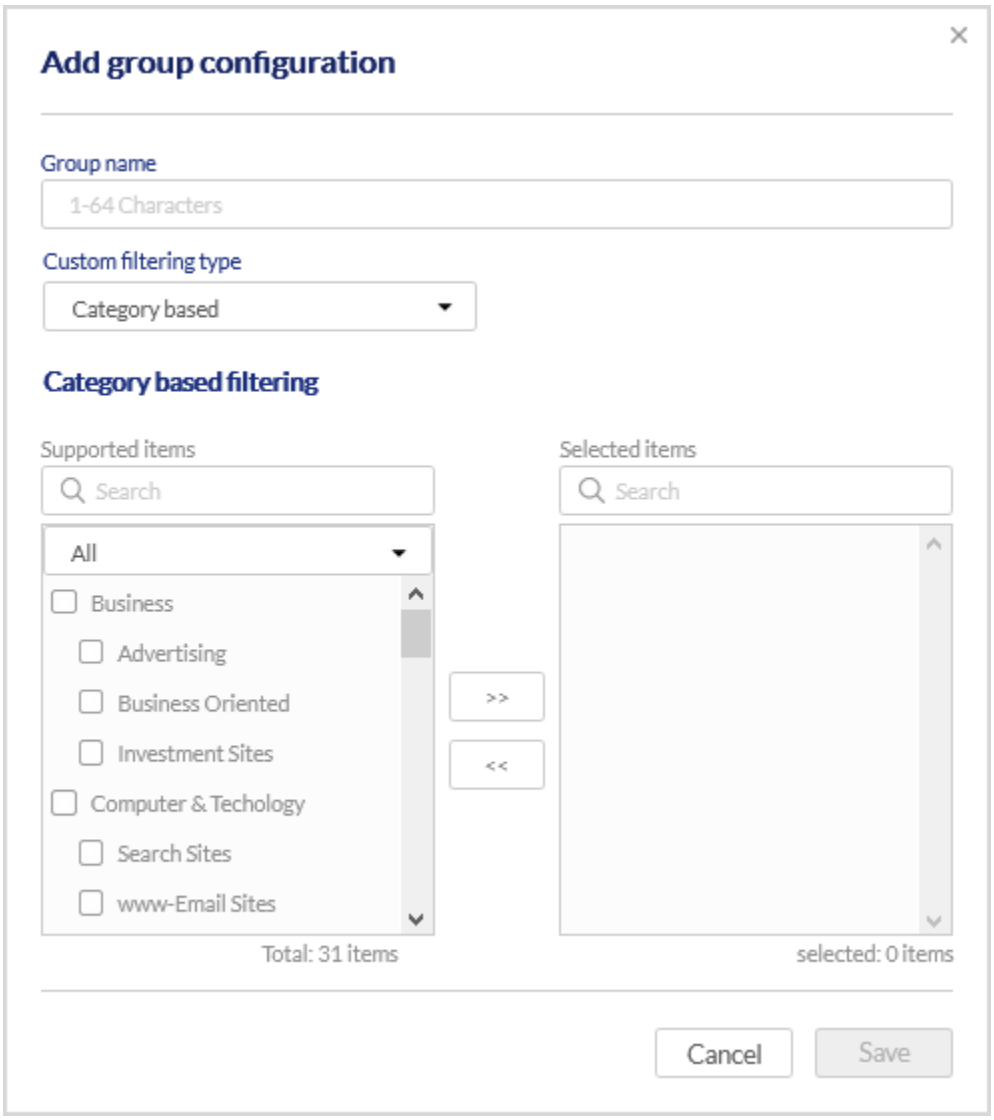
The fields displayed in the *Custom Group List* table are as follows:

Field	Description
Name	It displays the name of the group.
URLs	It displays the list of selected URLs.
Category filtering	It displays the category to which these URLs belong.
In use	It displays if that custom group is in use or not.
Actions	You can edit or delete the group list. ***Note**: This field is available only when the "Use profile configuration" field is disabled.*

Click **Add** to add a new group. This opens the *Add group configuration* page.

Note: You can add or delete an entry only when the "Use profile configuration" field is disabled.





The fields available on this page are as follows:

Field	Description
Group name	Enter a name for your group.
Custom filtering type	Select one of the following types of filtering you want to apply to your group: • **URL**: If you select this option, the *URL Filtering* section will be available. • **Category-based**: If you select this option, the *Category-based filtering* section will be available. • **URL+Category-based**: If you select this option, both the above sections will be available. Click the **Next** button located at the lower-right corner of the page to go to the *Category-based filtering* section.
Add URL/keyword	Select this option to add a new URL. Enter the URL in the box; 1 to 64 characters are allowed. To add a new URL, click the **+Add** button.
Bulk import	To import URLs in bulk, select “Bulk import.” Next, click **Browse** to locate the file on your system, and then import the file in ***.csv** format. You can download the sample template file here. *Note that the number of entries is limited to a maximum of 512 URLs.*
Supported items	Select one or more checkboxes of the categories that you want to filter. Then, click the **“>>”** button to move it to the box of the selected item. This is available when you select either “**C ategory-based**” or “**URL+Category-based**” filtering type.

Selected items	This box displays the items selected from the supported items list. To remove the item from the selected list, click the **"<<"** button. This is available when you select either "**Category-based**" or "**URL+Category-based**" filtering type.
Next	Click **Next** to go to the *Category-based filtering* section. This button is available only when you select **URL+ Category-based** filtering type.
Previous	Click **Previous** to go back to the *URL filtering* section. This button is available only when you select **URL+ Category-based** filtering type.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

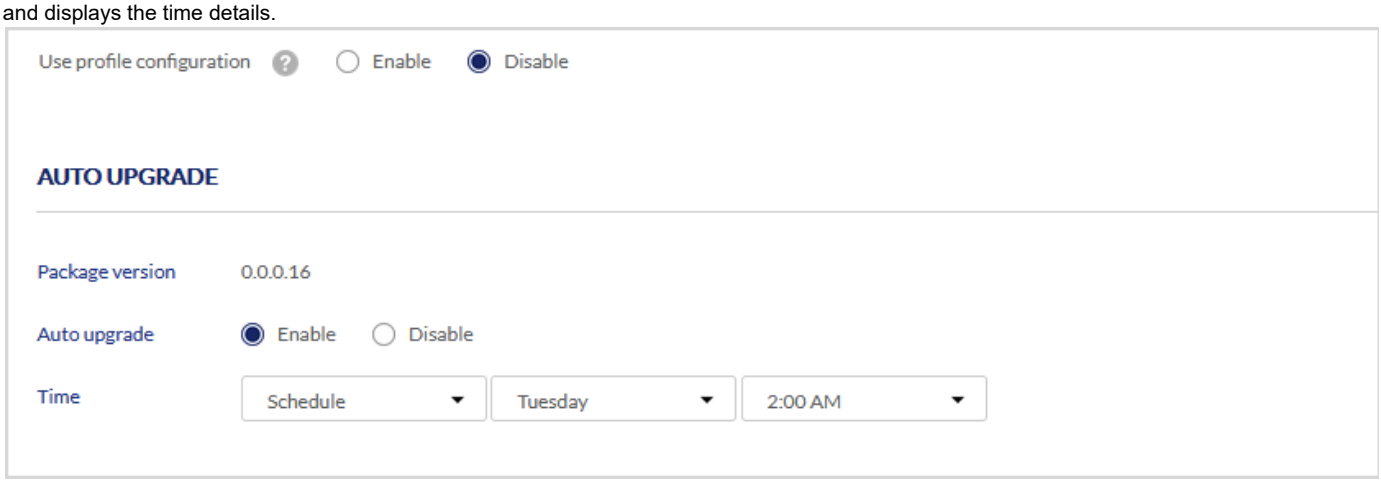
Application Control

Application Control is a feature that allows network administrators to allow, block, or control the traffic of applications that is transacting the traffic. It allows you to block or allow any specific applications, like Netflix, YouTube, Facebook, Twitter, etc.

This section covers the following topics:

Auto Upgrade

This section provides the current package version running on the device. You can enable or disable the *Auto upgrade* feature only when the *Use profile configuration* field is disabled. The auto-upgrade feature allows the user to define a time interval or a schedule for the device to auto-check for the updated packages on the server. When the *Use profile configuration* field is enabled, the *Auto upgrade* feature is automatically enabled and displays the time details.

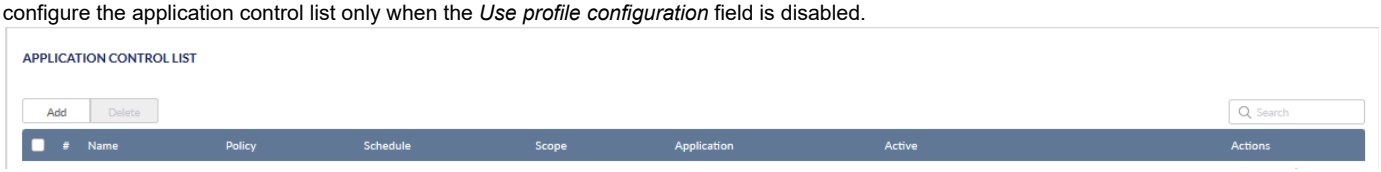


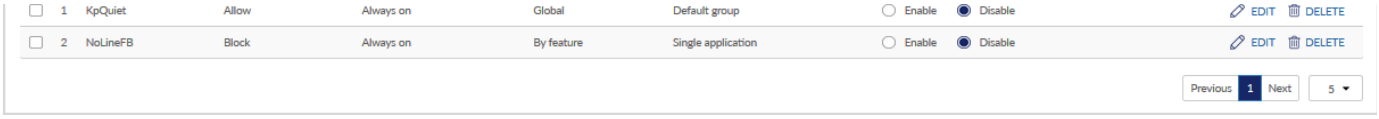
The fields available in this section are as follows:

Field	Description
Package version	It provides details about the running package version.
Auto upgrade	Enable or disable the Auto upgrade option. ***Note**: This field is available only when the "Use profile configuration" field is disabled.*
Time	Select either *Interval* or *Schedule* to check for updated packages on the server. If you select *Interval*, enter the number of minutes after which the device will check for the updates. If you select *Schedule*, choose a **Day** and **Time**.

Application Control List

The user can select a particular app or select a group to manage applications associated with that group. This provides an administrator with more options to set up policies to control access to the applications for the selected network users, IP addresses, or network segments. You can configure the application control list only when the *Use profile configuration* field is disabled.



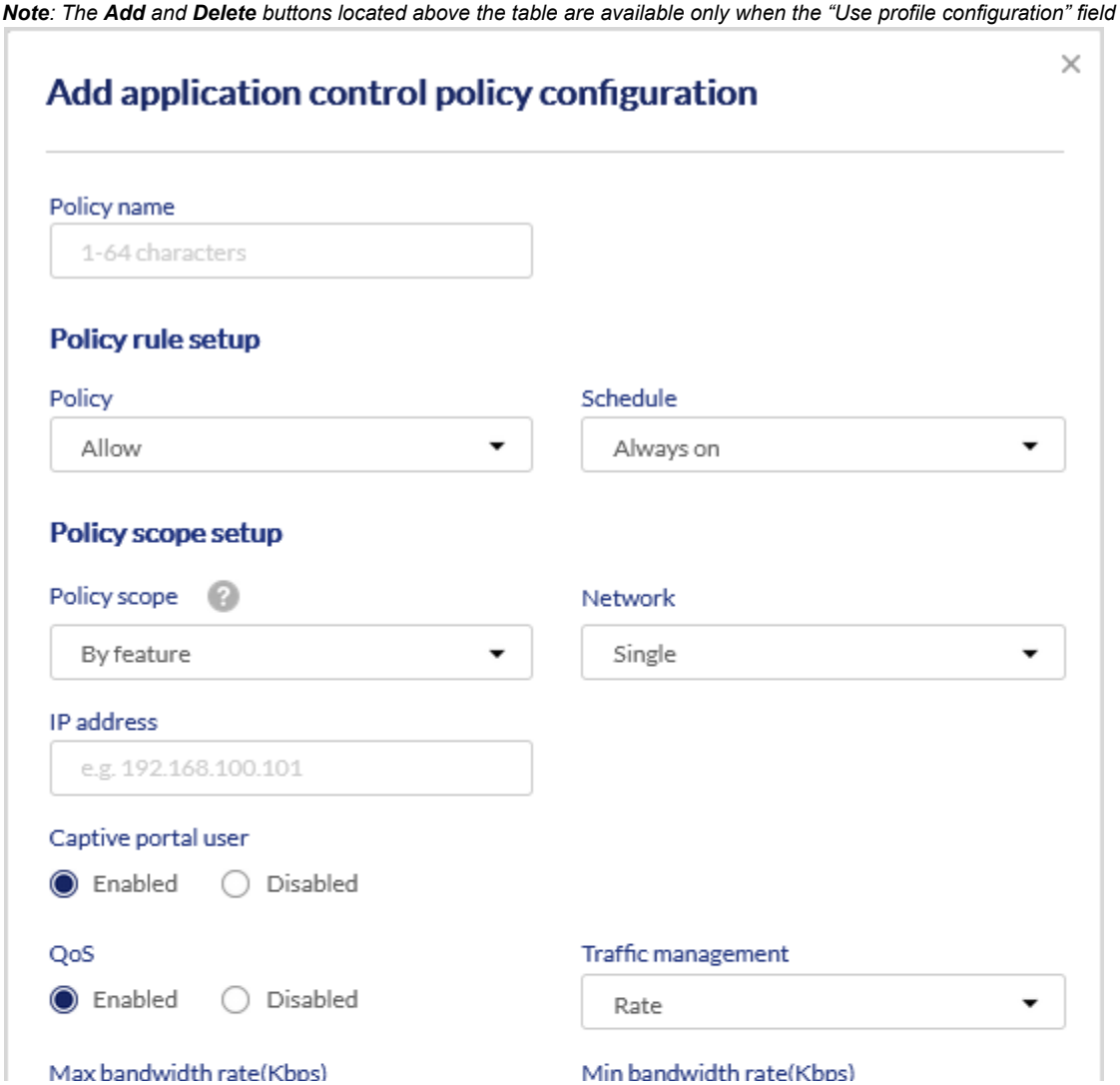


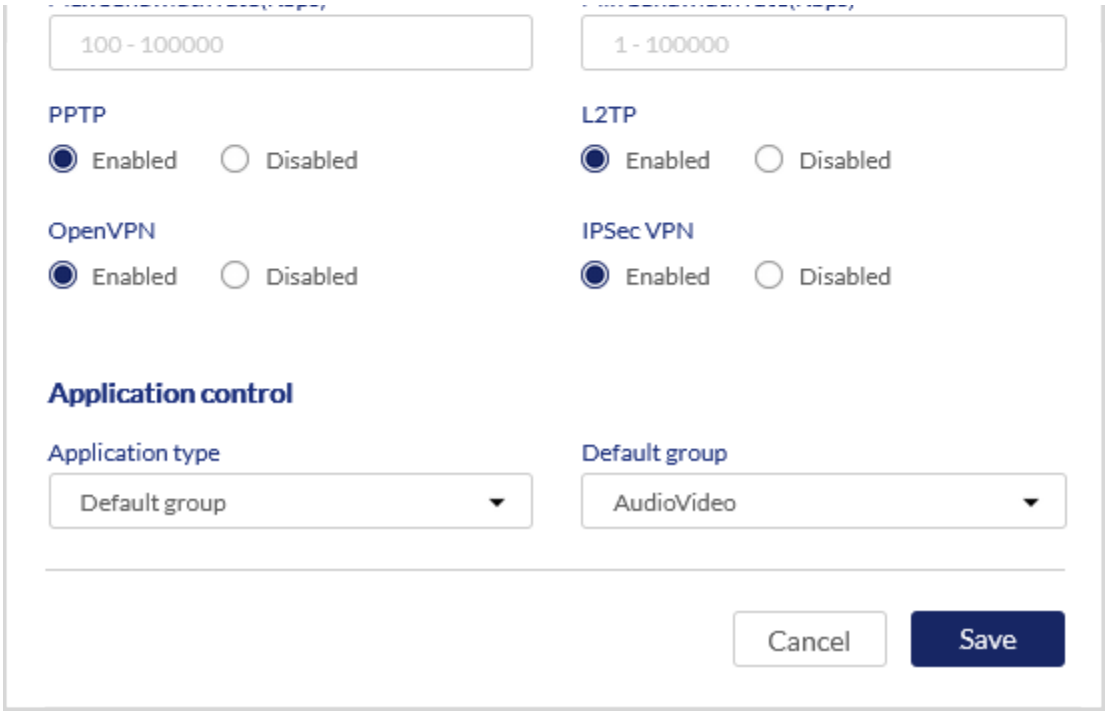
The fields displayed in the *Application control list* are as follows:

Field	Description
Name	It displays the name of the policy.
Policy	It displays the rule for the policy.
Schedule	It displays the schedule for your policy.
Scope	It displays the scope of the policy, i.e., whether the policy is *Global* or *By feature*.
Application	It displays the application type - Default group, Single APP, or Custom group.
Active	You can enable or disable the selected policy. ***Note**: You can edit this field only when the "Use profile configuration" is disabled.*
Actions	You can edit or delete the selected policy. ***Note**: This field is available only when the "Use profile configuration" is disabled.*

Click **Add** to add a new policy. This opens the *Add application control policy configuration* page. To delete multiple entries, select the checkboxes of the application control policies you want to delete, and click **Delete**.

***Note**: The **Add** and **Delete** buttons located above the table are available only when the "Use profile configuration" field is disabled.*





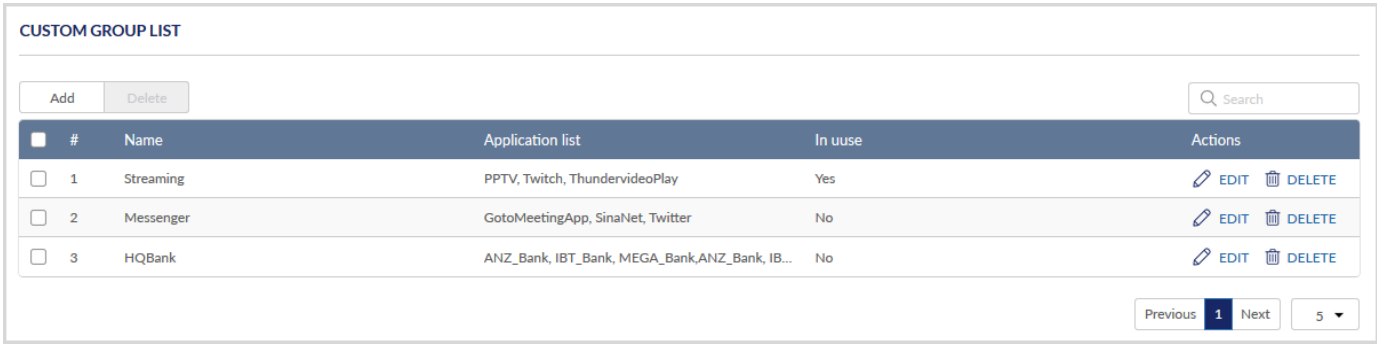
The fields available on the *Add application control policy configuration* page are as follows:

Field	Description
Policy Name	Enter a name to identify the policy.
Policy rule setup	
Policy	Select the policy rule. It could be either *allow* or *block*.
Schedule	It allows you to set a schedule when you want to apply the policy. To configure a new schedule, refer to the Schedule Policies section.
Policy scope setup	
Policy scope	Select either *Global* or *By feature* as the policy scope. The global policy affects all types of traffic matching the selected application(s). If the *By feature* is selected as the Policy type, the following fields will be available.
Network	Select any one of the following networks: • **Single**: If you select this option, enter the IP address. • **IP range**: If you select this option, enter the starting IP address and ending IP address. • **Interface**: If you select this option, select the interface from the drop-down list.
IP address	Enter the IP address. This field is available when the *Network* is **Single**.
Starting IP address	Enter the starting IP address of the IP range. This field is available when the *Network* is **IP range**.
Ending IP address	Enter the ending IP address of the IP range. This field is available when the *Network* is **IP range**.
Interface	Select the interface from the drop-down list. This field is available when the *Network* is **Inter face**.
Captive portal user	Enable or disable the Captive Portal option. Enabling this option allows all the Captive Portal clients to follow this policy.
QoS	Enable or disable the QoS option to select Bandwidth Rate or Priority for the traffic accessing through the selected application.
Traffic management	Select **Rate** or **Priority** for the traffic accessing through the selected application.

Priority	Specify the priority as *Low*, *Medium*, or *High*.
Max bandwidth rate (Kbps)	Enter the maximum bandwidth rate.
Min bandwidth rate (Kbps)	Enter the minimum bandwidth rate.
PPTP	Enable or disable the PPTP VPN. Enabling this option allows all the PPTP traffic to follow this policy.
L2TP	Enable or disable the L2TP VPN. Enabling this option allows all the L2TP traffic to follow this policy.
OpenVPN	Enable or disable the OpenVPN. Enabling this option allows all the OpenVPN traffic to follow this policy.
IPSec VPN	Enable or disable the IPSec VPN. Enabling this option allows all the IPSec traffic to follow this policy.
Application control	
Application type	Select the application type from the drop-down list. The options are Default group, Single application, and Custom group.
Category	This field is available when you select the option **Single application** as the *Application type* . Select the category of application from the drop-down list.
Application	This field is available when you select the option **Single application** as the *Application Type*. Select an application from the drop-down list available for each category.
Default group	This field is available when you select **Default group** as the *Application type*. Select a default group from the drop-down list.
Custom group	This field is available when you select the **Custom group** as the *Application Type*. Select the configured group from the drop-down list. If you want to create a new group, click the **Add custom group** button. It will redirect you to the *Add group configuration* page. For more details, refer to the Custom Group List for Application Control section.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

Custom Group List for Application Control

This section allows configuring groups and associating applications with them. It displays a list of configured groups along with the application list associated with them.

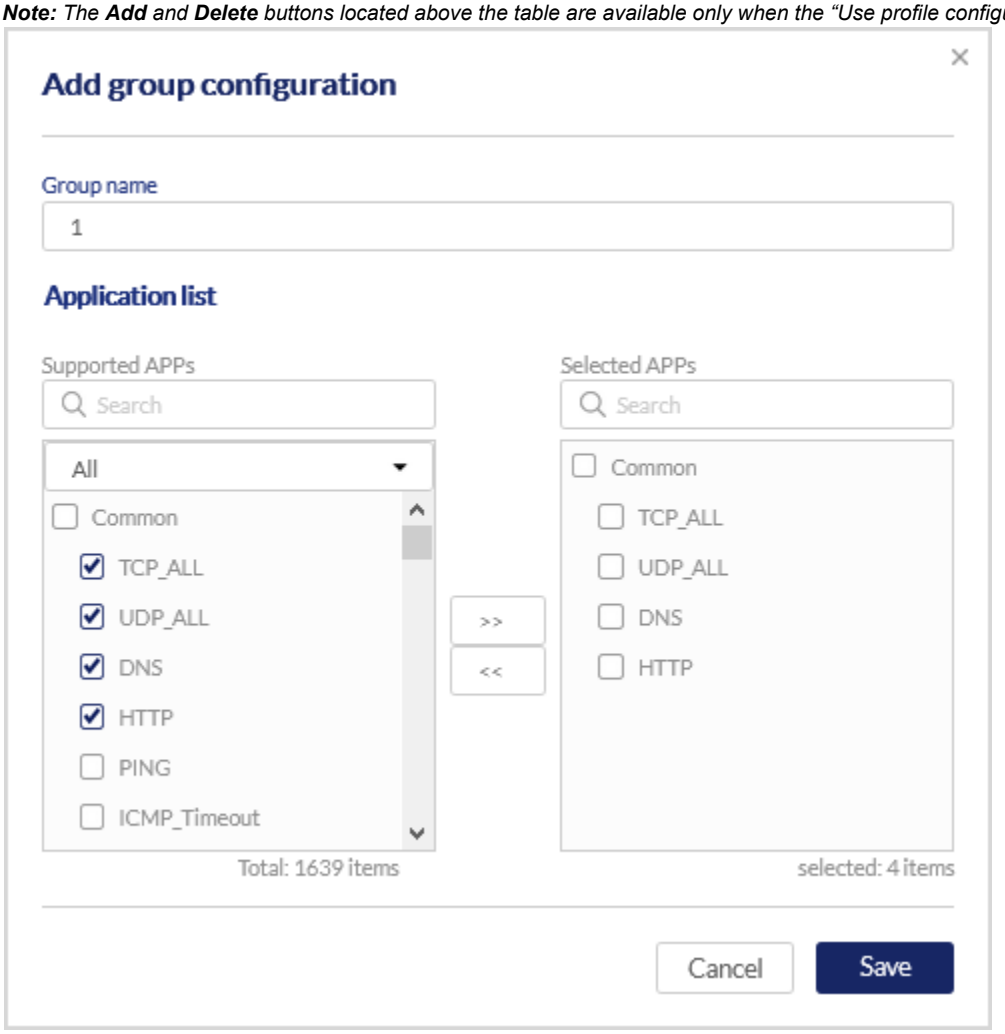


The fields displayed in the *Custom Group List* table are as follows:

Field	Description
Name	It displays the name of the group.
Application list	It displays the list of selected applications.
In use	It displays the status of the selected application, i.e., whether the group is in use or not.
Actions	You can edit or delete the selected group. ***Note**: This field is available only when the "Use Profile configuration" field is disabled.*

Click **Add** to configure a new group. This opens the *Add group configuration* page. To delete more than one group, select the corresponding checkboxes and click **Delete**.

Note: *The* ***Add*** *and* ***Delete*** *buttons located above the table are available only when the "Use profile configuration" field is disabled.*



The fields available on the *Add group configuration* page are as follows:

Field	Description
Group Name	Enter the name of the group. It can be of 1 to 64 characters.
Application list	It includes the following two boxes: • **Supported APPs**: It lists all the applications supported by the device. Select the checkbox of the corresponding application that you want to add to the group. Click the **">>"** button to add the application to the selected apps list. • **Selected APPs**: It lists all the applications to be added to the group. Select the checkbox of the corresponding application that you want to remove from the selected apps list. Click the **"<<"** button to remove the application from the selected apps list.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

Chapter 5 VPN

VPN provides a secure communication channel ("tunnel") between two gateway routers or a remote PC client. The Nuclias cloud gateway supports the following types of tunnels:

- Gateway-to-gateway VPN: To connect two or more routers to secure traffic between remote sites.

- Remote Client (client-to-gateway VPN tunnel): A remote client initiates a VPN tunnel as the IP address of the remote PC client is not known in advance. The gateway, in this case, acts as a responder.
- Remote Client behind a NAT router: The client has a dynamic IP address and is behind a NAT Router. The remote PC client at the NAT router initiates a VPN tunnel as the IP address of the remote NAT router is not known in advance. The gateway WAN port acts as a responder.
- PPTP server tunnel for PPTP client connections
- L2TP server tunnel for L2TP client connections
- OpenVPN server tunnel for OpenVPN client connections
- GRE tunnel

In this chapter, you will learn how to configure the VPN protocols supported by the cloud gateway.

This chapter covers the following topics:

Site to Site VPN

As the name suggests, 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 users select the networks based on their requirements. The site-to-site VPN page consists of the following two sections:

1. VPN Topology

VPN topology discusses how all the clients and networks are connected over the IPSec tunnel. The *Quick VPN* field allows users to build VPN tunnels between DBG-2000 devices deployed in the same Organization of the Nuclias cloud. There are the following three modes in the *Quick VPN* field:

- Disable (Manual)
- Site-to-Site
- Hub-and-Spoke

When you select Site-to-Site or Hub-and-Spoke mode in Quick VPN, each participating DBG-2000 device automatically performs the following functions:

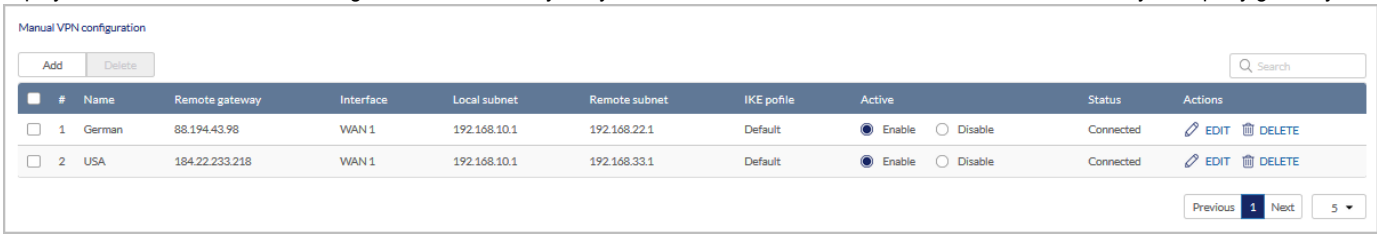
- Advertises its local subnets that are participating in the VPN
- Advertises its WAN IP addresses on the available WAN ports
- Applies the global VPN route table
- Applies the necessary configuration for establishing the VPN tunnel and traffic encryption

The net result is an automatic site-to-site VPN solution that is configured with a single click.

2. VPN Settings

Disable (Manual)

When you select *Disable (manual)* mode, DBG-2000 does not participate in the site-to-site or hub-and-spoke VPN, and the user will not be able to join the site-to-site or hub-and-spoke VPN connection automatically. Instead, the user can manually configure it in the *Manual VPN Configuration* section and build IPSec VPN tunnels. This mode is useful when you try to establish a tunnel between two DBG-2000 devices deployed in different Nuclias cloud organizations or when you try to establish a tunnel between DBG-2000 and/or with any third-party gateway.

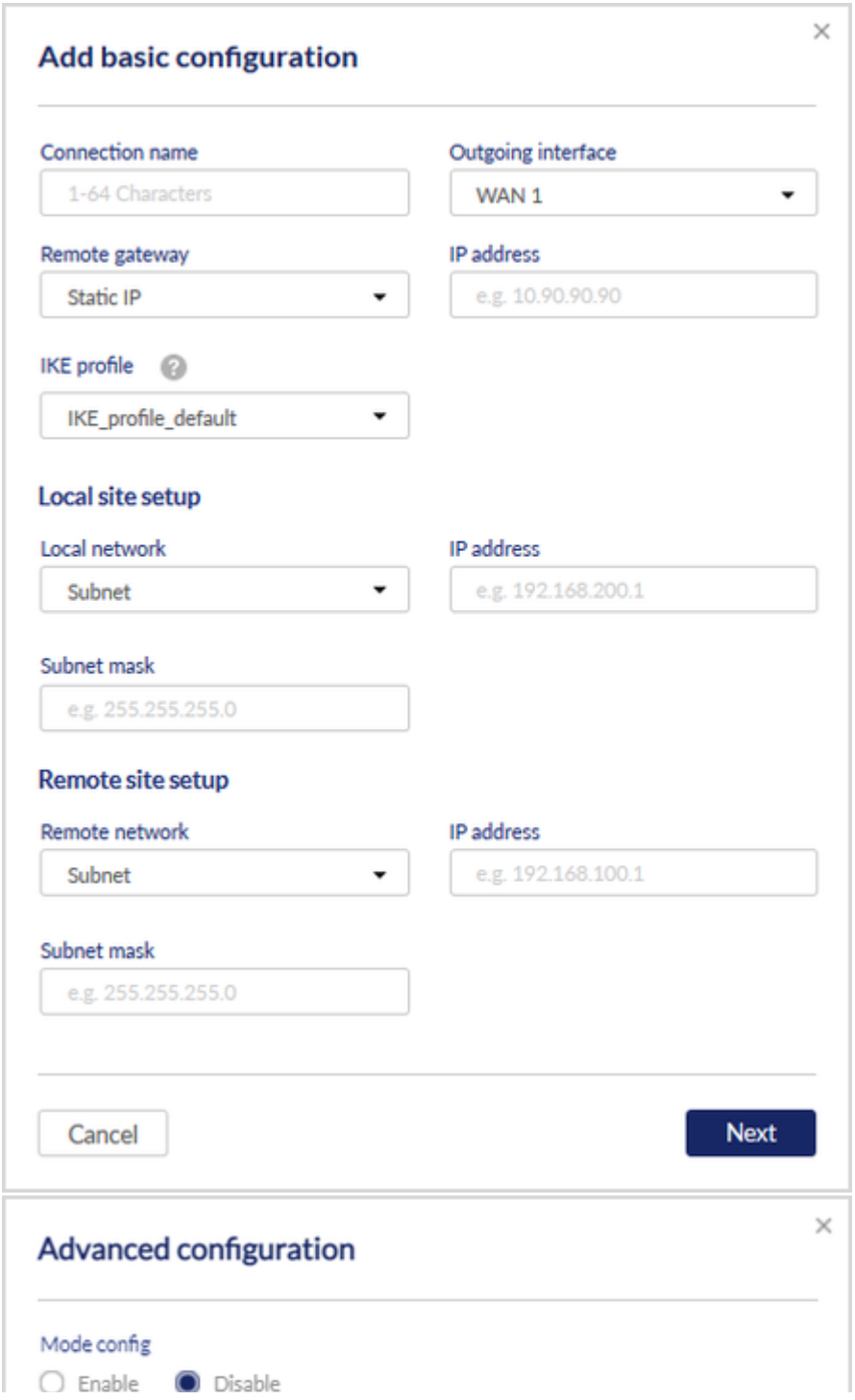


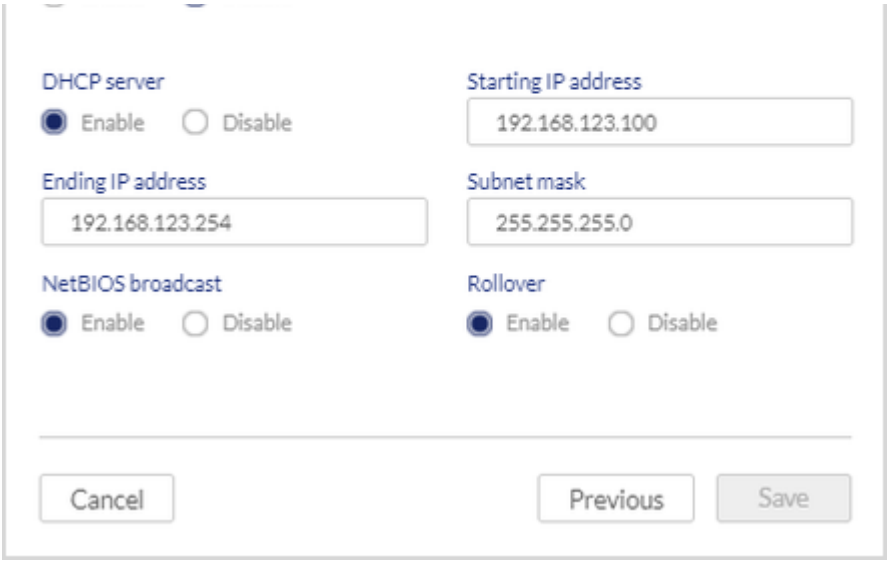
The fields available in the *Manual VPN configuration* table are as follows:

Field	Description
Name	It displays the name of the VPN.
Remote gateway	It displays the remote IP address to which the VPN tunnel is established.

Interface	It displays the interface being used for the VPN connection.
Local subnet	It displays the local subnet being used by this VPN connection.
Remote subnet	It displays the remote subnet being used by this VPN connection.
IKE profile	It displays the IKE profile selected for the configured VPN connection.
Active	You can enable or disable the connection.
Status	It displays if the VPN connection is connected or disconnected.
Actions	You can edit or delete the existing configuration.

Click **Add** to add a new VPN configuration. This opens the *Add basic configuration* page. To delete an entry or multiple entries, select the corresponding checkboxes, and click **Delete**.





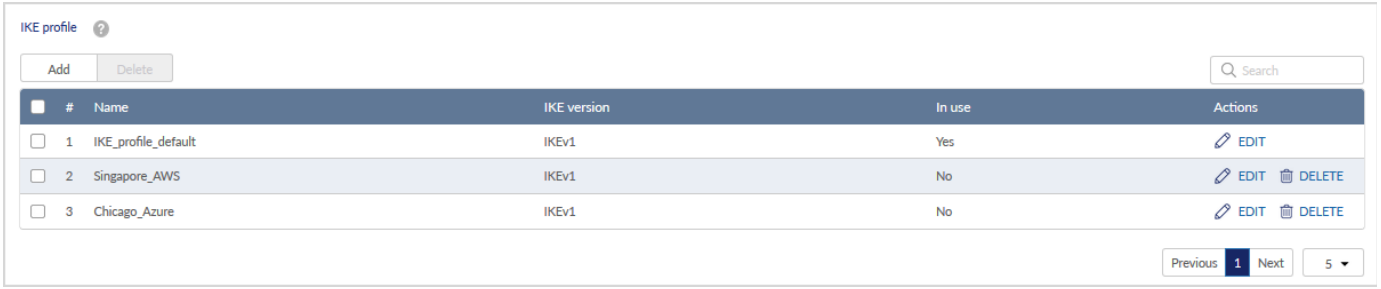
The fields available on the *Add basic configuration* and *Advanced configuration* pages are as follows:

Field	Description
Connection name	Enter a descriptive name for the VPN connection.
Outgoing interface	Specify the interface to be used for the outgoing data.
Remote gateway	Select the gateway you want to use for the connection. The options are *Static IP* and *FQDN*.
IP address	If you select *Static IP* as the remote gateway, enter the IP address.
Domain name	If you select *FQDN* as the remote gateway, enter the domain name.
IKE profile	Select one of the configured IKE profiles from the drop-down list.
Local site setup	
Local network	Select the network access type that you want to provide over the IPSec Tunnel. • **Any**: It specifies that the policy is for any traffic from the given local endpoint. • **Single IP**: It limits the policy to one host. Enter the IP address of the host that will be part of the VPN. • **Subnet**: It allows an entire subnet to connect to the VPN. Enter the network address and subnet mask in the provided fields.
IP address	Enter the IP address to connect to the VPN.
Subnet mask	Enter the subnet mask for the network address.
Remote site setup	
Remote network	Select the network access type that you want to provide over the IPSec Tunnel. • **Any**: It specifies that the policy is for any traffic from the given remote endpoint. • **Single IP**: It limits the policy to one host. Enter the IP address of the host that will be part of the VPN. • **Subnet**: It allows an entire subnet to connect to the VPN. Enter the network address and subnet mask in the provided fields.
IP address	Enter the IP address to connect to the VPN.
Subnet mask	Enter the subnet mask for the network address.
Next	Click **Next** to go to the *Advanced configuration* page.
Advanced configuration	
Mode config	

	Mode Config is similar to DHCP and is used to assign IP addresses to the remote VPN clients. You can enable or disable this feature.
Tunnel mode	Select either *Full tunnel* or *Split tunnel*. • Full Tunnel: It provides VPN client access to all the intranet and Internet services. • Split Tunnel: It provides VPN client access to all the intranet services.
Starting IP address	Enter the starting IP address of the assigned IP range to the VPN clients.
Ending IP address	Enter the ending IP address of the assigned IP range to the VPN clients.
Primary DNS	Enter the IP address of the primary DNS.
Secondary DNS (Optional)	Enter the IP address of the secondary DNS. It is an optional field.
DHCP Server	Enable it to allow VPN clients connected to your router over IPsec to receive an assigned IP using DHCP.
Starting IP address	Enter the first IP address of the DHCP IP range.
Ending IP address	Enter the last IP address of the DHCP IP range.
Subnet mask	Enter the subnet mask for the IP range.
NetBIOS broadcast	Enable it to allow NetBIOS broadcast to travel over the VPN tunnel.
Rollover	To enable a VPN rollover, you must have the *WAN Mode* set to **Rollover**.
Previous	Click **Previous** to go to the *Add basic configuration* page.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

IKE Profile

The IKE profile is the central configuration in IPSec that defines most of the IPSec parameters such as the protocol, algorithms, SA lifetime, and key management protocol. In addition, it contains information related to algorithms such as encryption, authentication, and DH group for Phase I and II negotiations. This section lists all the configured IKE profiles.



The fields displayed on the *IKE profile* table are as follows:

Field	Description
Name	It displays the name of the configured IKE profile.
IKE version	It displays the version of IKE that has been used.
In use	It indicates if the configured IKE profile is being used or not.
Actions	You can edit or delete the selected IKE profile. *Note: You can not delete the IKE default profile.*

Click **Add** to add a new entry to the list. This opens the *Add IKE profiles* page. To delete multiple entries, select the checkboxes of the IKE profiles you want to delete, and click **Delete**.

Profile name

1-64 Characters

IKE version

IKEv1 IKEv2

IKE phase-1 settings

Exchange mode

Main

Local identifer type

Local WAN IP

Remote identifer type

Remote WAN IP

DH group

Group 2 (1024 bit)

Encryption algorithm

Multiple select

Authentication algorithm

SHA-1

SA lifetime (sec.)

28800

Authentication method

Pre-shared key

Pre-shared key

••••••••

Dead peer detection

Enable Disable

Detection interval

10

Reconnect after failure

3

VPN tunnel backup

Enable Disable

Backup tunnel

Failure time to primary (seconds)

30

Extended authentication

Enable Disable

Extended authentication type

Local authentication

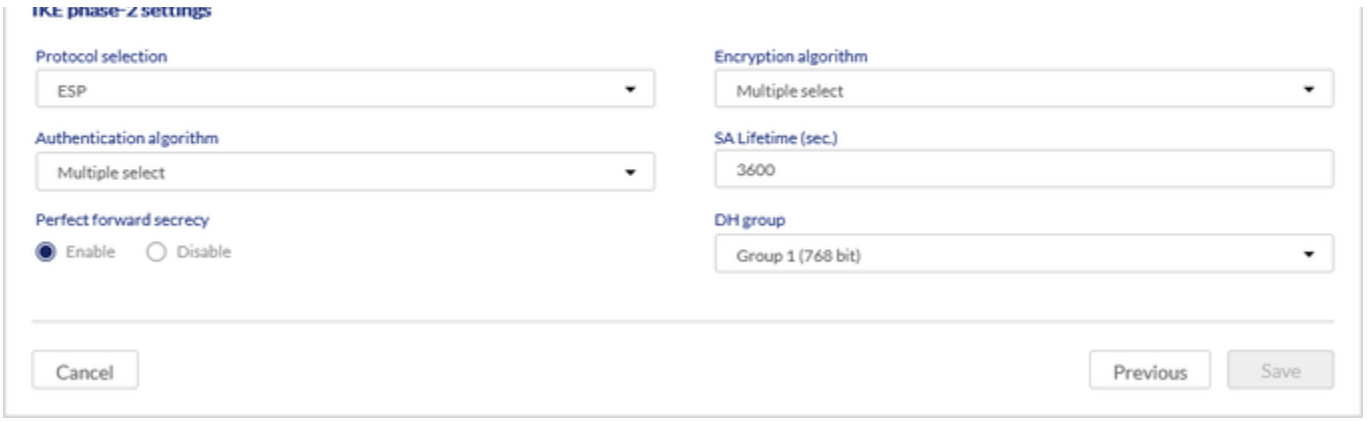
Local authentication

cp

Cancel

Next

Add IKE profile



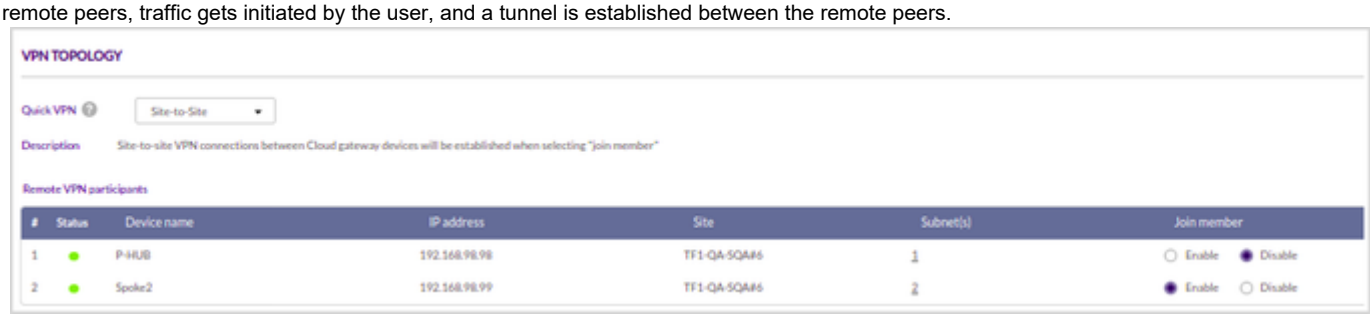
The fields available on the *Add IKE profiles* page 1 and page 2 are as follows:

Field	Description
Profile name	Enter a unique name for the IKE profile.
IKE version	Select the version of IKE.
IKE phase-1 settings	
Exchange mode	Select the exchange mode: *Main* or *Aggressive*.
Local identifier type	Select the local identifier type. The options are Local WAN IP, FQDN, and User-FQDN. If you select **User-FQDN**, enter the FQDN name in the *Local identifier* field. When you select **Local WAN IP** or **FQDN**, it uses the Local IP address of the WAN interface, and the FQDN name of the WAN configured on the Dynamic DNS page.
Remote identifier type	Select the remote identifier type. The options are Remote WAN IP, FQDN, and User-FQDN. If you select **FQDN** or **User-FQDN**, enter the FQDN name in the *Remote identifier* field. When you select **Remote WAN IP**, it uses the remote IP address entered in the VPN policy.
DH group	Select the DH (**Diffie-Hellman**) group. It defines the strength of the key used in the key exchange process.
Encryption algorithm	Select the encryption algorithm to be followed during key exchange. You may select multiple algorithms.
Authentication algorithm	Select the authentication algorithm from the drop-down list. You may select multiple algorithms.
SA lifetime (sec.)	It refers to the security association lifetime, and the range varies from 300 to 604800 seconds.
Authentication method	Select the authentication method. The options are the Pre-shared key and RSA-Signature (Certificate).
Pre-shared key	Enter the preshared key. This field is available only when you select the **Pre-shared key** as the *Authentication method*.
Certificate	Select the certificate to be used for authentication. This field is available only when you select **RSA-Signature (Certificate)** as the *Authentication method*.
Dead peer detection	You can enable or disable the *Dead peer detection* feature. If enabled, it allows you to detect if the remote peer is reachable or not. If it is not reachable, this feature will make the tunnel down.
Detection interval	Enter the interval at which you want to send peer detection packets to the peer to check its liveliness.
Reconnect after failure	This is the failure count, after which it is considered the other peer as down. Enter the failure count.
VPN tunnel backup	You can enable or disable the *VPN tunnel backup* feature.
Backup tunnel	

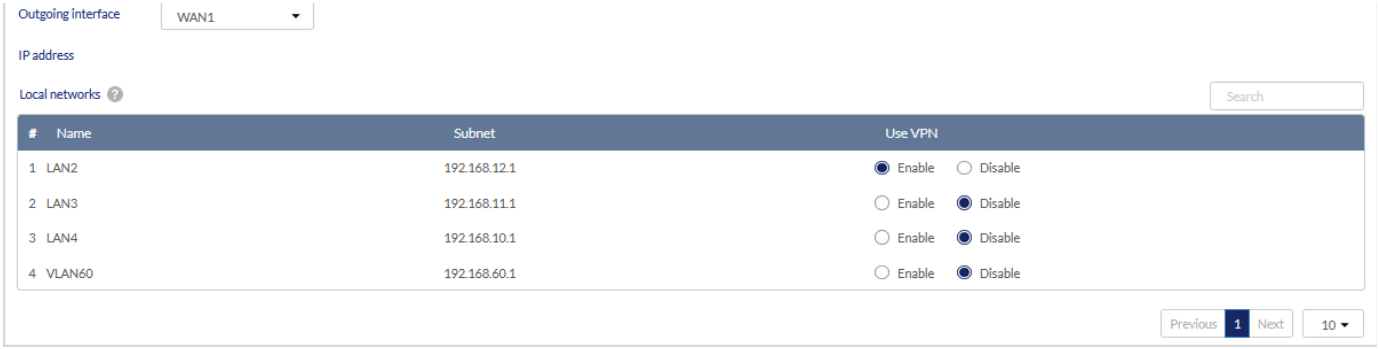
	If *VPN tunnel backup* is enabled, you can use the VPN backup of the selected profile if the primary tunnel is down. When the primary tunnel is up, the backup tunnel will be turned down.
Failure time to primary (seconds)	Specify the time after which the backup tunnel will be down.
Extended authentication	Enable or disable the extended authentication feature.
Extended authentication type	Select the authentication type that you want to use. The options are Local authentication, Authentication server, and IPSec host (Initiator).
Authentication server	Select any one of the external authentication servers from the drop-down, and select the respective server.
Username	Enter the user name. This field is available when you select the **IPSec host (Initiator)** as the *Extended authentication type*. The length of the user name may vary from 1 to 64 characters.
Password	Enter the password. This field is available when you select the **IPSec host (Initiator)** as the *Extended authentication type*. The length of the password may vary from 8 to 63 characters.
Local authentication	You may select one of the saved authentications on the local server. This field is available when you select **Local authentication** as the *Extended authentication type*.
Next	Click **Next** to go to the IKE Phase-2 page.
IKE phase-2 settings	
Protocol selection	Select the protocol for IKE phase-2.
Encryption algorithm	Select the encryption algorithm to be used. You may select multiple algorithms.
Authentication algorithm	Select the authentication algorithm from the drop-down list. You may select multiple algorithms.
SA Lifetime (sec.)	It refers to the security association lifetime, and the range varies from 300 to 604800 seconds.
Perfect forward secrecy	If enabled, it does not allow the same key to be generated, forcing the user to use a new DH key exchange.
DH group	Select the DH group.
Previous	Click **Previous** to go to the *IKE Phase-1 Settings* page.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to previous settings.

Site-to-Site

The site-to-site VPN establishes the Gateway-to-Gateway IPsec tunnel with other DBG-2000 devices registered in the same or different sites of the same organization. Once a user selects the quick VPN type as Site-to-Site, all other DBG-2000 participants with the same quick VPN mode are listed. To establish a tunnel with a particular remote device, enable the *Join member* field. 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.

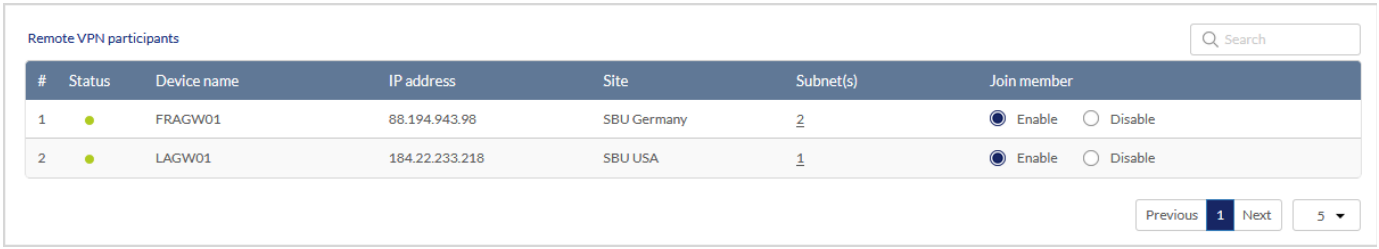


In the *Local networks* section, if you have multiple subnets, you can specify which one subnet participates in the VPN, i.e., traffic from the enabled subnet will be encrypted by the IPSec VPN. All local subnets must be unique within the VPN topology.



The fields displayed in the *Local networks* table are as follows:

Field	Description
Outgoing interface	It is the WAN interface on which the tunnel will be established.
IP address	It displays the current WAN IP address of the device.
Name	It displays the LAN/VLAN interface's name of the local subnet.
Subnet	It displays the subnet IP address.
Use VPN	Enable the subnet if you want to encrypt its traffic by IPSec VPN.



The *Remote VPN participants* table lists all the remote VPNs and displays the following fields:

Field	Description
Status	It indicates the status of the remote device, whether it is online or offline. The green color indicates that it is online, and the red color indicates that it is offline.
Device name	It displays the name of the remote device with which the VPN connection is established.
IP address	It displays the WAN IP address of the remote gateway devices.
Site	It displays the site of the remote gateway devices.
Subnet(s)	It displays the subnets of the remote gateway devices. It is a hyperlink; if you hover your mouse over it, you can view the subnet and the subnet mask of the remote device.
Join member	If this option is enabled, the tunnel configuration needed to establish a tunnel is pushed to the remote peers.

Hub-and-Spoke

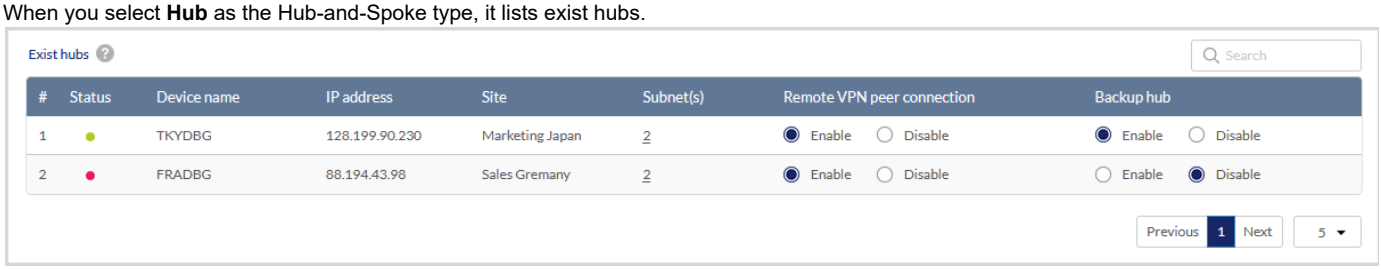
The Site-and-Site VPN connections between DBG-2000 devices will automatically be established between all Site-and-Site enabled peers in the same organization. However, this is often undesirable because such connections may establish unnecessary IPSec tunnels between remote sites and create performance-degrading networking overhead. Therefore, it is best to configure Hub and spoke in such cases, which designates one DBG-2000 device as the **Hub** and all remote sites as the **Spoke**. In addition, the Hub-and-Spoke mode can be useful in organizations where several auxiliary sites require a connection to the HQ.

There are two options for configuring the DBG-2000 in the Hub-and-Spoke mode:

1. **Hub (Mesh)**: The DBG-2000 device will establish VPN tunnels to all remote VPN peers that are also configured in this mode. If another DBG-2000 in the same organization is configured as a hub, it can be added as an **Exist hub**. If a DBG-2000 device is selected as a

HUB, it will be advertised on all the remaining devices' SITE-SITE VPN page if the *Quick VPN type* is selected as Hub-and-Spoke. If any other HUB devices are existing in the organization, they will be displayed as Exist Hubs. Users can use these exist HUBs to form a site-site tunnel by enabling *Remote VPN Peer Connection,* or they can use it as a backup hub by enabling the *Backup Hub* field.

When you select **Hub** as the Hub-and-Spoke type, it lists exist hubs.



The fields displayed in the *Exist hubs* table are as follows:

Field	Description
Status	It displays the current status of the remote hub devices, whether it is online or offline. The green color indicates that it is online, and the red color indicates that it is offline.
Device name	It displays the name of the remote devices that have the Quick VPN type as **Hub-and-Spoke** and the role as **HUB**.
IP address	It displays the WAN IP address of the remote gateway devices.
Site	It displays the site name of the “Exist Hub” devices.
Subnet (s)	It displays the subnet of the remote devices. It is a hyperlink; if you hover your mouse over it, you can view the subnet and the subnet mask of the remote device.
Remote VPN peer connection	You can enable or disable a site-to-site tunnel to the existing hub.
Backup hub	You can select the other hub as the backup hub for the current hub.

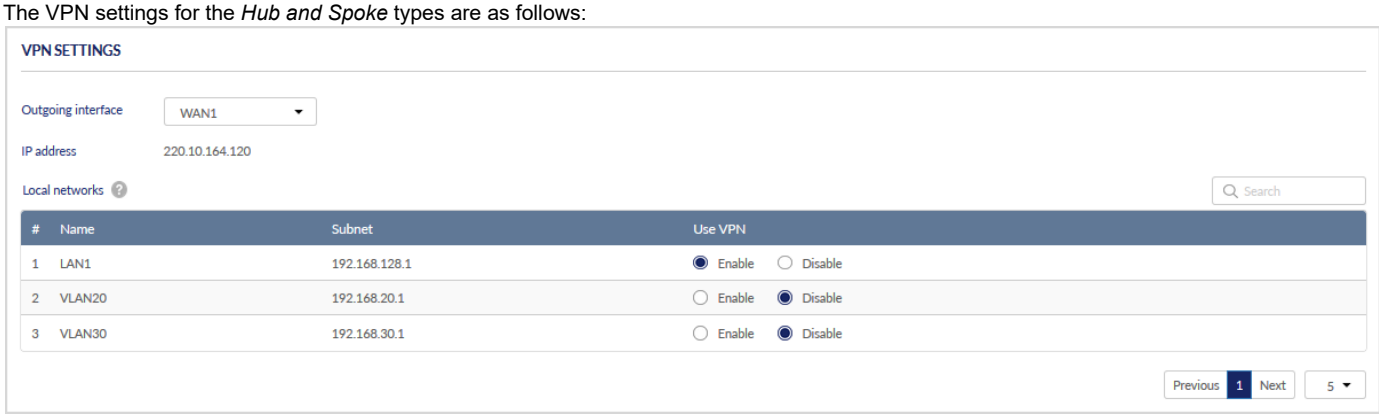
2. **Spoke:** The DBG-2000 device (Spoke) establishes direct tunnels only to the specified remote DBG-2000 devices as hubs. When a DBG-2000 device is configured as a Spoke, you can configure multiple VPN hubs for that DBG-2000. In this configuration, the Spoke DBG-2000 sends all site-to-site traffic to its configured VPN hubs. The spokes do not exchange data directly with one another.

If you select the *Hub-and-Spoke Type* as **Spoke**, it displays a list of all the Exist hubs under the *VPN Topology* section. In addition, it lists the Exist hub devices available with an 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.

The fields displayed in the *Exist hubs* table are as follows:

Field	Description
Status	It displays the status of the available exist hubs. If the hub is online, a green dot is displayed, and if the hub is offline, a red dot is displayed.
Device name	It displays the name of the hub device with which we want to establish the tunnel.
IP address	It displays the WAN IP address of the hub with which the tunnel will be established.
Site	It refers to the site name configured to identify the hub device.
Subnet(s)	It displays the number of local/private networks shared by the remote devices. It is a hyperlink; if you hover your mouse over it, you can view the subnet and the subnet mask of the remote device.
Primary Hub	Enable this option to select it as the primary hub for the configuring device.

The VPN settings for the *Hub and Spoke* types are as follows:



The fields available on the *VPN settings* section for the Hub and Spoke VPN are as follows:

Field	Description
Outgoing interface	It is the WAN interface on which the user wants to establish a tunnel.
IP address	It displays the current WAN IP address of the device.
Local networks	
Name	It displays the LAN/VLAN interface name of the local subnet.
Subnet	It displays the subnet of the above interface.
Use VPN	You can **enable** or **disable** the Use VPN feature. When it is enabled, subnets get selected for the local traffic selectors for the VPN policy.

PPTP/L2TP

Server Mode

The Nuclias cloud gateway can establish a PPTP/L2TP VPN. Once enabled, a PPTP/L2TP server is available on the gateway for the LAN and WAN PPTP/L2TP client users to access, i.e., PPTP/L2TP clients can reach the gateway's PPTP/L2TP server. Furthermore, once authenticated by the PPTP/L2TP server (the tunnel endpoint), PPTP/L2TP clients can access the LAN network managed by the gateway.

The range of IP addresses allocated to PPTP/L2TP clients should not coincide with the LAN subnet. Also, the PPTP/L2TP server will default to local PPTP/L2TP user authentication but can be configured to employ an external RADIUS authentication server should one be configured.

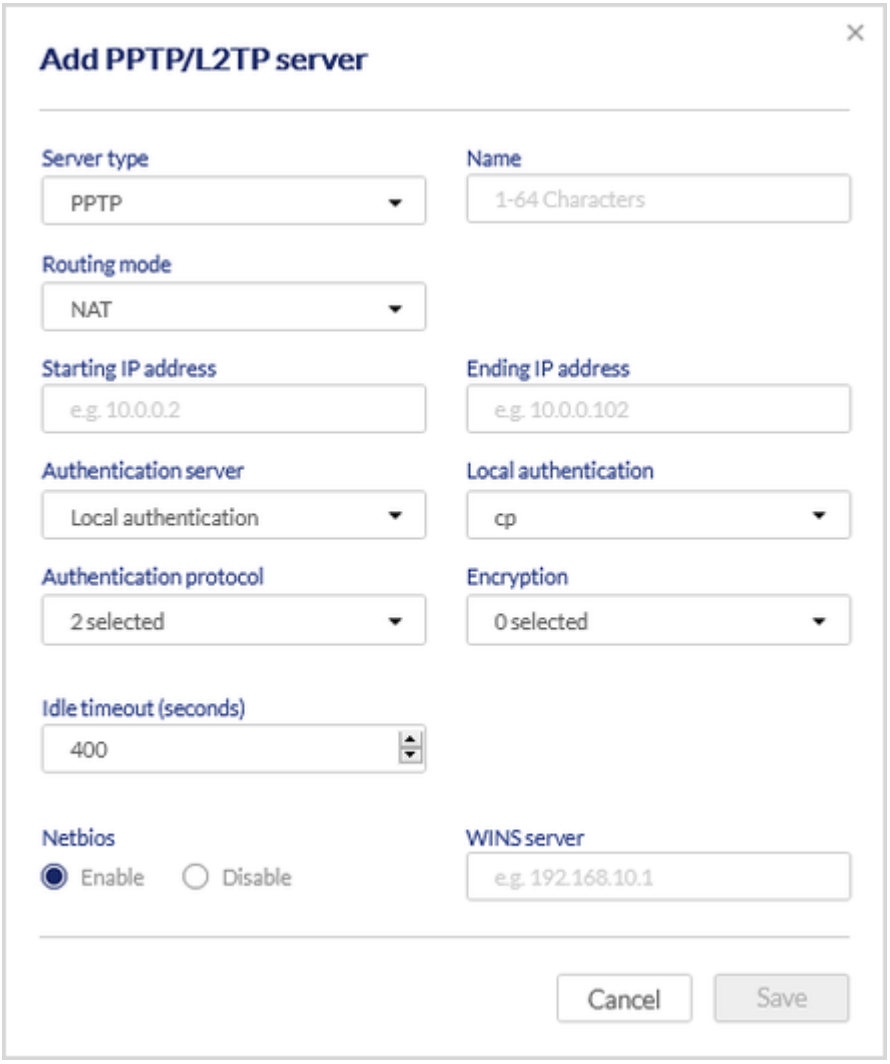
The fields available in the *Server mode* table are as follows:

Field	Description
Name	It displays the name of the PPTP/L2TP server.
Server type	It displays the server type, i.e., either PPTP or L2TP.
L2TP Over IPsec	It displays if the *L2TP over IPsec* is enabled or disabled.
IP address	It displays the IP address range allocated to PPTP/L2TP clients.
Active	You can enable or disable the server.

Actions	You can edit or delete the configured PPTP/L2TP server.

Click **Add** to add a new entry to the list. This opens the *Add PPTP/L2TP server* page. To delete an entry or multiple entries, select the corresponding checkboxes, and click **Delete**.

Adding a PPTP Server

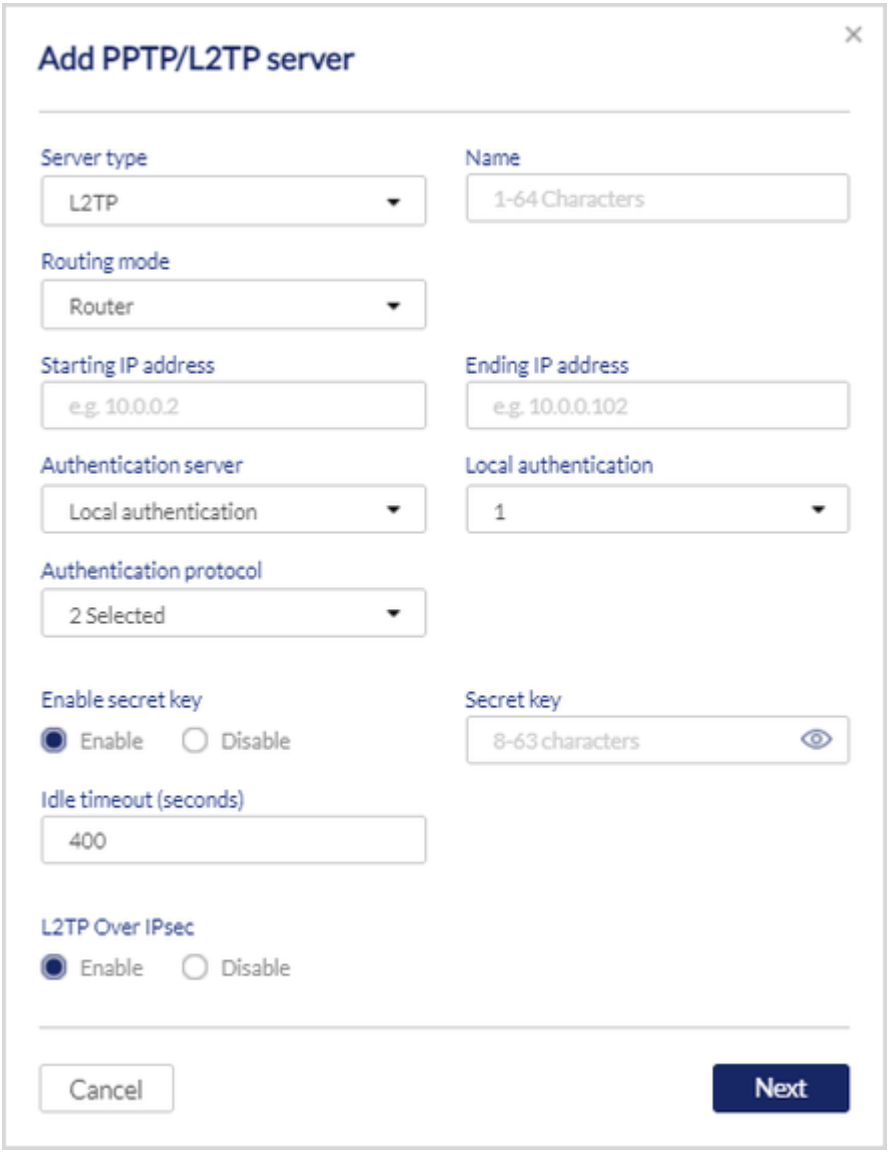


The fields available on the *Add PPTP/L2TP server* page for the **PPTP server** type are as follows:

Field	Description
PPTP Server	
Server Type	Select **PPTP** as the server type.
Name	Enter the name of the PPTP server.
Routing mode	Select the routing mode, either *NAT* or *Router*.
Starting IP address	Enter the starting IP address of the IP address range to assign to your PPTP clients.
Ending IP address	Enter the ending IP address of the IP address range to assign to your PPTP clients.
Authentication Server	Select any one of the available authentication servers. The options are *Local authentication*, *RADIUS*, and *None* authentication.
Radius Server	Select the RADIUS server. It is available when you select **Radius** as the *Authentication Server*.
Local authentication	Select one of the saved authentications on the local server.

Authentication protocol	Select one or multiple authentication types from the drop-down list (*All*/*PAP*/*CHAP*/*MS-CHAP*/*MSCHAPv2*).
Encryption	This field is available only when **MS-CHAP** or **MS-CHAPv2** is selected as the *Authentication protocol*. • **All**: Select the checkbox to select all the encryption options. • **Mppe 40 Bit**: Select the checkbox to enable Mppe 40 bit encryption. • **Mppe 128 Bit**: Select the checkbox to enable Mppe 128 bit encryption. • **Stateful Mppe**: Select the checkbox to enable Stateful Mppe encryption. This mode of Mppe encryption is less secure and can be used for compatibility.
Idle timeout (seconds)	Enter the amount of time in seconds, after which the connection will disconnect when idle.
Netbios	Enable it to allow NetBIOS broadcasts to travel over the VPN tunnel.
WINS server	Enter the WINS server address for Netbios. This field is available when you enable Netbios.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

Adding an L2TP Server

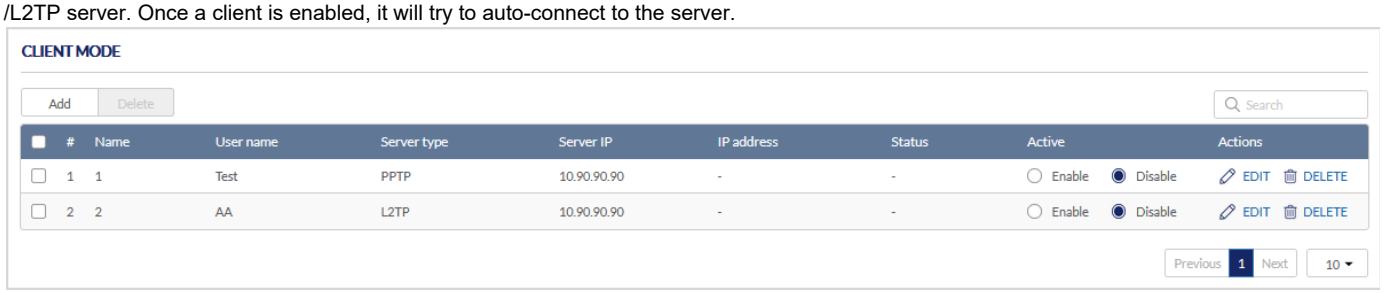


The fields available on the *Add PPTP/L2TP server* page for the **L2TP server** type are as follows:

Field	Description
L2TP Server	
Server Type	Select **L2TP** as the server type.
Name	Enter the name of the L2TP server.
Routing mode	Select the routing mode, either *NAT* or *Router*.
Starting IP address	Enter the starting IP address of the IP address range to assign to your L2TP clients.
Ending IP address	Enter the ending IP address of the IP address range to assign to your L2TP clients.
Authentication server	Select the authentication server. The options are *Local authentication*, *RADIUS*, and *None* authentication.
Local authentication	Select one of the saved authentications on the local server. This field is available when you select **Local authentication** as the authentication server.
Radius server	Select the Radius server. This field is available when you select **Radius** as the authentication server.
Authentication protocol	Select any authentication types from the drop-down menu (*All*/*PAP*/*CHAP*/*MS-CHAP*/*MSCHAPv2*).
Encryption	Enable it to add a secret key.
Enable Secret key	If the *Encryption* field is enabled, enter the secret key.
Idle timeout (seconds)	Enter the amount of time in seconds that the connection will disconnect when idle.
L2TP over IPsec	When the *L2TP over IPsec* configuration is enabled, the IPsec tunnel initiation starts automatically. Still, the establishment of the tunnel depends on the configuration at the client and the server-side and the response from the server. Click **Next** to configure the *IKE profile* for IPsec. For details, refer to https://dlink-dbg.atlassian.net/wiki/spaces/CGD/pages/2687700/Site+to+Site+VPN#IKE-Profile.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

Client Mode

The Nuclias cloud gateway can configure the PPTP/L2TP VPN Client. Using this client, we can access a remote network that is local to the PPTP /L2TP server. Once a client is enabled, it will try to auto-connect to the server.



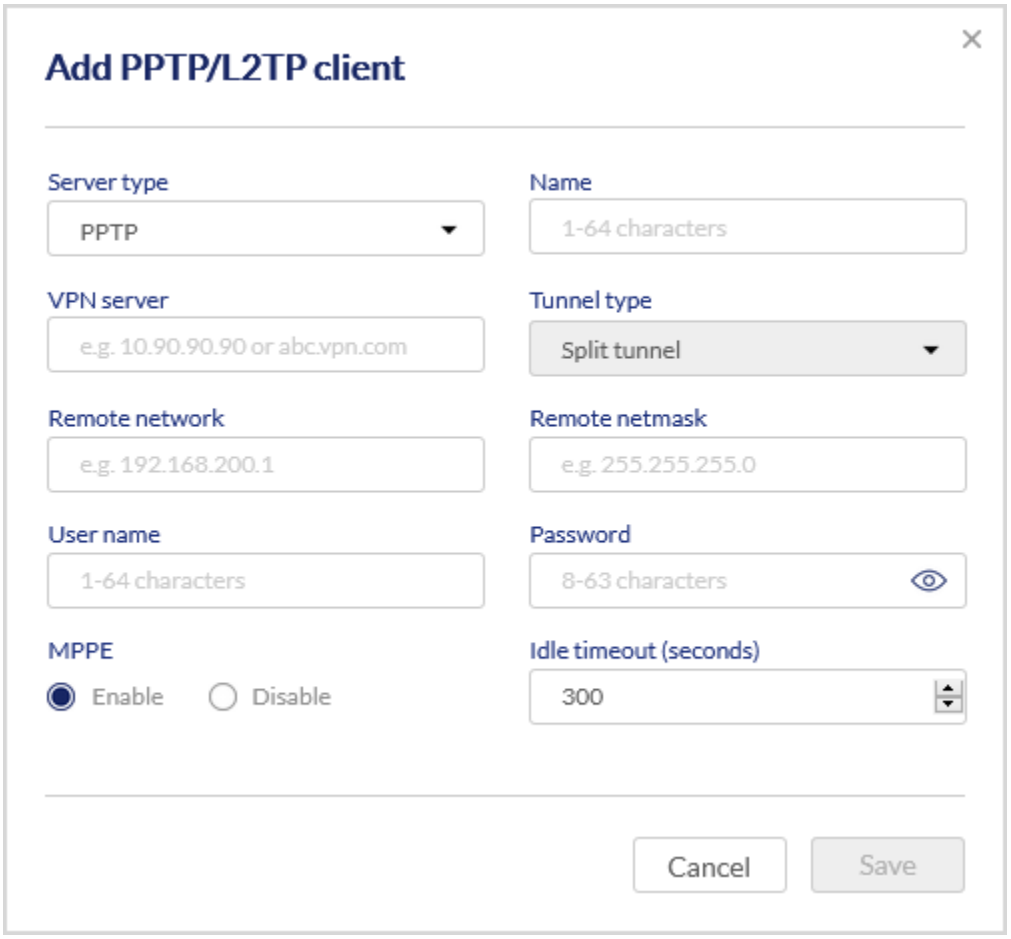
The fields displayed in the *Client Mode* table are as follows:

Field	Description
Name	It displays the name of the client.
User name	It displays the user name which is being used.
Server type	It displays the server to which the client is connected.
Server IP	It displays the server IP address.

IP address	It displays the IP address of the client.
Status	It displays the status of the client, whether it is connected or not.
Active	You can enable or disable the client.
Actions	You can edit or delete the selected client from the list.

Click **Add** to add a new entry to the list. This opens the *Add PPTP/L2TP client* page. To delete an entry or multiple entries, select the corresponding checkboxes, and click **Delete**.

Adding a PPTP Client

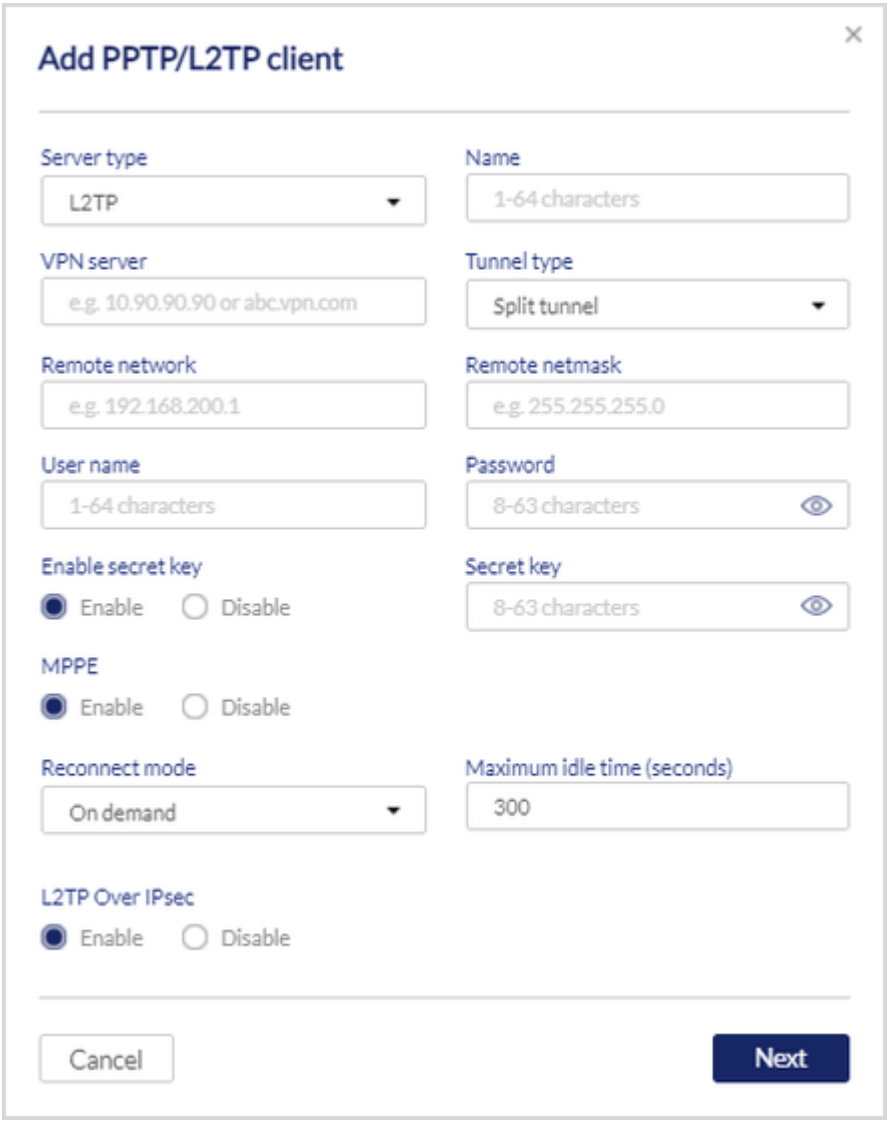


The fields available on the *Add PPTP/L2TP client* page are as follows:

Field	Description
Server type	Select the server type as **PPTP**.
Name	Enter the name.
VPN server	Enter the IP address or domain name of the PPTP server you want to connect to.
Tunnel type	Select the tunnel type. • **Full tunnel**: If this is selected, it will access the Internet and the LAN host connected to the server device through the PPTP server once the connection is established, • **Split tunnel**: If this is selected, it will access only the selected remote network.
Remote network	Enter the remote network address. This address is local for the PPTP Server.
Remote netmask	Enter the remote network subnet mask.
User name	Enter the user name to connect to the server.

Password	Enter the password to connect to the server.
MPPE	Enable or disable Microsoft Point-to-Point Encryption (MPPE).
Idle timeout (seconds)	Enter the amount of time (in seconds) that you will disconnect from the PPTP server when idle.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

Adding an L2TP Client



The fields available on the *Add PPTP/L2TP client* page are as follows:

Field	Description
Server type	Select the server type as **L2TP**.
Name	Enter the name.
VPN server	Enter the IP address of the L2TP server you want to connect to.
Tunnel type	Select the tunnel type. • **Full tunnel**: If this is selected, it will access the Internet and the LAN host connected to the server device through the L2TP server once the connection is established.

	• **Split tunnel**: If this is selected, it will access only the selected remote network.
Remote network	Enter the remote network address. This address is local for the L2TP Server.
Remote netmask	Enter the remote network subnet mask.
User name	Enter the user name to connect to the VPN server.
Password	Enter the password to connect to the VPN server.
Enable secret key	You may enable or disable the Secret key.
Secret key	If the Secret key is enabled, enter the secret key.
MPPE	Enable or disable Microsoft Point-to-Point Encryption (MPPE).
Reconnect mode	Select either *Always On* or *On Demand*.
Maximum idle time (seconds)	Enter the idle time in seconds before the gateway disconnects from the L2TP server. This field is available only when *Reconnect mode* is **On Demand**.
L2TP over IPsec	You may enable or disable this feature. If enabled, it will redirect you to the IPsec settings. Click **Next** to configure the *IKE profile* for IPsec. For details, refer to https://dlink-dbg.atlassian.net/wiki/spaces/CGD/pages/2687700/Site+to+Site+VPN#IKE-Profile.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

OpenVPN

The Nuclias cloud gateway provides the OmniSSL feature, a customized OpenVPN, similar to the SSL VPN connectivity. OmniSSL provides an executable configuration file via a portal page (<*https://<Device WAN IP>/omnissl*>) that facilitates the client installation from the device and is an enhancement to the existing OpenVPN. In addition, this VPN tool can be used via mobile devices, thereby eliminating browser and Java dependencies typical to the SSL VPN solutions.

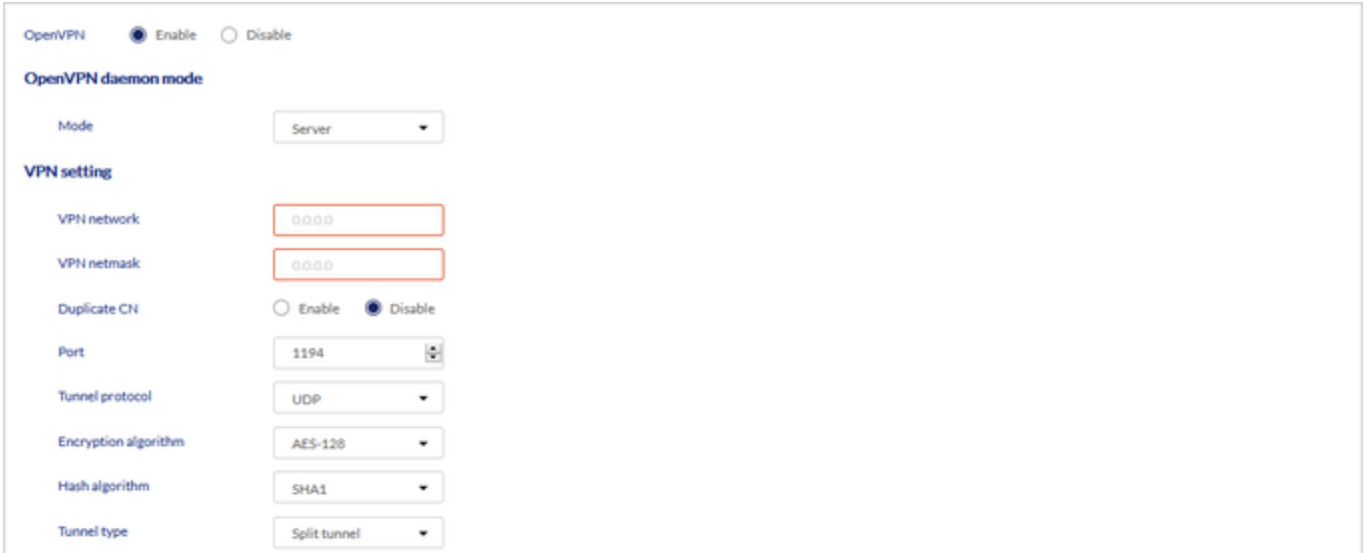
OpenVPN allows peers to authenticate each other using certificates or username/password. When used in a multi-client-server configuration, it allows the server to release an authentication certificate for every client, using signature and Certificate authority. An OpenVPN can be established through this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

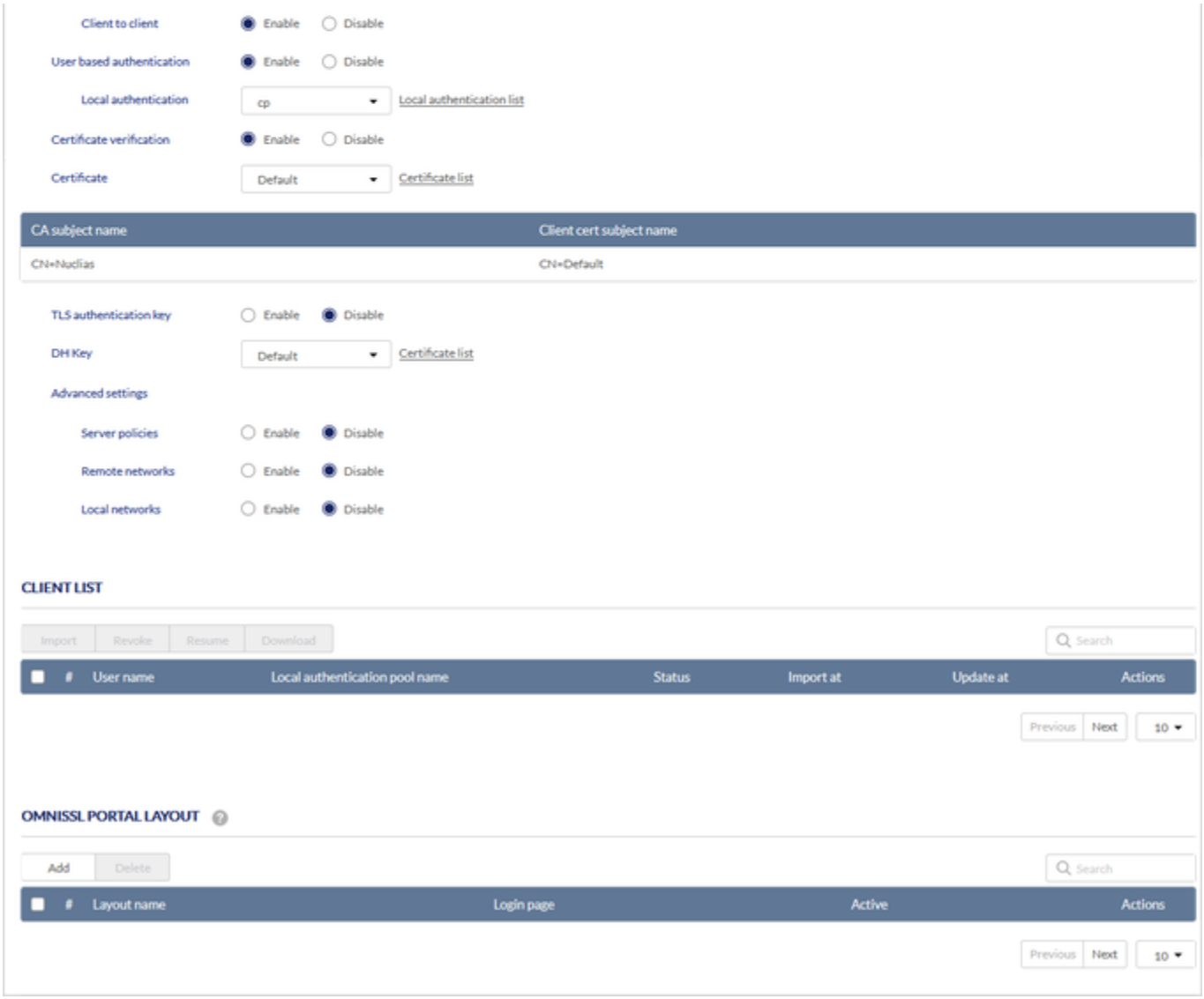
In access server-client mode, the user downloads the auto-login profile from the OpenVPN Access Server and uploads the same to connect. You can select the following modes:

- Server mode
- Client mode
- Access server-client mode

Server mode

In this section, you will learn about the OpenVPN configuration in the *Server* mode.





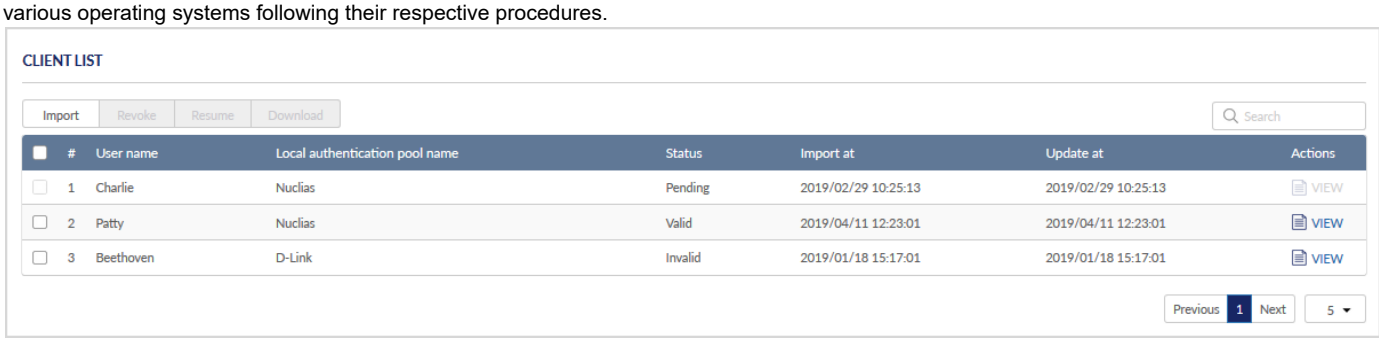
The fields available on this page are as follows:

Field	Description
OpenVPN	You can enable or disable the OpenVPN feature.
OpenVPN daemon mode	
Mode	Select **Server**.
VPN setting	
VPN network	Enter the IP network for the VPN.
VPN netmask	Enter the netmask.
Duplicate CN	Enable it to allow the user to use the same certification to connect for multiple clients. User-based authentication is also required for this feature, and multiple clients require to have their respective user names and passwords.
Port	Enter the port number on which the OpenVPN server runs. The default port is 1194.
Tunnel protocol	Select either *TCP* or *UDP* to communicate with the remote host.
Encryption algorithm	Select the encryption algorithm from the drop-down menu. The options are *AES-128*, *BF-CBC*, *AES-192*, and *AES-256*.
Hash algorithm	

	Select the hash algorithm from the drop-down menu. The options are *SHA1*, *SHA256*, and *SHA512*.
Tunnel type	Select either **Full Tunnel** or **Split Tunnel**. Full Tunnel mode sends all the traffic from the client across the VPN tunnel to the gateway. Split Tunnel mode only sends traffic to the private LAN based on pre-specified client routes. If you select **Split Tunnel**, refer to Local Networks to create local networks.
Client to client	Enable this field to allow OpenVPN clients to communicate with each other in the split tunnel case. By default, it is disabled.
User-based authentication	This option provides an additional authentication method. You can enable this field to select an authentication server.
Local authentication	Select a configured local authentications saved on the local server. To add a new local authentication server, click the *Local authentication list* link. For more details, refer to the Local authentication list section.
Certificate verification	Enable or disable certificate verification. This method does not require the client certificate; the client authenticates using the username/password only. It is enabled by default.
Certificate	Select the profile which has a list of certificates uploaded for the configured mode server /client.
TLS authentication key	Enabling this adds TLS authentication, which adds a layer of authentication. It can be checked only when the TLS key is uploaded. It is disabled by default.
TLS key	Select the type of TLS certificate name.
DH key	Select the DH key from the drop-down list.
Advanced settings	
Server policies	Enable or disable the *Server Policies* feature; if enabled, configure the Server policies under the Server Policies section.
Remote networks	Enable or disable the *Remote networks* feature; if enabled, configure this feature in the Remote networks section.
Local networks	Enable or disable the *Local networks* feature; if enabled, configure this feature in the Local networks section. This section is available when you select **Split Tunnel** as the *Tunnel type*.

Client List

It allows the user to generate the client's configuration. Furthermore, OmniSSL is an adaptable feature as it supports and gets installed on various operating systems following their respective procedures.

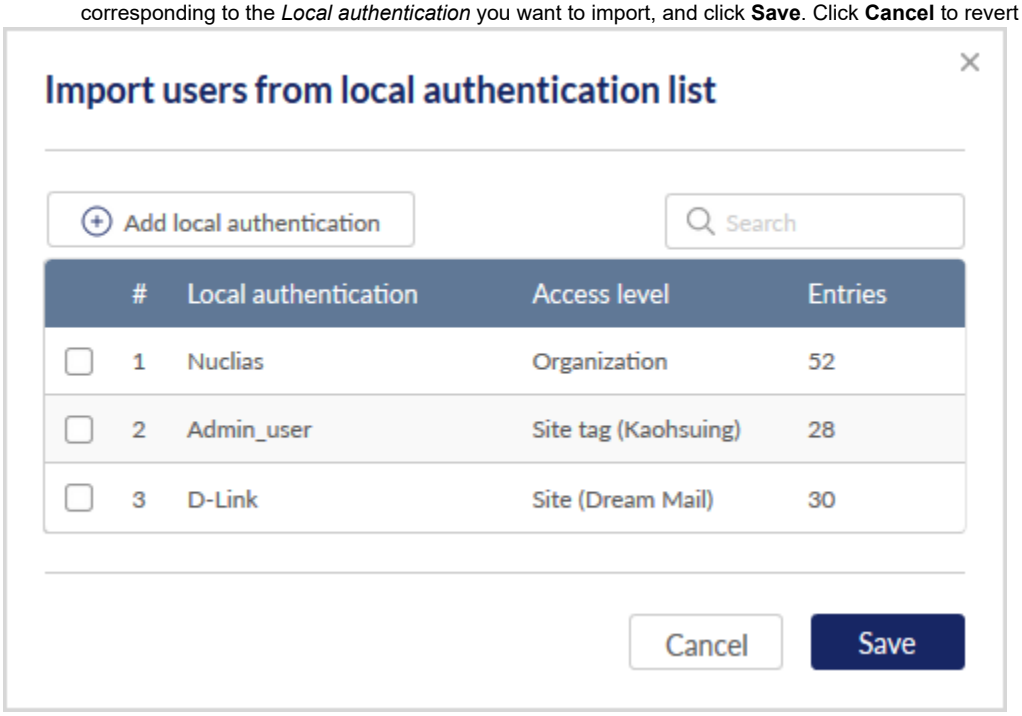


The fields available on the *Client list* table are as follows:

Field	Description
User name	It displays the OmniSSL client name.
Local authentication pool name	It displays the name of the local authentication pool where the clients belong.
Status	It displays the status of certificates.
Import at	It displays the date and time when the user's certificates were first imported.
Update at	It displays the date and time when the user's certificates were last updated.

Actions	It allows you to view the client details. ***Note:*** *You cannot view the client details if the status is Pending.*
Import	Click **Import** to import the OmniSSL Client list.
Revoke	Click **Revoke** to validate the client certificate against the revoked certificates.
Resume	When the client is in the revocation status, the user can click **Resume** to resume the client, and the Cloud generates a new CRL.
Download	Click **Download** to download the selected certificate and use it when required.

- Click **Import** to import an OmniSSL Client list. This opens the *Import users from local authentication list* page. Select the checkbox corresponding to the *Local authentication* you want to import, and click **Save**. Click **Cancel** to revert to the previous settings.



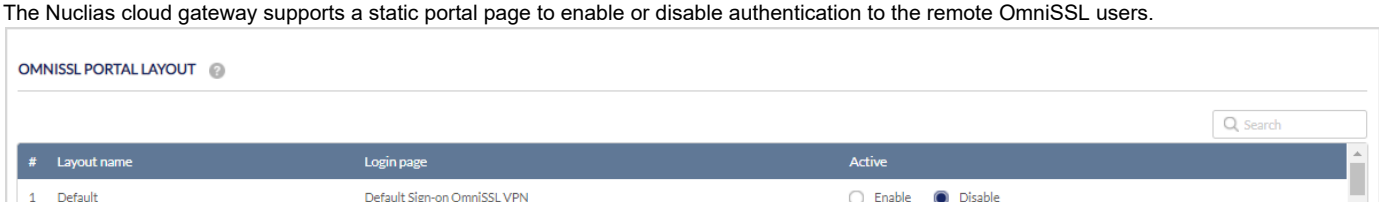
The fields available on this page are as follows:

Field	Description
Local authentication	It displays the name of the local authentication.
Access level	It displays the access level for the local authentication.
Entries	It displays the number of login credentials saved in the local authentication server.
Add local authentication	Click this button to add a local authentication. This opens the *Add local authentication list* page. For details, refer to the Local authentication list.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

- Click **Download** to download the OmniSSL list in the *.csv format.

OmniSSL Portal Layout

The Nuclias cloud gateway supports a static portal page to enable or disable authentication to the remote OmniSSL users.



The fields displayed in the *OmniSSL Portal layout* table are as follows:

Field	Description
Layout name	It displays a name for the portal layout.
Login page	It displays the portal login page link.
Active	You can enable or disable the portal layout. When you enable it, the OmniSSL URL will appear above the table in the right corner.

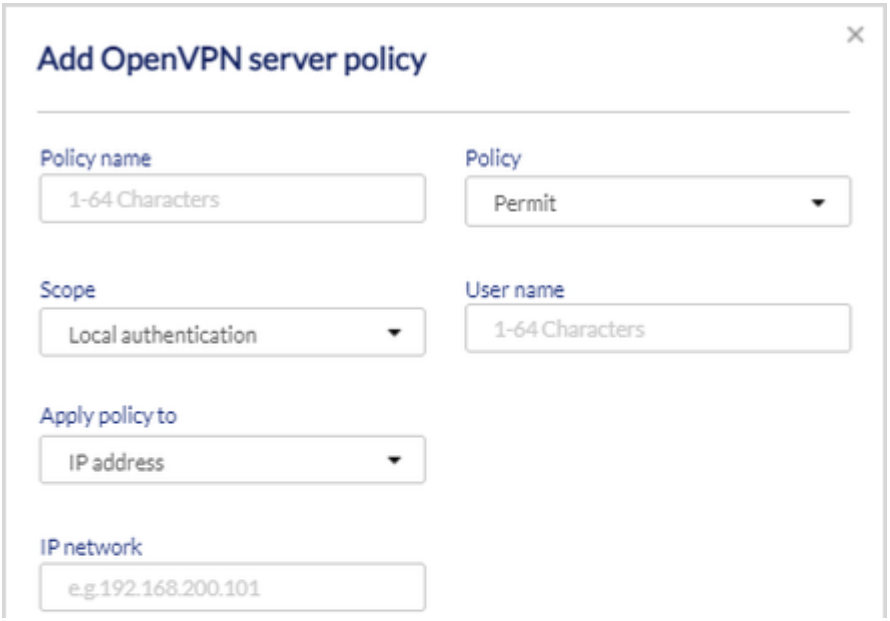
Server Policies

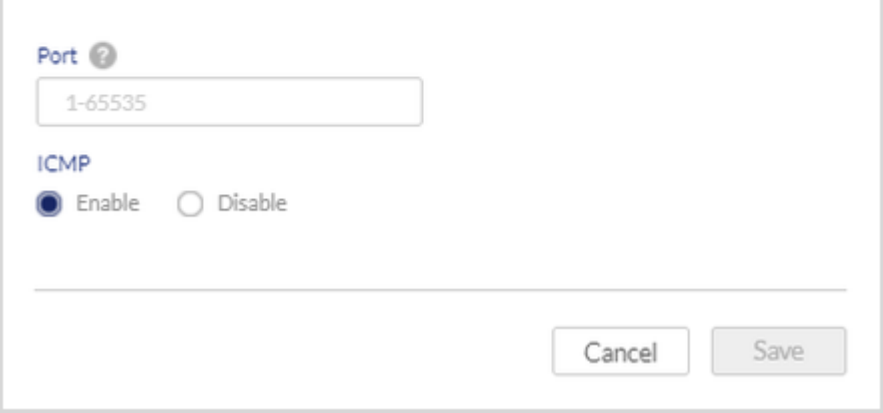
OmniSSL Server Policies are useful in permitting or denying access to specific IP addresses or IP networks. They may be defined at the user or global level.

The fields displayed in the *Server policies* table are as follows:

Field	Description
Name	It displays the name of the server policy.
Policy	It displays the policy applied to the IP address.
Scope	It displays the scope. It is either *Global* or *Local authentication*.
Destination	It displays the IP address to which the OpenVPN policy is applied.
Port	It displays the port number to which the policy is applied.
Actions	You can edit or delete the selected server policy. When you click **Edit**, it opens the *Edit OpenVPN server policy* page.

Click **Add** to add a new entry to the list. This opens the *Add OpenVPN server policy* page. To delete multiple entries, select the corresponding checkboxes, and click **Delete**.



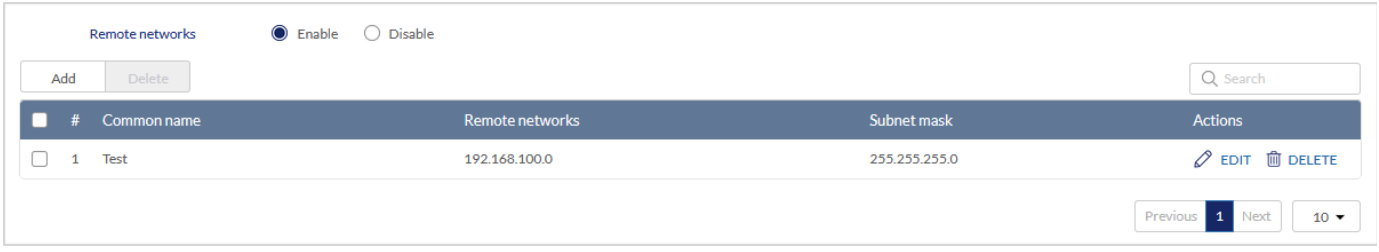


The fields available on the *Add OpenVPN server policy* page are as follows:

Field	Description
Policy name	Enter a name for the server policy.
Policy	Select the policy, whether to permit or deny access to the specific IP address or IP network.
Scope	Select the scope from the drop-down menu. It is either *Global* or *Local authentication*.
Local authentication	If **Local authentication** is selected as the *Scope*, specify the user name (client) to which this policy is to be applied.
Apply policy to	Select an accessible IP address or IP network to which the policy is applied.
IP network	Enter the IP network to which the OpenVPN policy needs to be applied.
Subnet mask	Enter the subnet mask for the above IP network.
IP address	Enter the IP address to which the OpenVPN policy needs to be applied.
Port	Enter the range of port numbers to which the policy will be applied.
ICMP	Enable it to support ICMP traffic.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

Remote Networks

This section displays a list of configured remote networks. The configured IP addresses can remotely access the server through an OpenVPN tunnel.

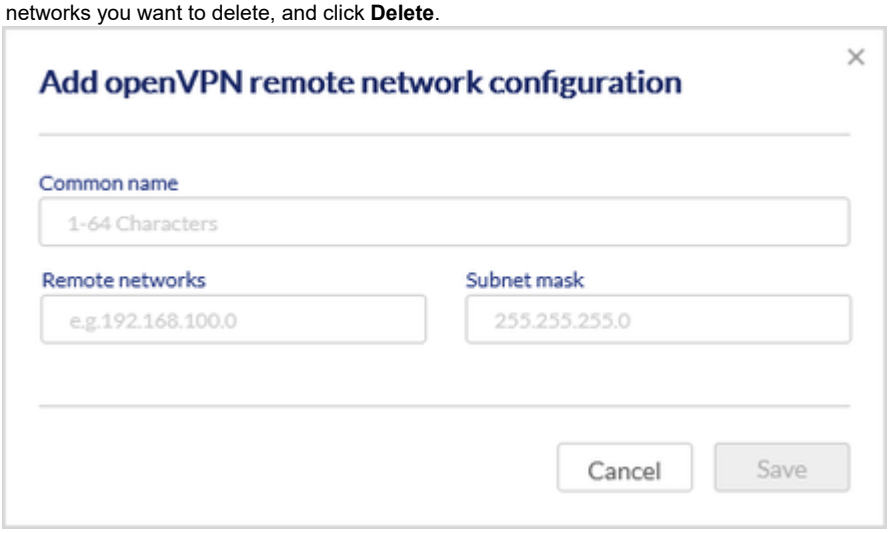


The fields displayed on the *Remote networks* table are as follows:

Field	Description
Common name	It displays the name of the remote network.
Remote networks	It displays the IP address of the remote networks.
Subnet mask	It displays the subnet mask for the IP address of the remote network.
Actions	

	You can edit or delete the corresponding remote network. When you click **Edit**, it opens the *Edit OpenVPN remote network configuration* page.

Click **Add** to add a new entry to the list. This opens the *Add OpenVPN remote network configuration* page. To delete multiple entries, select the checkboxes of the remote networks you want to delete, and click **Delete**.

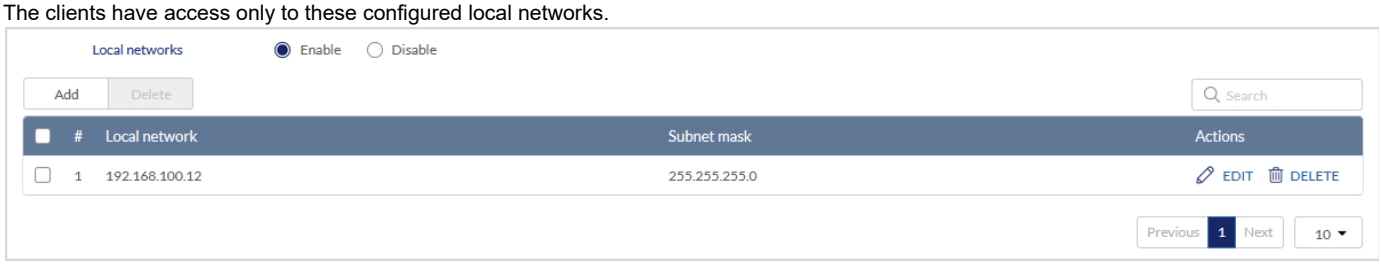


The fields available on the *Add OpenVPN remote network configuration* page are as follows:

Field	Description
Common name	Enter the name of the remote network.
Remote networks	Enter the IP address of the remote networks.
Subnet mask	Enter the subnet mask for the IP address of the remote network.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

Local Networks (Split Tunnel)

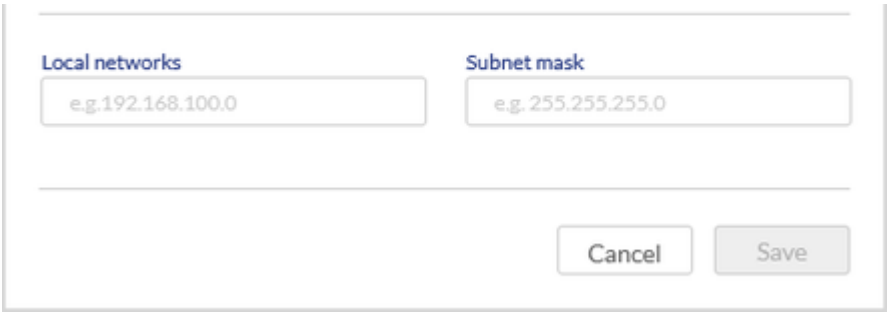
This section is available only when the **Split Tunnel** is selected as the *Tunnel type*. It displays a list of the configured OpenVPN local networks. The clients have access only to these configured local networks.



The fields displayed on the *Local networks* list are as follows:

Field	Description
Local network	It displays the IP address of the local network.
Subnet mask	It displays the subnet mask for the IP address of the local network.
Actions	You can edit or delete the corresponding local network. When you click **Edit**, it opens the *Edit OpenVPN local network configuration* window.

Click **Add** to add a new entry to the list. This opens the *Add OpenVPN local network configuration* page. To delete multiple local networks, select the checkboxes corresponding to the local networks you want to delete, and click **Delete**.

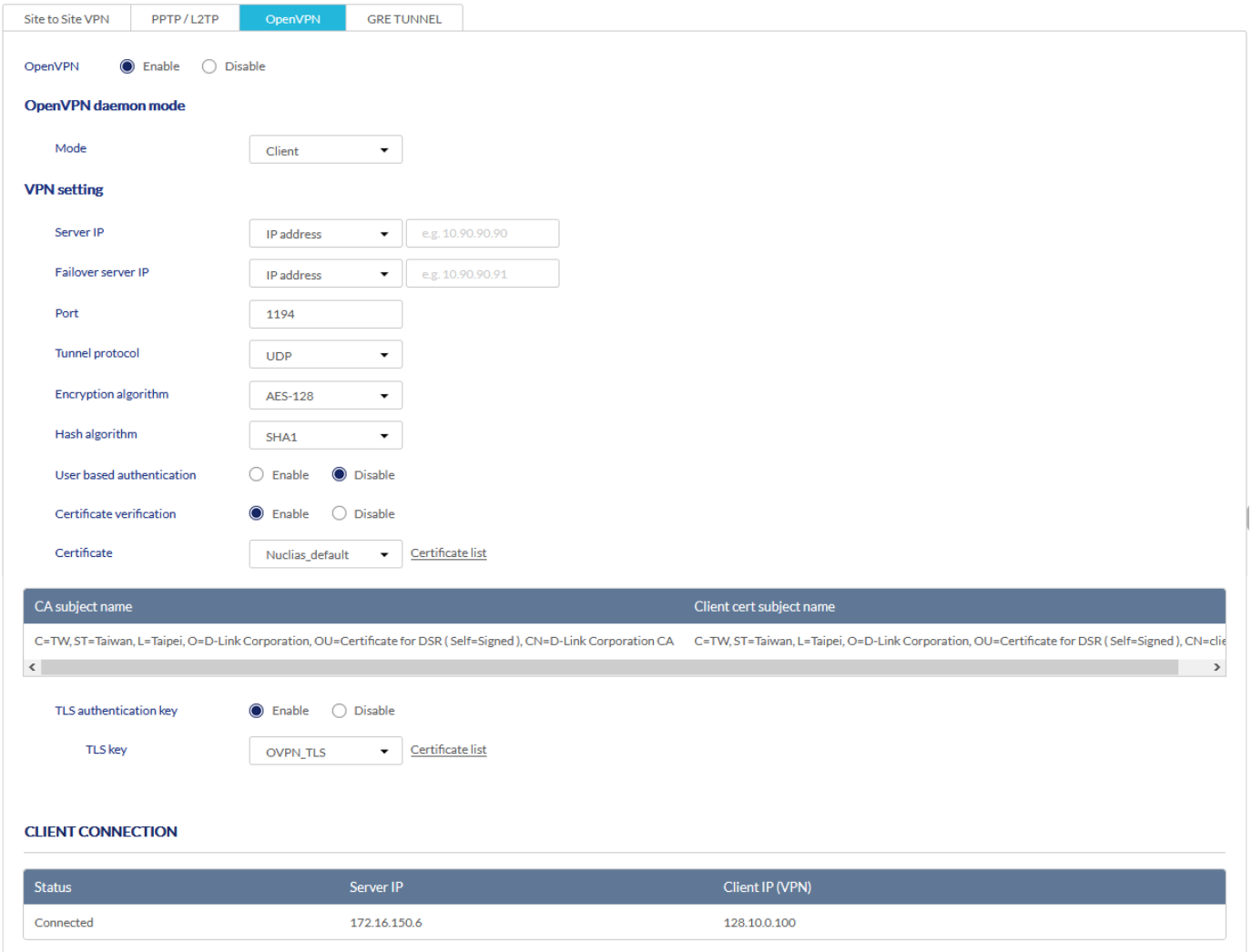


The fields available on the *Add OpenVPN local network configuration* page are as follows:

Field	Description
Local networks	Enter the IP address of the local network.
Subnet mask	Enter the subnet mask for the IP address of the local network.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

Client mode

In this section, you will learn about the OpenVPN configuration in the *Client* mode.

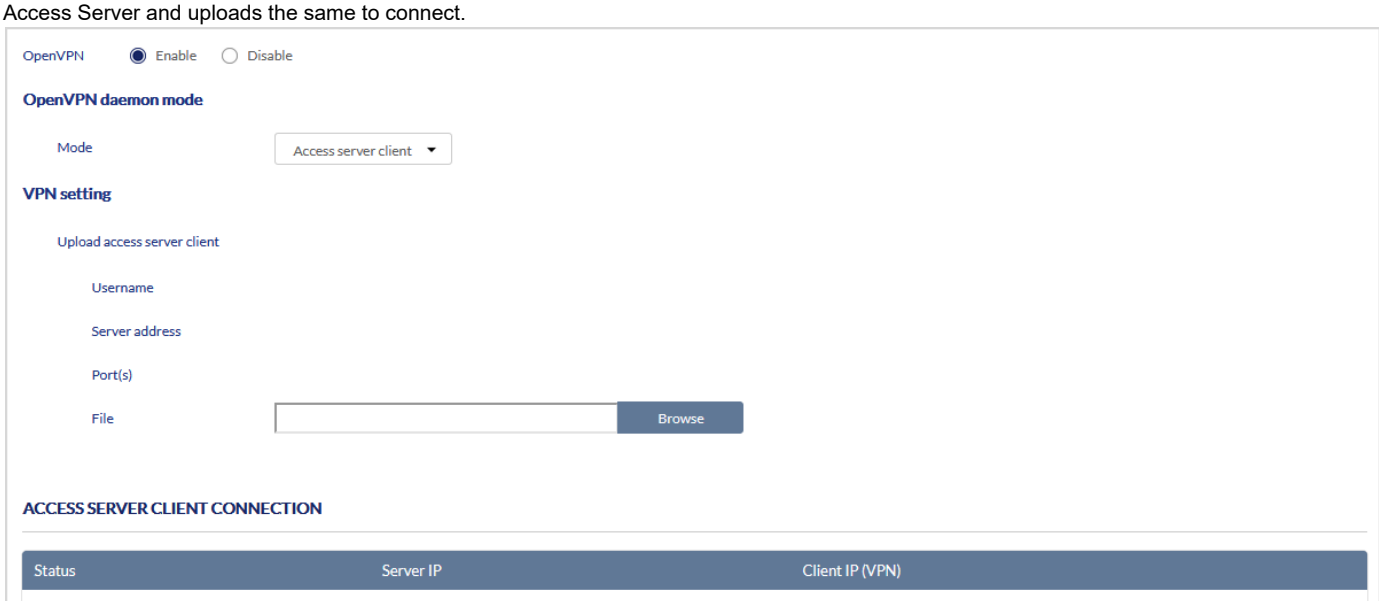


The fields available when the *Client mode* is selected are as follows:

Field	Description
Mode	Select **Client**.
VPN setting	
Server IP	Enter the IP address/FQDN of the OpenVPN server.
Failover server IP	Select the type of identifier you want to provide for the failover mechanism at the Failover Server IP: **IP Address** or **FQDN** (Fully Qualified Domain Name). This feature allows configuring an additional OpenVPN server for the client, which will be used when the primary server is down. This is applicable only in client mode.
Port	Enter the port number on which the OpenVPN server (or Access Server) runs.
Tunnel protocol	Select either *TCP* or *UDP*.
Encryption algorithm	Select the encryption algorithm from the drop-down menu.
Hash algorithm	Select the hash algorithm from the drop-down menu.
User-based authentication	This option provides an additional authentication method using a user name/password. It is disabled by default.
User name	Enter the user name. This field is available when *User-based authentication* is enabled.
Password	Enter the password. This field is available when *User-based authentication* is enabled.
Certificate verification	This method enables tunnel authentication to be with certificates. It is enabled by default.
Certificate	Select the profile which has list certificates uploaded for the configured client mode.
TLS authentication key	Enabling this adds TLS authentication, which adds a layer of authentication. It can be enabled only when the TLS key is uploaded. It is disabled by default.
TLS key	Select the type of TLS certificate name. When you click the *Certificate list* link, it will redirect you to the *Certificate Management* page to add a new certificate and key.
Client Connection	
Status	It displays the connection status of the VPN.
Server IP	It displays the IP address of the server to which the client is connected.
Client IP (VPN)	It displays the IP address of the connected client.

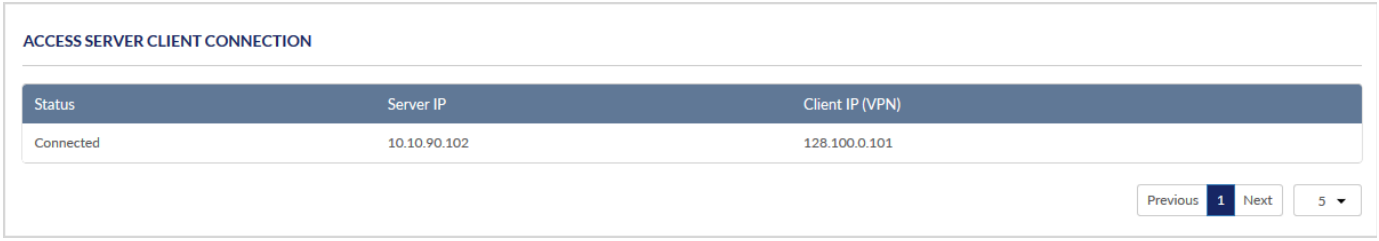
Access server-client mode

Select the mode as access server-client mode. In access server-client mode, the user downloads the auto-login profile from the OpenVPN Access Server and uploads the same to connect.



The fields available when the *Access server-client* mode is selected are as follows:

Field	Description
Mode	Select the **Access Server-Client** mode.
VPN setting	
Upload access server client	
Username	It displays the user name of the client who is trying to connect to the server.
Server address	It displays the IP address of the OpenVPN server to which the client is trying to connect.
Port(s)	It displays the port numbers on which the client will connect with the OpenVPN server (or Access Server).
File	Click **Browse** and locate the configuration file. Click **Open**, and then click **Upload**.



The above table provides the status of the *Access server-client connection,* and the fields displayed in this table are as follows:

Field	Description
Status	It displays the status of the VPN connection. It indicates whether the client is connected to the server or not.
Server IP	It displays the IP address of the server.
Client IP (VPN)	It displays the client's IP address.

GRE Tunnel

GRE tunnels allow LAN broadcast traffic of the gateway to pass over the Internet and receive by the remote LAN hosts. While creating a GRE tunnel, a unique IP address should identify the GRE tunnel endpoint. It will be referenced in the other gateway's static route as the Gateway IP address. The Remote end-address in the GRE tunnel configuration page is the WAN IP address of the other endpoint gateway.

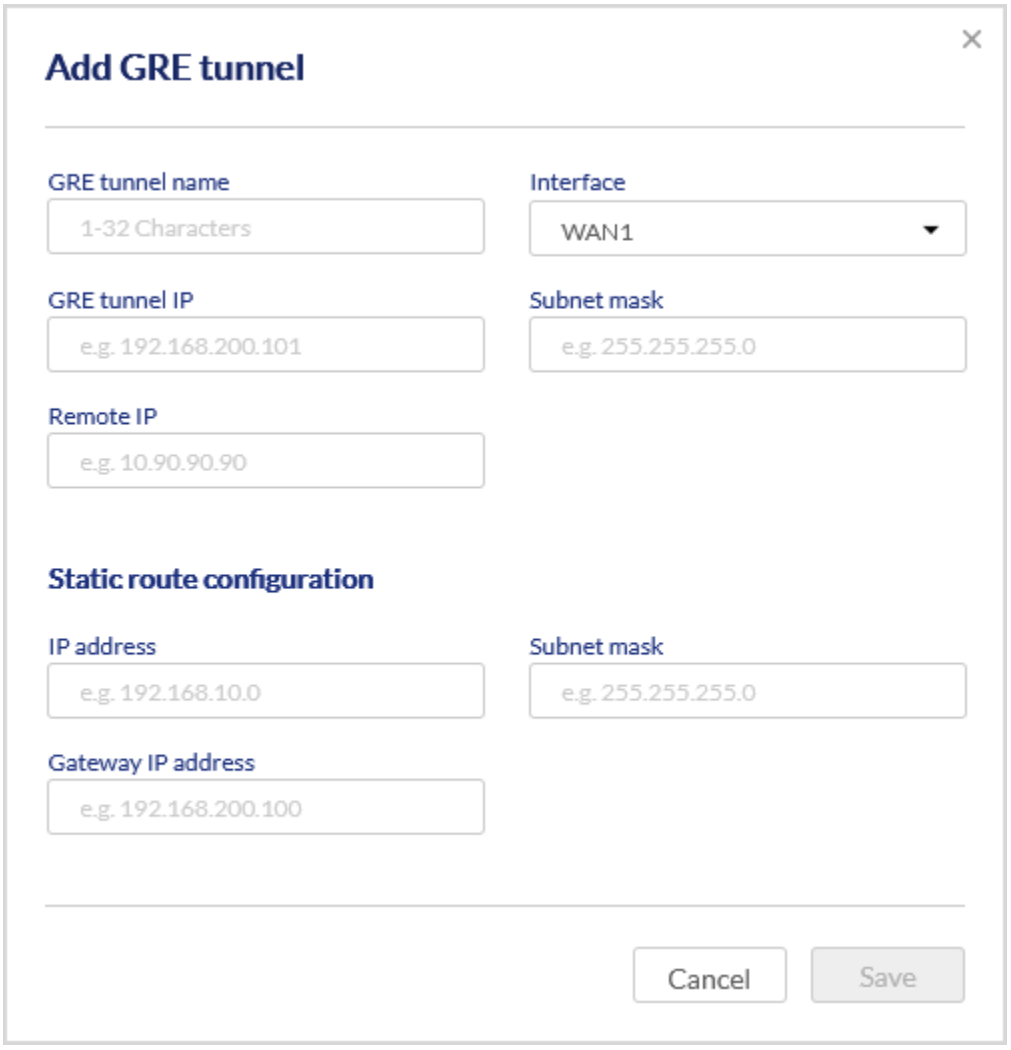
Once the tunnel is established, a static route on the gateway can be made using the interface of the configured GRE tunnel. The destination IP address of the static route is the remote LAN subnet. The route's gateway IP address will be the GRE tunnel IP of the terminating gateway (the same gateway that manages the remote LAN subnet). Once these two steps are completed, the traffic can flow between the configured remote LAN subnets via the GRE tunnel.

The fields displayed in the *Configuration* table are as follows:

Field	Description
Name	It displays the name of the GRE tunnel.
Interface	It displays the interface with which this tunnel is created.
GRE tunnel IP	It displays the IP address of this endpoint.

Remote IP	It displays the WAN IP address of the endpoint gateway.
Active	You can enable or disable the configured tunnel.
Status	It displays the status of the GRE tunnel, i.e., whether it is connected or disconnected.
Actions	You can edit or delete the selected GRE tunnel. When you click **Edit**, it opens the *Edit GRE tunnel* window.

Click **Add** to add a new entry. This opens the *Add GRE tunnel* page. To delete multiple entries, select the checkboxes of the GRE tunnels you want to delete, and click **Delete**.



The fields available on the *Add GRE tunnel* page are given below.

Field	Description
GRE tunnel name	Enter a name for the GRE tunnel.
Interface	Select the interface to create this tunnel.
GRE tunnel IP	Enter the IP address of this endpoint. It will be referenced in the other gateway's static route as the Gateway IP address.
Subnet mask	Enter the subnet mask.
Remote IP	Enter the WAN IP address of the endpoint gateway.
Static route configuration	
IP address	Enter the destination IP address of the static route from the remote LAN subnet.

Subnet mask	Enter the subnet mask.
Gateway IP address	Enter the IP address of the termination gateway.
Save	Click **Save** to save your settings.
Cancel	Click **Cancel** to revert to the previous settings.

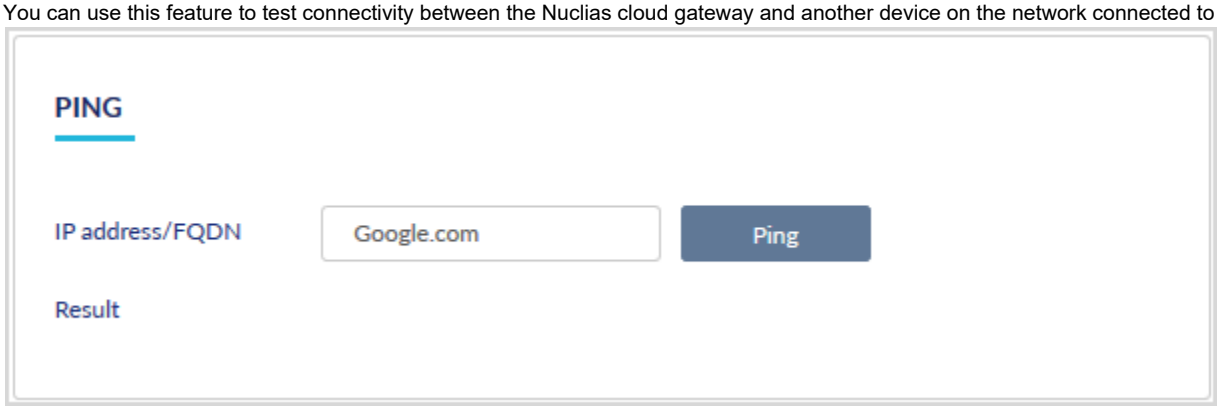
Chapter 6 Tools

This chapter of the user guide provides you with the information and configuration of the diagnostic tools supported by the Nuclias cloud gateway, like ping and traceroute. You can also find out the performance of the WAN connection. Clicking a button will show you the upload and download speed of the WAN port. You can use these tools to detect the connectivity and troubleshoot it when required.

This chapter covers the following topics:

Ping

As part of the diagnostics tools supported by the Nuclias cloud gateway, you can ping an IP address or FQDN (Fully Qualified Domain Name). You can use this feature to test connectivity between the Nuclias cloud gateway and another device on the network connected to the gateway.

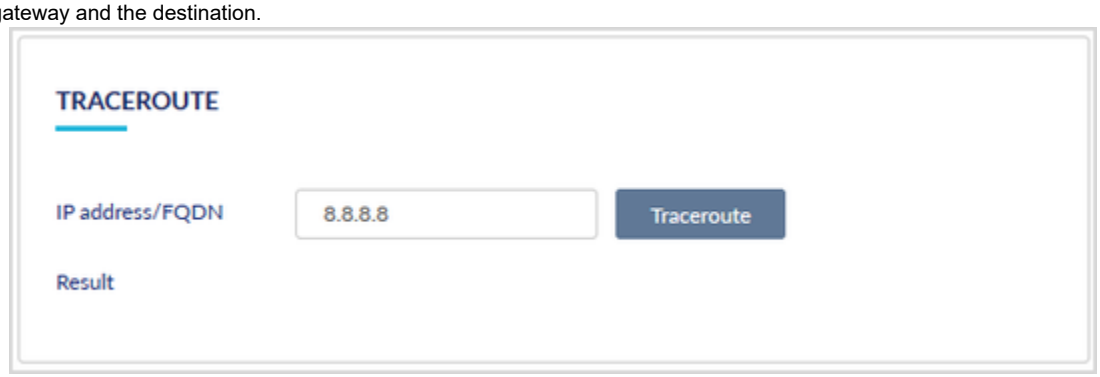


The fields available in this section are as follows:

Field	Description
IP address/FQDN	Enter the IP address or FQDN.
Ping	Click **Ping** to send an ICMP echo request packet to the destination using the IPv4 network.
Result	It displays the result of the IP address. If the destination IP address is active, you can see a response. A *response timed-out* message indicates that the destination is either not active or is blocking ping requests.

Traceroute

The Nuclias cloud gateway provides a *Traceroute* function to map the network path to a public host. In addition, it displays up to 30 “hops” between this gateway and the destination.



The fields available in the *Traceroute* section are as follows:

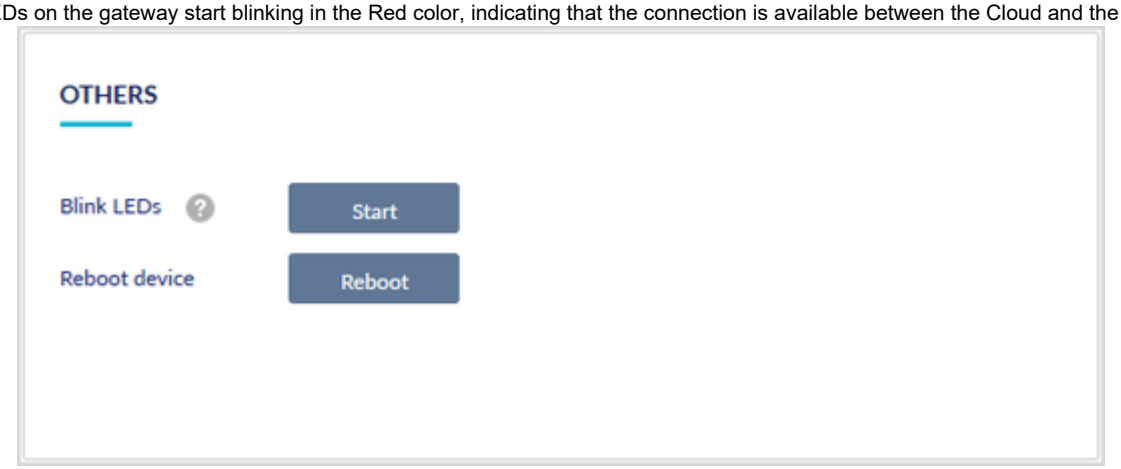
Field	Description

IP address/FQDN	Enter the IP address or FQDN.
Traceroute	Click **Traceroute** to display all the routers present between the destination IP address and this gateway.
Result	This section displays the results of the Traceroute operation.

Others

Blink LEDs

The front panel of the cloud gateway consists of two LEDs that indicate the gateway's power and the cloud status of the gateway. The *Blink LEDs* feature helps you check if the connection has been established between the gateway and the cloud. After you click the **Start** button, the Power and Cloud LEDs on the gateway start blinking in the Red color, indicating that the connection is available between the Cloud and the gateway.



Power Supply LED

The power LED indicates the power status of the gateway.

LED	Color	Status	Description
Power	Orange/Green/Red	Solid Orange	Power-on is in progress.
		Blinking Orange	Firmware upgrade in progress.
		Solid Green	Power-on completed.
		Solid Red	Factory reset in progress.
		Blinking Red	The **Start** button of *Blink LEDs* is clicked.
		Off	The device is power-off.

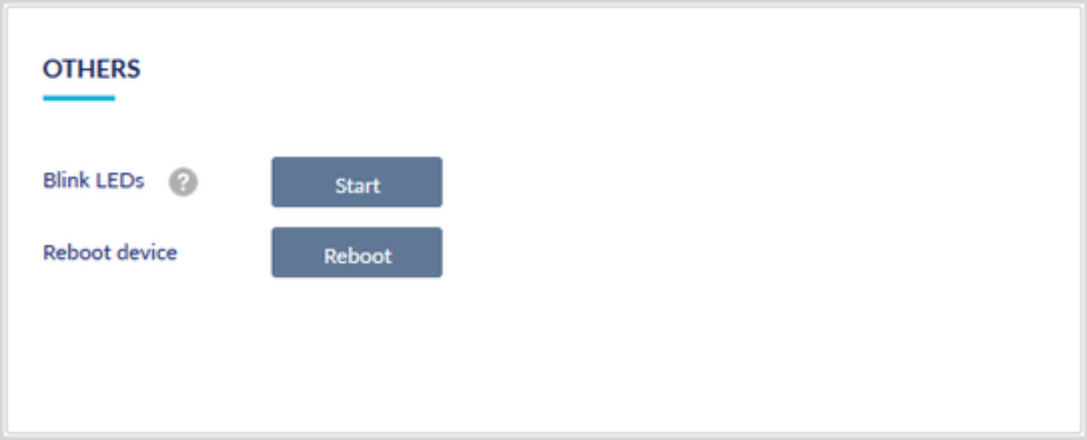
Cloud Status LED

The cloud status LED indicates the Nuclias cloud connection status of the device.

LED	Color	Status	Description
Cloud	Orange/Green/Red	Solid Orange	Establishing Cloud connection
		Solid Green	Established Cloud connection
		Solid Red	No cloud connection established
		Blinking Red	The **Start** button of *Blink LEDs* is clicked.
		Off	The device is power-off.

Reboot device

Click the **Reboot** button to perform the power cycle.



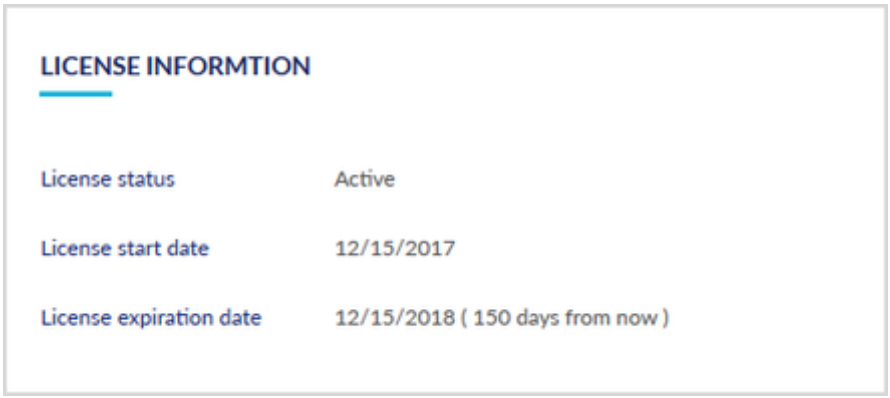
Chapter 7 License

The Nuclias cloud gateway supports cloud features, and these features come with a license. In this chapter, you will learn about the license active on your device. It will also guide you on how to add a license to your device.

This chapter covers the following topics:

License Information

This section of the License menu provides license details, like the date of activation, its present status, and its expiry date.

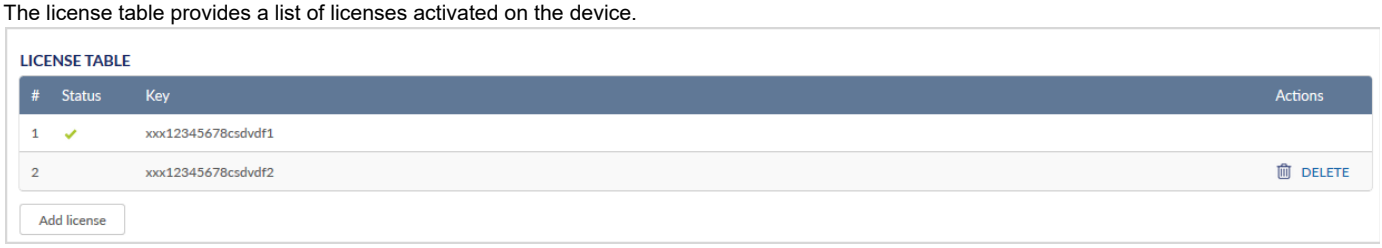


The fields available in this section are as follows:

Field	Description
License status	It displays the current status of your license, i.e., whether the license is active or not.
License start date	It displays the date when you activated the license.
License expiration date	It displays the date when the license gets expired and the number of days left for expiration.

License Table

The license table provides a list of licenses activated on the device.



The fields displayed on this page are as follows:

Field	Description
Status	It displays the status of the license, i.e., whether the license is active or not. If active, a tick mark is displayed.
Key	It displays the activation code of the license.
Actions	You can delete the selected license.

To add a new license, click **Add license**. This opens the *Add license* page. Select a license key and click **Save**. Click **Cancel** to close the page.