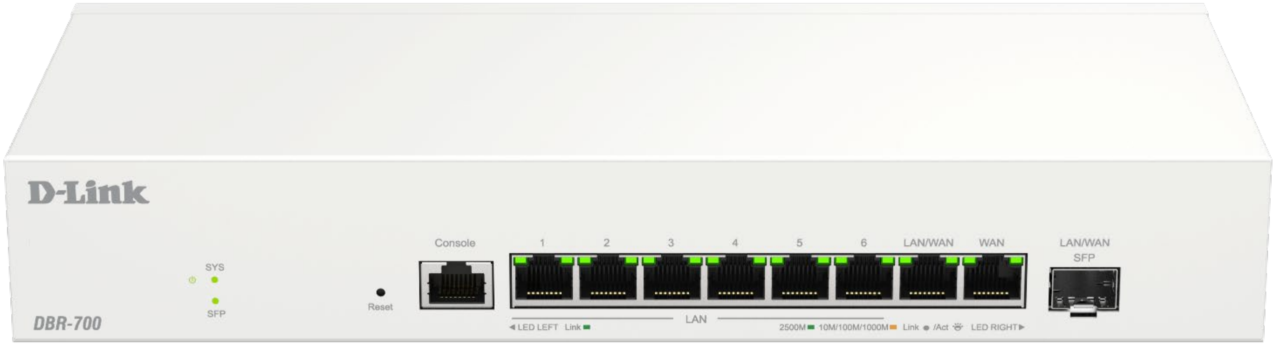
Version 1.00 | 07/30/2025



User Manual

Business Router

DBR-700

Chapter 1 Introduction

1.1 Introduction

Congratulations on your purchase of this outstanding product: advanced Business router. For remote worker or Small office applications, D-Link DBR-700 Business router is absolutely the right choice.

DBR-700 products are loaded with luxuriant security features including VPN, firewall, port forwarding, DHCP server and many other powerful features for remote workers or small office

Main Features:

- All 2.5 Gbps WAN/LAN Interfaces
- Dual WAN for Load Balancing or Failover
- 2.5G SFP Port
- High-Performance VPN Server/Client support (IPSec, PPTP/L2TP, WireGuard)
- Comprehensive Security Features: SPI Firewall, DoS/DDoS Protection, IPS, URL Blocking
- Captive Portal for guest access management
- Smart Access Point (AP) Management

Before installing and using this product, please read this manual thoroughly to take full advantage of its powerful features.

1.2 Contents List

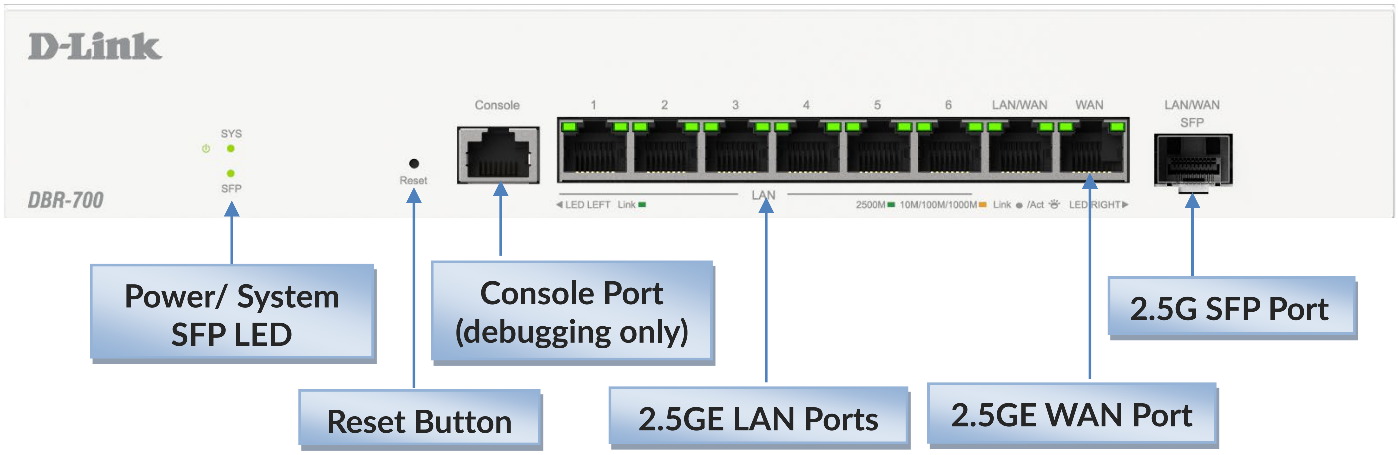
1.2.1 Package Contents

Standard Package

Items	Description	Quantity
1	**DBR-700**	1pcs
3	**RJ45 Cable**	1pcs
4	**Power Adapter (12V/2A)**	1pc
5	**Rack Mount Kit**	1 set

1.3 Hardware Configuration

➢ Front View



※Reset Button

The RESET button provides users with a quick and easy way to restore the device to its factory default settings. To perform a reset, press and hold the RESET button for approximately 6 seconds, then release it. The device will automatically reboot and restore all settings to their default values.

1.4 LED Indication

Device LED

LED Indicator	Color	LED Status	Description (Power on/processing/off)
Power	Green	Solid Green	Completion of power on
		Blinking Green (normal)	The device is under power-on process
		Off	The device is powered off
LED Indicator	Color	LED Status	Description (System Ready/Firmware Upgrade/recovery mode)
System	Green	Solid Green	System is ready
		Blinking Green (normal)	System is upgrading firmware or operating in recovery mode.
LED Indicator	Color	LED Status	Description (Link , Speed , activity)
SFP	Green	Solid Green	A valid link is established

			on the fiber port.
		Blinking Green (normal)	The fiber port is transmitting or receiving data.
		Off	No active SFP module or no link established.

Embedded LED

Embedded LED Location	Color	Right LED Status	Description (Link, Speed and activity)
Port 1~8 RJ45 Phone Jack	Green or Amber	Solid Green	A valid 2.5Gbps link is established.
		Blinking Green (normal)	The port is transmitting or receiving data at 2.5Gbps.
		Solid Amber	A valid 10Mbps, 100Mbps, or 1000Mbps link is established.
		Blinking Amber (normal)	The port is transmitting or receiving packets at 10Mbps, 100Mbps or 1000Mbps.
		Off	No link is established.
Embedded LED Location	**Color**	**Left LED Status**	**Description (link, speed and activity)**
Port 1~8 RJ45 Phone Jack	Green	Solid Green	An Ethernet device is connected and the link is up.
		Off	No link is established.

1.5 Installation & Maintenance Notice

1.5.1 System Requirements

Network Requirements	• A Gigabit Ethernet RJ45 cable or DSL modem • 10/100/1000 Ethernet adapter on PC
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter **Browser Requirements:** • Internet Explorer 6.0 or higher • Chrome 2.0 or higher • Firefox 3.0 or higher • Safari 3.0 or higher

Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.
This transmitter must not be co-located or operated in conjunction with any other antenna or transmitter.

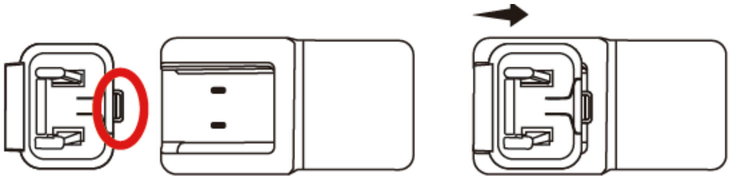
1.6 Hardware Installation

This chapter describes how to install and configure the hardware

1.6.1 Power On the device

The AC adapter plug is detachable. If excessive force (e.g., tripping over the cable) is applied, the plug may loosen or detach. Using a damaged or improperly attached plug may cause sparks, fire, or smoke. Stop using the product immediately if the plug is loose or broken.

.



Align the pin assembly with the adapter body.

Slide the pin assembly into the adapter body until it snaps into place.

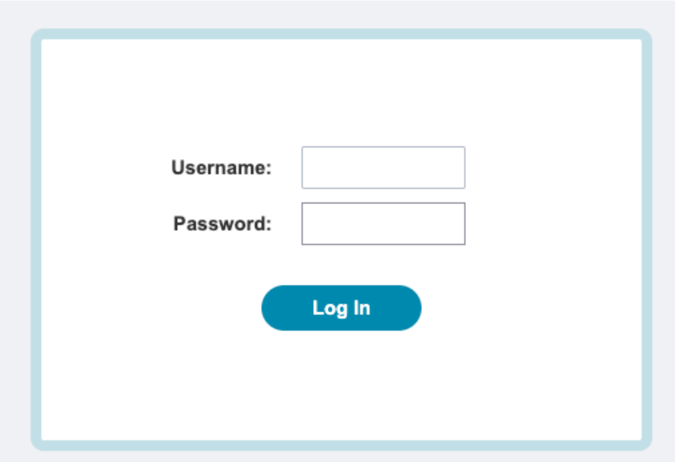
1.6.4 Connecting to the Network or a Host

The DBR-700 has eight RJ45 ports supporting 10/100/1000/2500Mbps Ethernet with auto speed detection. Connect one end of an Ethernet cable to a LAN port on the device and the other end to your computer to configure the device.

1.6.5 Setup by Configuring WEB UI

To configure the device, open a web browser and enter the IP address: **https://192.168.10.1**

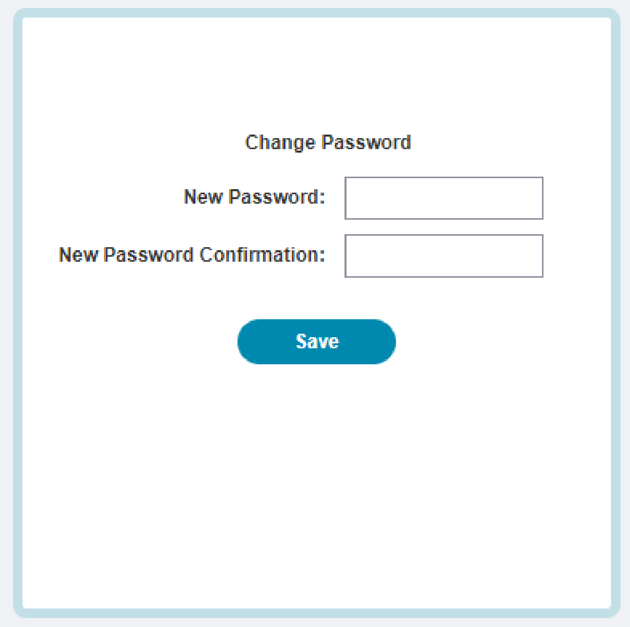
On the login page, enter the username and password, then click “Log in.” The default credentials are username: **admin**, password: **Admin$123.**



Username:

Password:

For security reasons, you will be prompted to change the login password upon first login.



Change Password

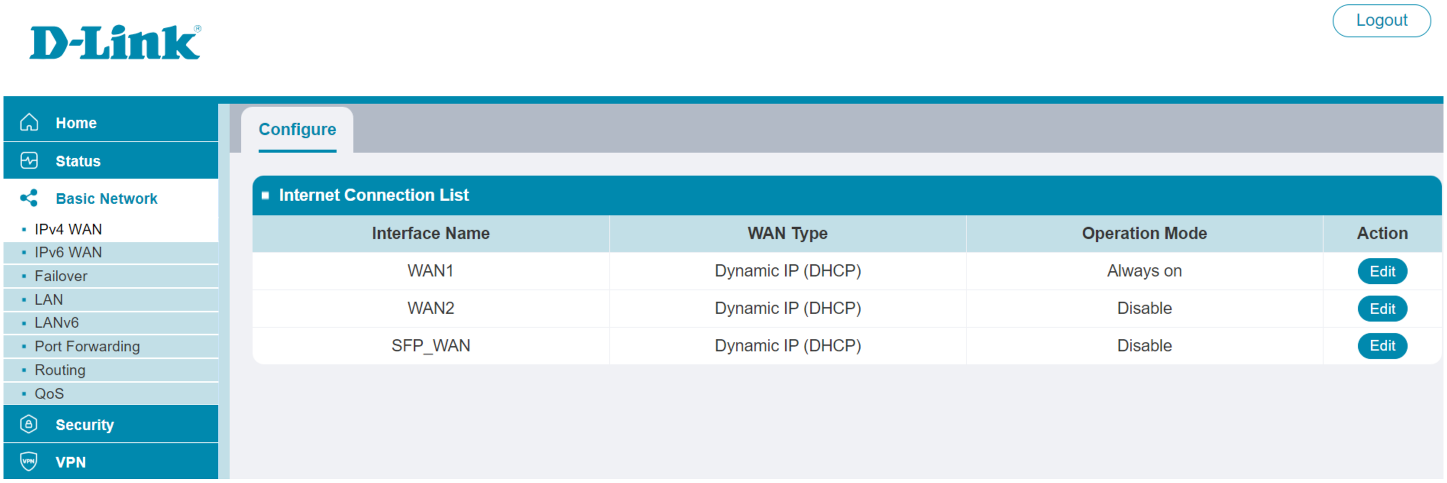
New Password:

New Password Confirmation:

After that, you will be asked to log in again with the new password.

Chapter 2 Basic Network

2.1 IPv4 WAN



Internet Connection List

Interface Name	WAN Type	Operation Mode	Action
WAN1	Dynamic IP (DHCP)	Always on	Edit
WAN2	Dynamic IP (DHCP)	Disable	Edit
SFP_WAN	Dynamic IP (DHCP)	Disable	Edit

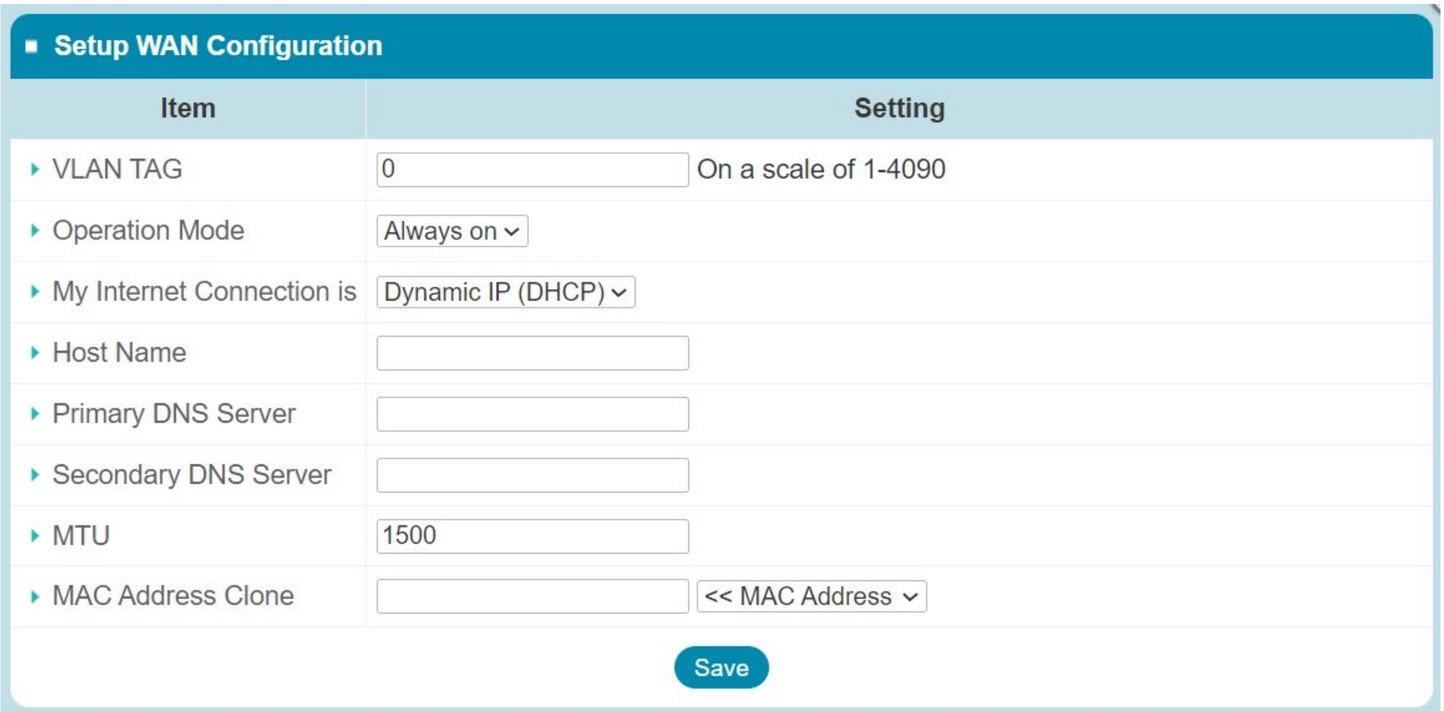
The DBR-700 gateway provides multiple WAN interfaces, allowing intranet clients to access the Internet through different ISPs. Since ISPs use various protocols and transmission media, each WAN interface can be configured separately to meet specific requirements.

To configure a WAN interface, start by selecting the type of connection media in the IPv4 or IPv6 WAN settings.

Operation Mode Options:

- **Always On:** Keeps the WAN interface active at all times. If multiple WANs are set to this mode, traffic will be distributed according to load balancing rules.
- **Failover:** Acts as a backup connection. This WAN becomes active only if the primary connection fails.
- **Disable:** Disables the WAN interface.

2.1.1 Physical Interface



Setup WAN Configuration

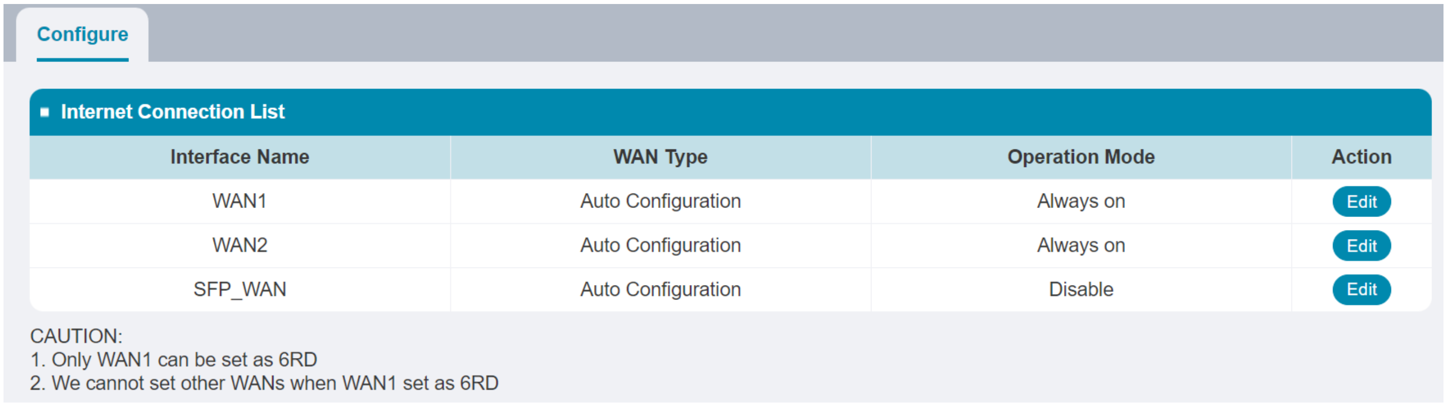
Item	Setting
VLAN TAG	0 On a scale of 1-4090
Operation Mode	Always on
My Internet Connection is	Dynamic IP (DHCP)
Host Name	
Primary DNS Server	
Secondary DNS Server	
MTU	1500
MAC Address Clone	<< MAC Address

The fields available on this page are as follows:

Field	Description
VLAN TAG	Specifies VLAN ID for WAN tagging. Use only if your ISP requires VLAN. Integer from 1 to 4090 (default: 0)
Operation Mode	Defines the WAN interface behavior: Always on, Failover, Disable.
My Internet Connection is	Select the WAN connection type as required by your ISP. **Dynamic IP (DHCP):** Automatically obtains an IP address from the ISP using DHCP. **Static IP:** Manually set a fixed IP address provided by the ISP. **PPPoE:** Requires a username and password to establish a connection via ISP's server.
Host Name	Optional hostname sent to the ISP when using DHCP. Required only if your ISP needs a specific hostname.
Primary DNS Server	Optional override for DNS server provided by ISP.
Secondary DNS Server	Optional second DNS server if the primary is unreachable.
MTU	Maximum Transmission Unit size for packets. Usually left at default. (default: 1500)
MAC Address Clone	Allows cloning of MAC address (if ISP binds service to specific MAC).

2.2 IPv6 WAN

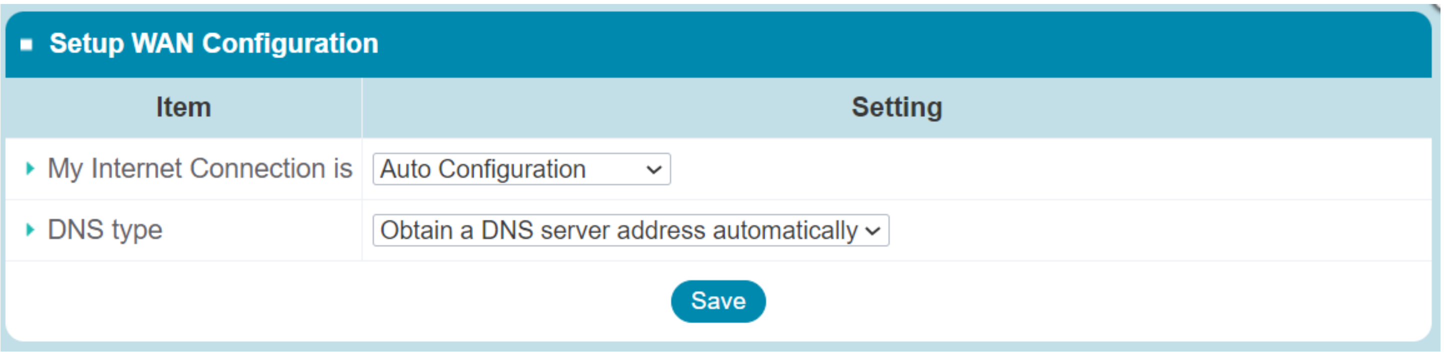
This section allows you to configure IPv6 connectivity for each WAN interface.



Internet Connection List

Interface Name	WAN Type	Operation Mode	Action
WAN1	Auto Configuration	Always on	Edit
WAN2	Auto Configuration	Always on	Edit
SFP_WAN	Auto Configuration	Disable	Edit

CAUTION:
1. Only WAN1 can be set as 6RD
2. We cannot set other WANs when WAN1 set as 6RD



Setup WAN Configuration

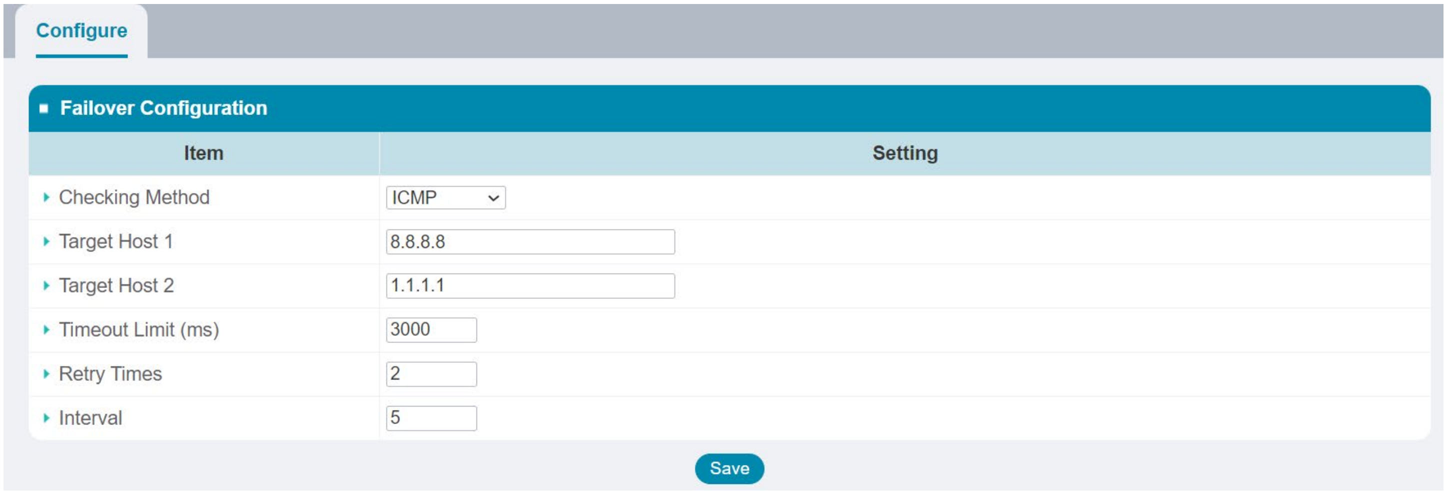
Item	Setting
My Internet Connection is	Auto Configuration
DNS type	Obtain a DNS server address automatically

The fields available on this page are as follows:

Field	Description
My Internet Connection is	**Static IPv6**: Use this option if your Internet Service Provider (ISP) has provided a fixed IPv6 address. You must manually enter IP, subnet, gateway, and DNS. **Auto Configuration:** Automatically obtains IPv6 configuration from the ISP. **PPPoE:** Required by ISPs that use PPPoE authentication. You must enter the provided username and password. **6RD (IPv6 Rapid Deployment):** Enables IPv6 connectivity over IPv4 infrastructure using 6RD tunneling. **Local Connectivity Only:** No Internet connection will be established. This mode allows only local (LAN) access, typically for internal network use or testing purposes.
DNS Type	**Obtain a DNS server address automatically:** The DNS server address is assigned dynamically by the ISP via DHCP. This is the default setting for most users. **Use the following DNS address:** Allows manual configuration of preferred and alternate DNS server addresses.

2.3 Failover

When WAN2 is set to *Failover* mode, the detection criteria can be configured under **Basic Network > Failover**. This allows the system to detect WAN disconnection and trigger failover if necessary.



■ Failover Configuration

Item	Setting
Checking Method	ICMP
Target Host 1	8.8.8.8
Target Host 2	1.1.1.1
Timeout Limit (ms)	3000
Retry Times	2
Interval	5

The fields available on this page are as follows:

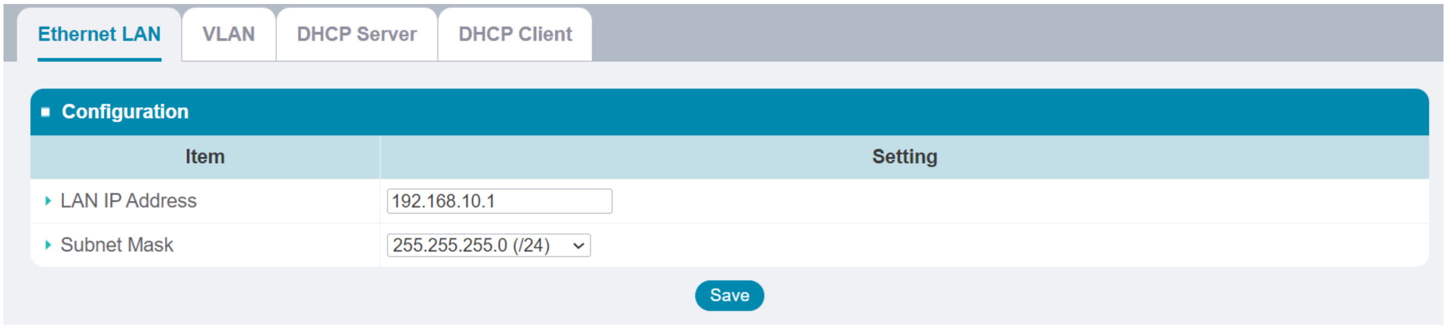
Field	Description
Checking Method	Specifies the method used to detect WAN availability. **ICMP**: sends ping requests to verify connection status. **DNS Query**: Sends a DNS request to verify if the network can resolve domain names properly.
Target Host 1	The primary IP address or hostname used for connectivity checking. The system will periodically check connectivity to this host. Example: 8.8.8.8.
Target Host 2	A secondary IP address or hostname used as a backup for connectivity checking. This is used if the primary host fails to respond. Example: 1.1.1.1.
Timeout Limit (ms)	Sets the maximum time (in milliseconds) the system will wait for a response from the target host before considering the attempt failed. Example: 3000 ms = 3 seconds. Range: 1-10000.
Retry Times	Defines how many consecutive failures must occur before the WAN is considered down.
Interval	Sets the time interval (in seconds) between each check. Determines how frequently the system tests the connection.

2.4 LAN

This section covers the configuration of Ethernet LAN, VLAN, DHCP Server, and DHCP Client.

2.4.1 Ethernet LAN

Configure the LAN IP address and subnet mask of the device.



▪ Configuration

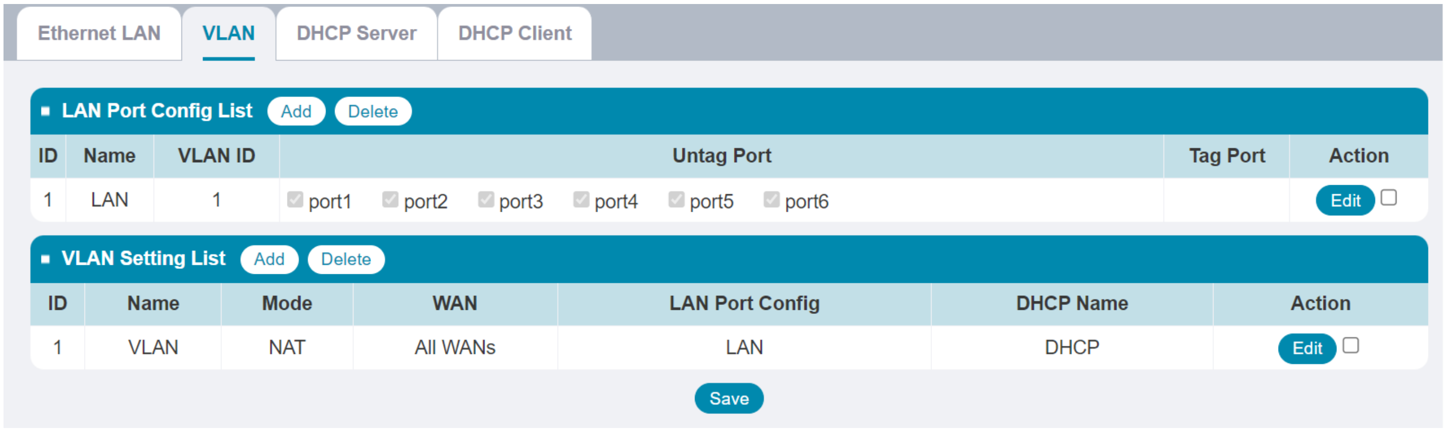
Item	Setting
‣ LAN IP Address	192.168.10.1
‣ Subnet Mask	255.255.255.0 (/24)

The fields available on this page are as follows:

Field	Description
LAN IP Address	The device's default LAN IP address
Subnet Mask	Defines the IP range and network size.

2.4.2 VLAN

This section allows users to configure **Virtual LAN (VLAN)** settings to segment network traffic for improved security and traffic management.



▪ LAN Port Config List

ID	Name	VLAN ID	Untag Port	Tag Port	Action
1	LAN	1	☑ port1 ☑ port2 ☑ port3 ☑ port4 ☑ port5 ☑ port6		Edit ☐

▪ VLAN Setting List

ID	Name	Mode	WAN	LAN Port Config	DHCP Name	Action
1	VLAN	NAT	All WANs	LAN	DHCP	Edit ☐

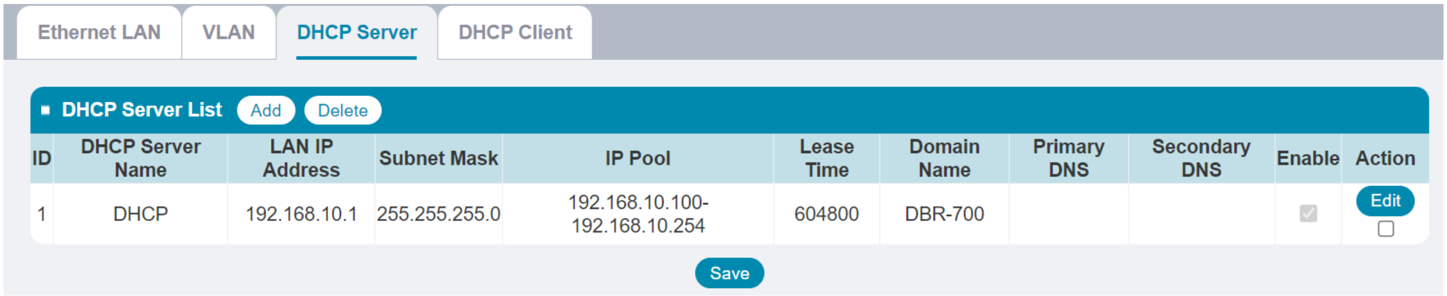
The fields available on this page are as follows:

Field	Description
Name	Defines the name of the port group associated with a specific VLAN. Used to identify and apply settings to selected LAN ports.

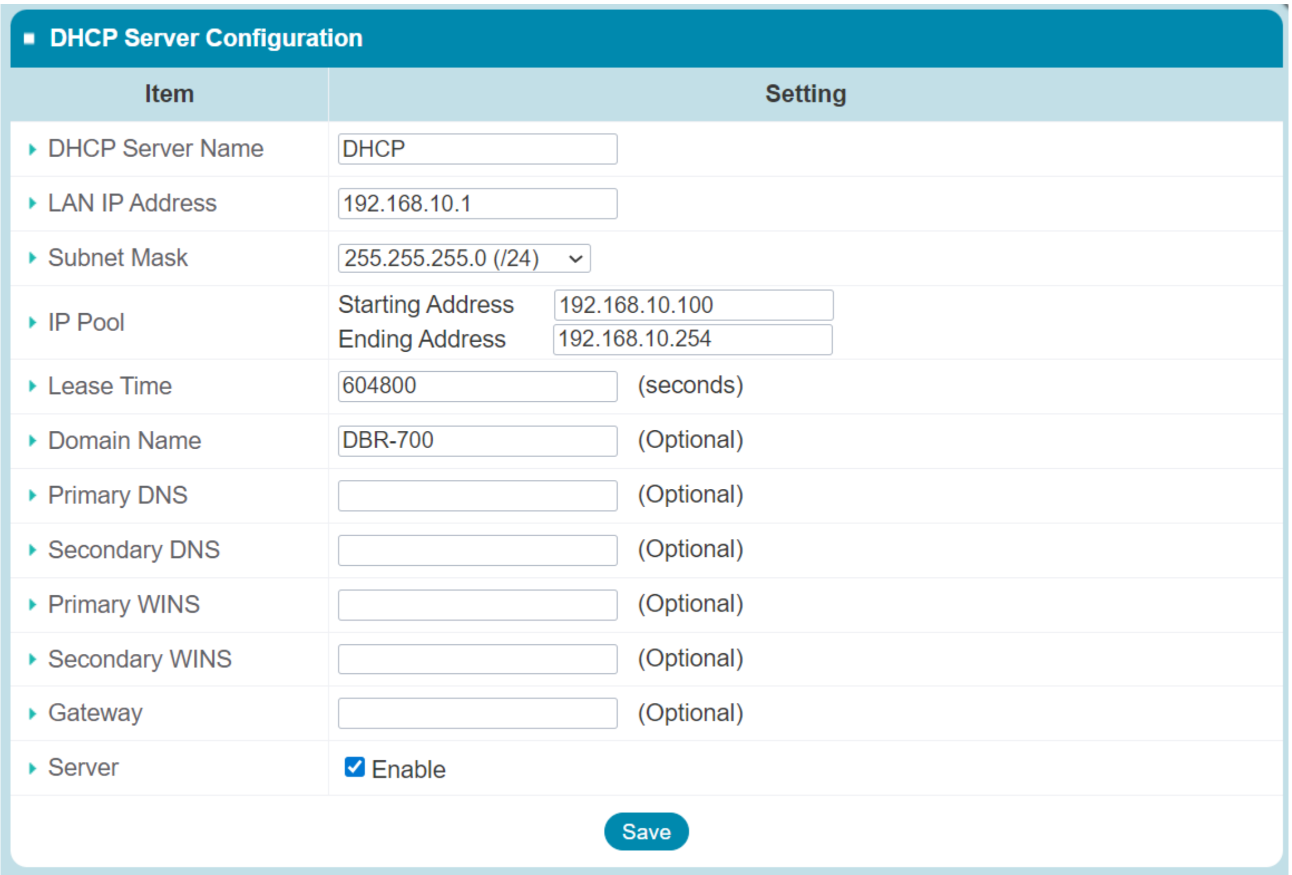
VLAN ID	Identifies the VLAN group.
Untag Port	Ports that send and receive traffic without VLAN tags.
Tag Port	Ports that handle tagged VLAN traffic.
Bridge	Enables bridging mode to link this VLAN with other interfaces.
DHCP Option	**DHCP Option**: Specifies whether the VLAN uses a DHCP Server, DHCP Relay, or disables DHCP. **DHCP Server:** The device will act as a **DHCP server** within the VLAN, automatically assigning IP addresses to client devices. **DHCP Relay:** The device will act as a **DHCP relay agent**, forwarding DHCP requests from VLAN clients to a designated external DHCP server on another network. **Disable:** DHCP is turned off for this VLAN. Devices must be configured with static IP addresses manually.
DHCP Name	Associates the VLAN with a specific DHCP configuration.

2.4.3 DHCP Server

The DHCP Server setting allows users to create and customize DHCP Server policies to assign IP Addresses to the devices on the local area network (LAN).



ID	DHCP Server Name	LAN IP Address	Subnet Mask	IP Pool	Lease Time	Domain Name	Primary DNS	Secondary DNS	Enable	Action
1	DHCP	192.168.10.1	255.255.255.0	192.168.10.100- 192.168.10.254	604800	DBR-700			☑	Edit □



DHCP Server Configuration

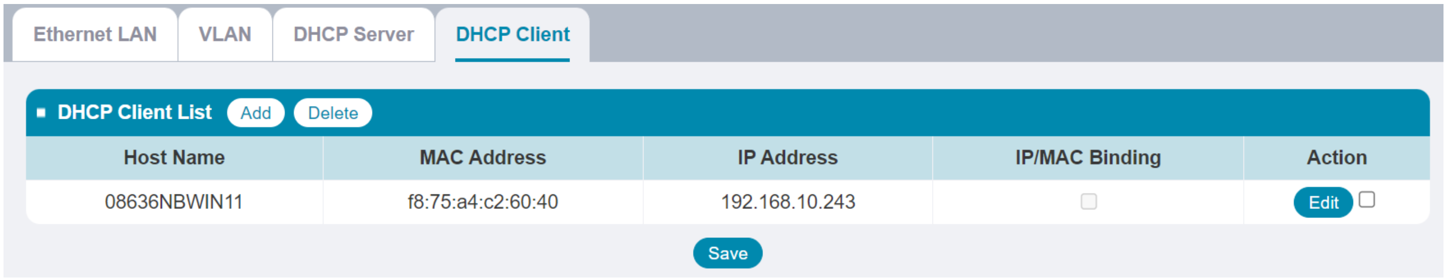
Item	Setting
DHCP Server Name	DHCP
LAN IP Address	192.168.10.1
Subnet Mask	255.255.255.0 (/24)
IP Pool	Starting Address 192.168.10.100 Ending Address 192.168.10.254
Lease Time	604800 (seconds)
Domain Name	DBR-700 (Optional)
Primary DNS	(Optional)
Secondary DNS	(Optional)
Primary WINS	(Optional)
Secondary WINS	(Optional)
Gateway	(Optional)
Server	☑ Enable

The fields available on this page are as follows:

Field	Description
DHCP Server Name	Identifier for the DHCP server.
LAN IP Address	The IP address of the router on the local network (interface IP).
Subnet Mask	Defines the network portion of the IP address.
IP Pool	The range of IP addresses that the DHCP server can assign to clients.
Lease Time	Duration (in seconds) that an IP address is leased to a client. 604800 seconds equals 7 days. After this time, the lease expires unless renewed.
Domain Name	Optional domain name for the network. Used by DHCP clients to set their local domain.
Primary DNS	Optional. IP address of the primary DNS server that clients will use for domain name resolution.
Secondary DNS	Optional. IP address of the secondary DNS server for redundancy.
Primary WINS	Optional. IP address of the primary WINS server (used for NetBIOS name resolution, mostly in older Windows networks).
Secondary WINS	Optional. IP address of a backup WINS server.
Gateway	Optional. Default gateway for DHCP clients.

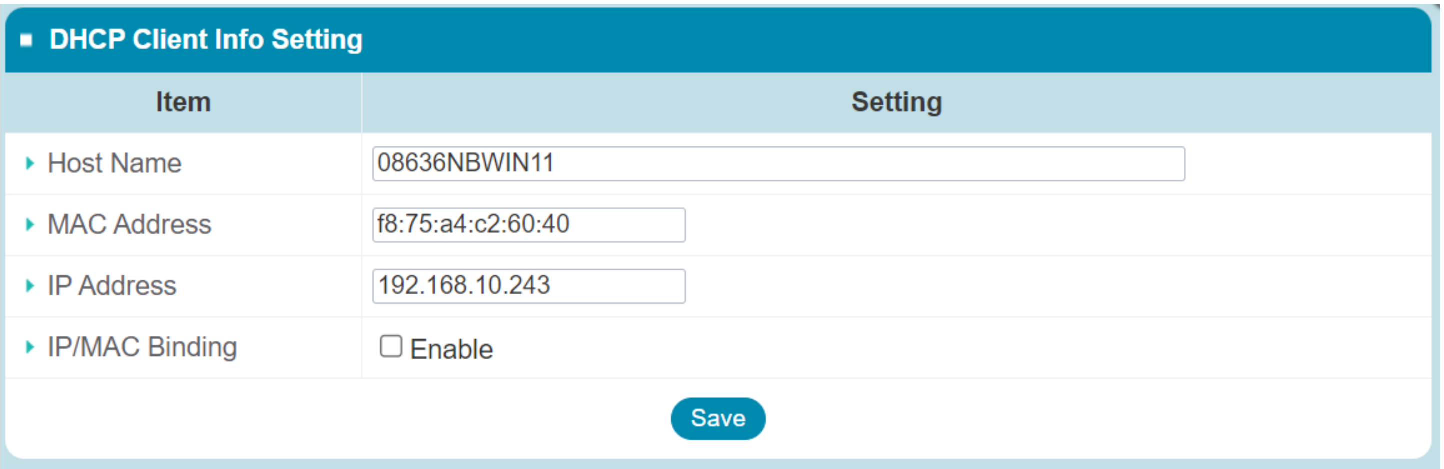
2.4.4 DHCP Client

The DHCP Client feature consists of two main functions: IP Reservation and IP/MAC Binding.



DHCP Client List

Host Name	MAC Address	IP Address	IP/MAC Binding	Action
08636NBWIN11	f8:75:a4:c2:60:40	192.168.10.243	□	Edit □



DHCP Client Info Setting

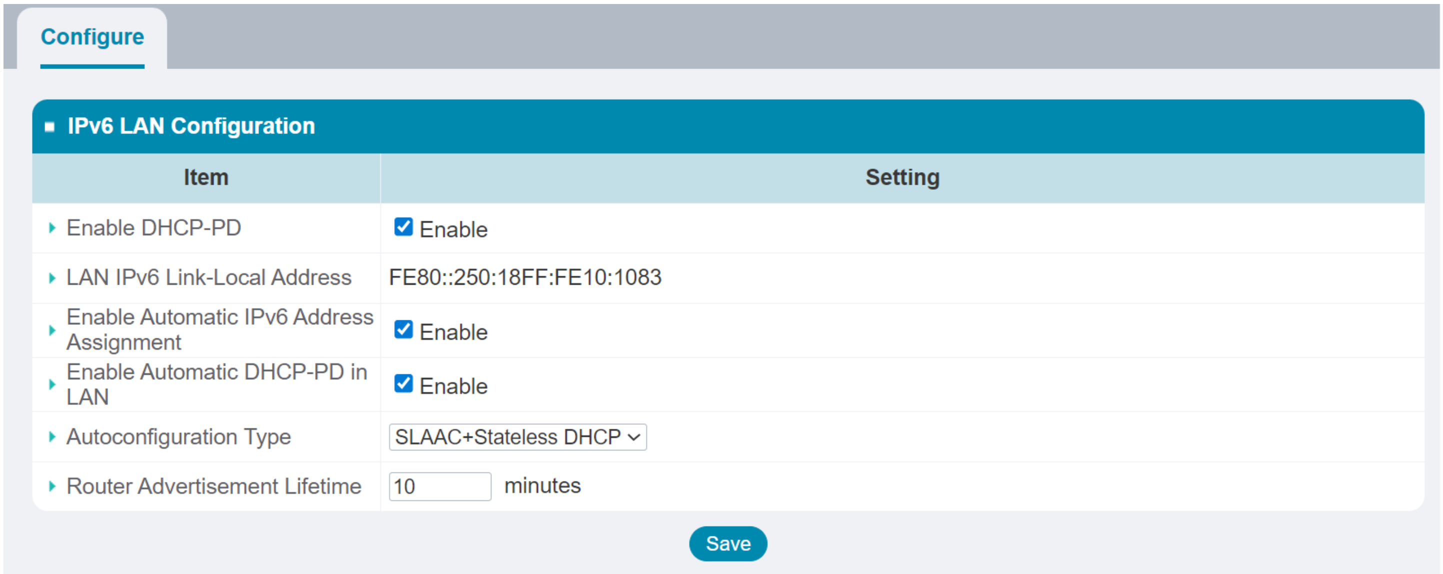
Item	Setting
Host Name	08636NBWIN11
MAC Address	f8:75:a4:c2:60:40
IP Address	192.168.10.243
IP/MAC Binding	□ Enable

The fields available on this page are as follows:

Field	Description
DHCP Server Name	Identifier for the DHCP server.
LAN IP Address	The IP address of the router on the local network (interface IP).
Subnet Mask	Defines the network portion of the IP address.
IP Pool	The range of IP addresses that the DHCP server can assign to clients.
Lease Time	Duration (in seconds) that an IP address is leased to a client. 604800 seconds equals 7 days. After this time, the lease expires unless renewed.
Domain Name	Optional domain name for the network. Used by DHCP clients to set their local domain.
Primary DNS	Optional. IP address of the primary DNS server that clients will use for domain name resolution.
Secondary DNS	Optional. IP address of the secondary DNS server for redundancy.
Primary WINS	Optional. IP address of the primary WINS server (used for NetBIOS name resolution, mostly in older Windows networks).
Secondary WINS	Optional. IP address of a backup WINS server.
Gateway	Optional. Default gateway for DHCP clients.

2.5 LANv6

This section allows you to configure IPv6 features for your Local Area Network (LAN), ensuring your internal network operates efficiently in an IPv6-supported environment.



IPv6 LAN Configuration

Item	Setting
Enable DHCP-PD	☑ Enable
LAN IPv6 Link-Local Address	FE80::250:18FF:FE10:1083
Enable Automatic IPv6 Address Assignment	☑ Enable
Enable Automatic DHCP-PD in LAN	☑ Enable
Autoconfiguration Type	SLAAC+Stateless DHCP
Router Advertisement Lifetime	10 minutes

The fields available on this page are as follows:

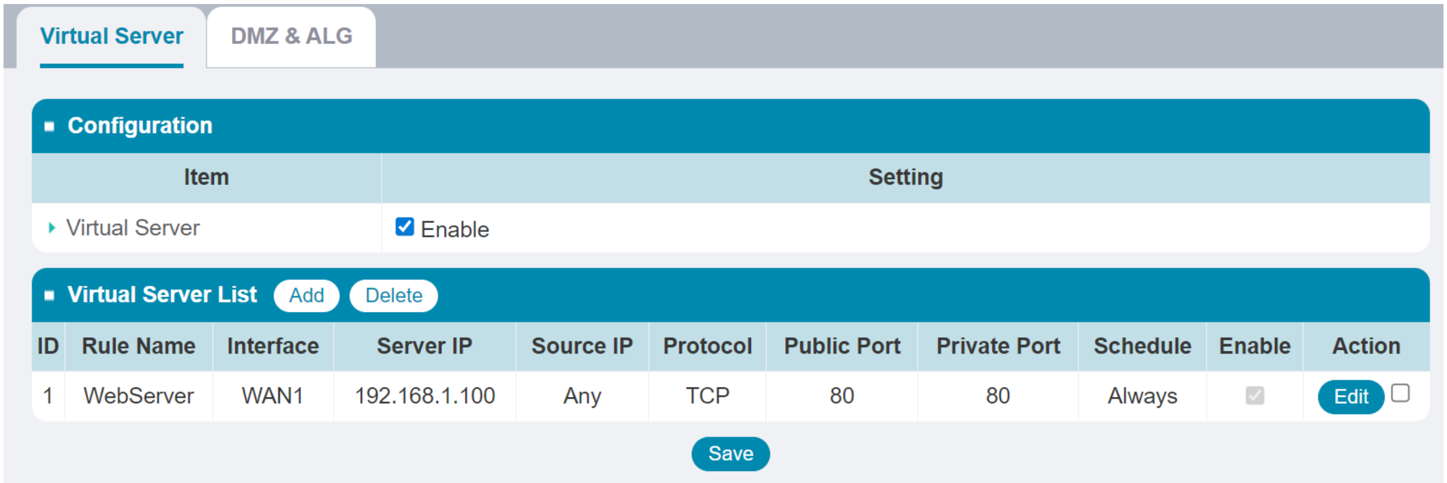
Field	Description
Enable DHCP-PD	Enables DHCP Prefix Delegation (DHCP-PD), allowing the router to receive an IPv6 prefix from the ISP and assign it to the LAN.
LAN IPv6 Link-Local Address	The IPv6 link-local address used by the LAN interface.
Enable Automatic IPv6 Address Assignment	Allows client devices to automatically assign themselves an IPv6 address using SLAAC (Stateless Address Autoconfiguration).
Enable Automatic DHCP-PD in LAN	Automatically applies the received delegated IPv6 prefix to the LAN side so that local devices can use globally routable IPv6 addresses.
Autoconfiguration Type	**SLAAC + RDNSS:** Auto-generates IPv6 address; DNS info is provided via router advertisements. **SLAAC + Stateless DHCP:** Auto-generates IPv6 address; extra settings like DNS are received from a DHCP server. **Stateful DHCPv6:** Both IPv6 address and settings are assigned by a DHCPv6 server.
Router Advertisement Lifetime	The duration (in minutes) that the router’s IPv6 advertisement remains valid. Devices use this to know how long to consider the router as their IPv6 gateway.

2.4 Port Fowarding

Port Forwarding is a network feature that allows external devices to access services on your local network through specific ports. It acts like a virtual gateway, directing incoming internet traffic to the correct device or application inside your private network.

2.4.1 Virtual Server

Virtual Server allows you to forward specific external ports to internal devices (servers) on your local network, enabling services like web hosting, FTP, or remote desktop.

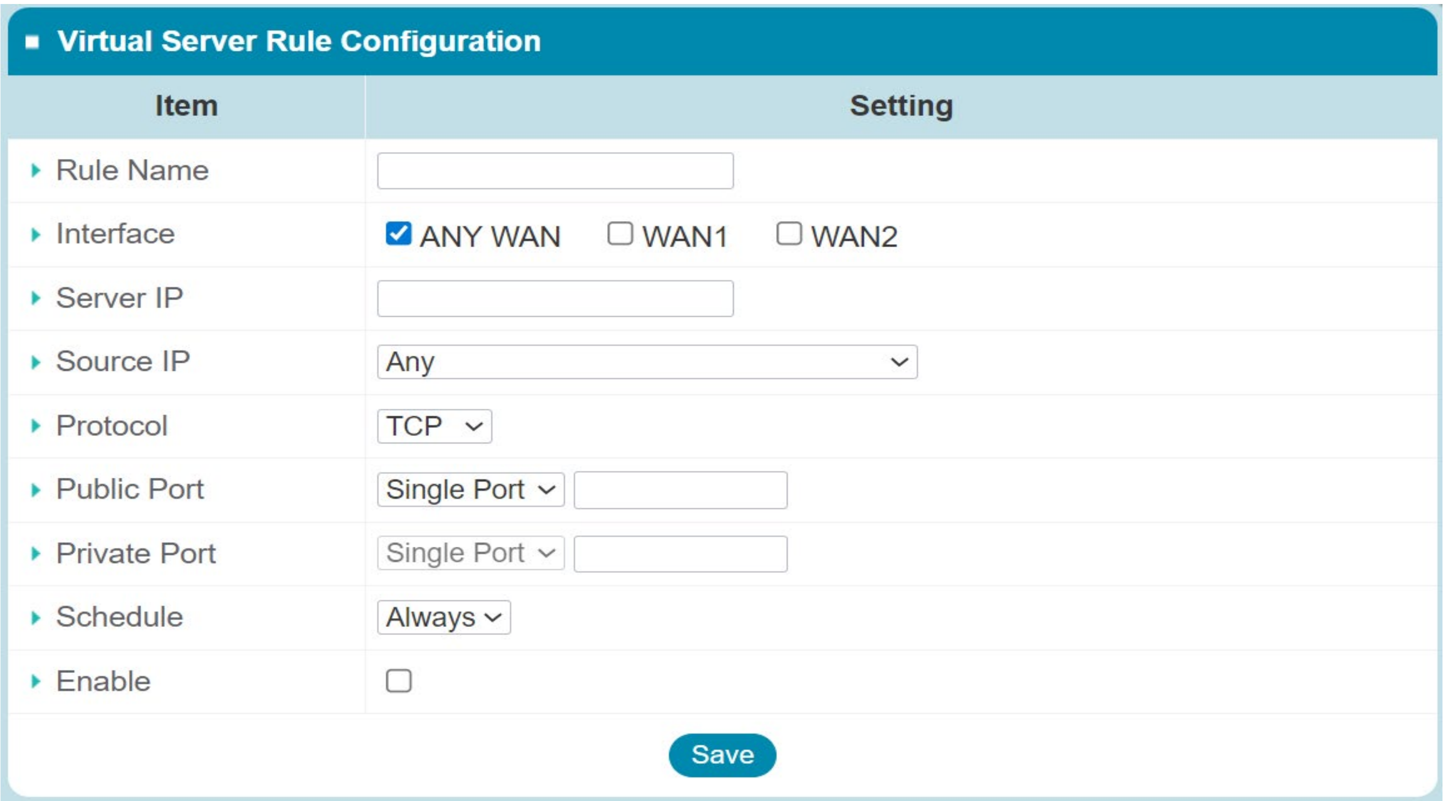


■ Configuration

Item	Setting
Virtual Server	☑ Enable

■ Virtual Server List Add Delete

ID	Rule Name	Interface	Server IP	Source IP	Protocol	Public Port	Private Port	Schedule	Enable	Action
1	WebServer	WAN1	192.168.1.100	Any	TCP	80	80	Always	☑	Edit □



■ Virtual Server Rule Configuration

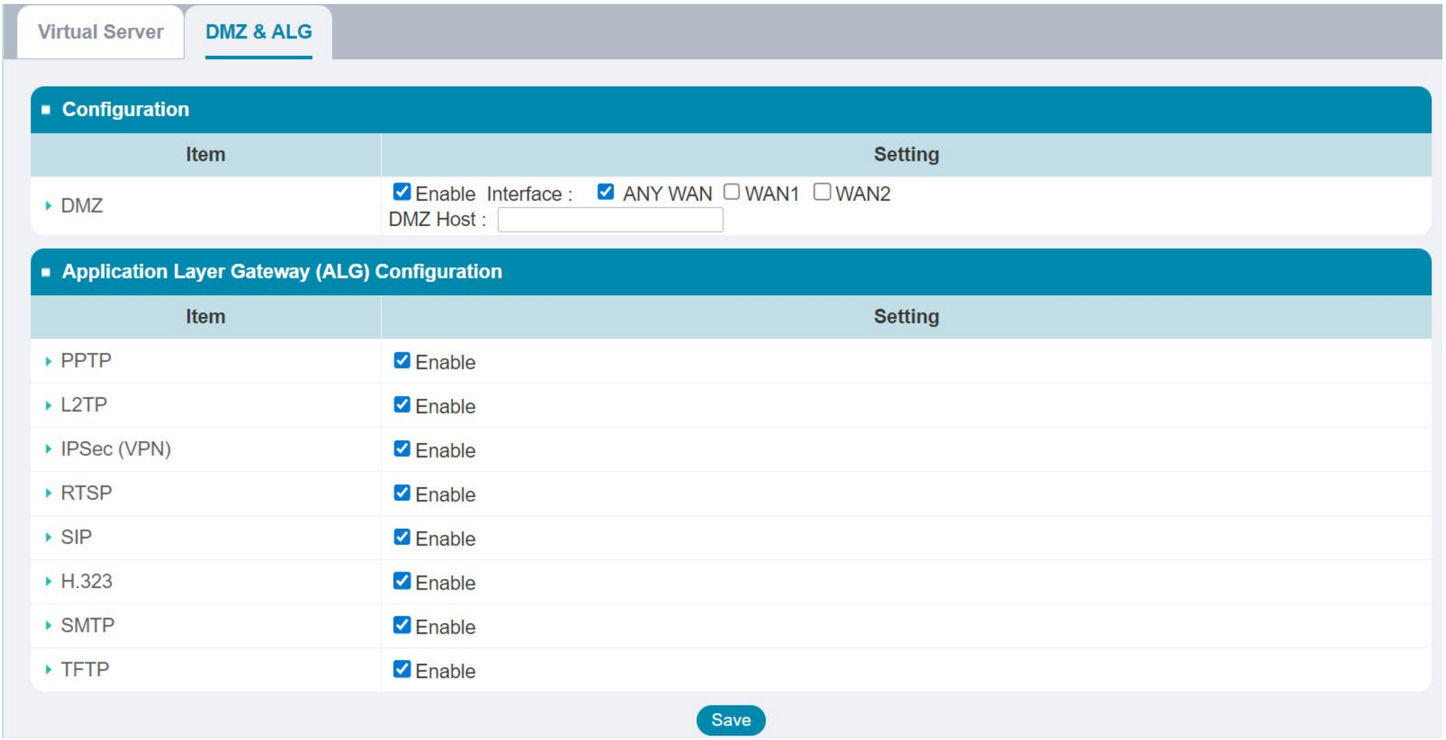
Item	Setting
Rule Name	
Interface	☑ ANY WAN □ WAN1 □ WAN2
Server IP	
Source IP	Any
Protocol	TCP
Public Port	Single Port
Private Port	Single Port
Schedule	Always
Enable	□

The fields available on this page are as follows:

Field	Description
Rule Name	Enter a name for your rule (e.g., WebServer, GameServer). Used for reference only.
Interface	Select which WAN interface this rule applies to.
Server IP	Enter the **local IP address** of the device you want to forward traffic to.
Source IP	Optional. Define which external IPs are allowed to access this rule. Use Any to allow all.
Protocol	Choose TCP, UDP, or Both depending on your service requirement.
Public Port	Enter the port number on the **WAN side** that will accept incoming requests.
Schedule	Select when this rule should be active.

2.4.2 DMZ & ALG

The DMZ function allows all unknown incoming internet traffic to be forwarded to a specific device (DMZ Host) on your local network. Use this feature only if you want one device (e.g. a game console or server) to be fully accessible from the internet.



Configuration

Item	Setting
DMZ	☑ Enable Interface : ☑ ANY WAN □ WAN1 □ WAN2 DMZ Host :

Application Layer Gateway (ALG) Configuration

Item	Setting
PPTP	☑ Enable
L2TP	☑ Enable
IPSec (VPN)	☑ Enable
RTSP	☑ Enable
SIP	☑ Enable
H.323	☑ Enable
SMTP	☑ Enable
TFTP	☑ Enable

The fields available on this page are as follows:

Field	Description

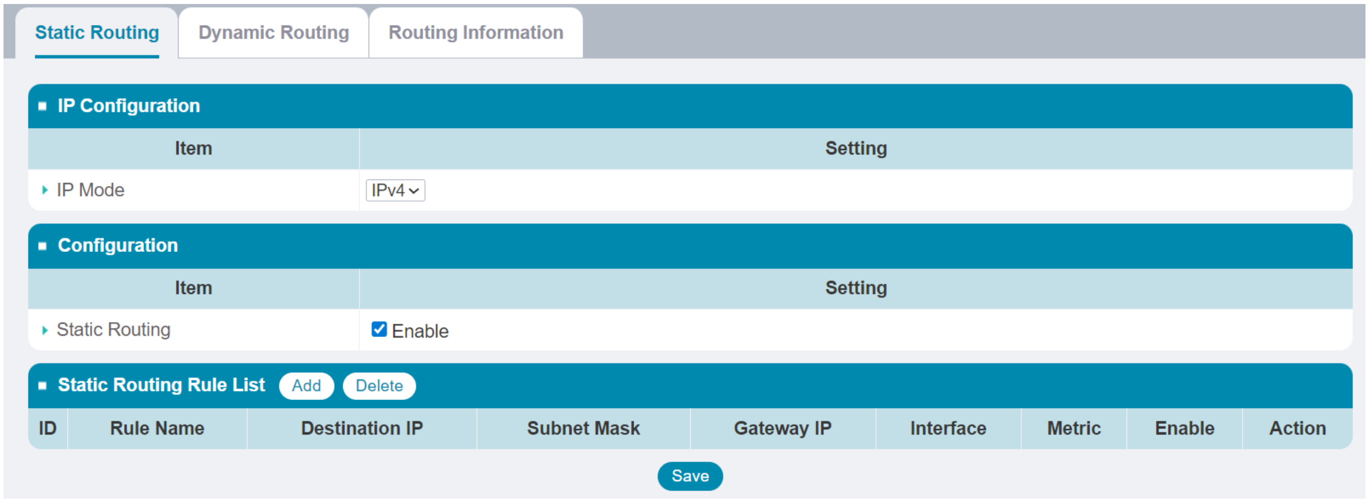
Interface	Choose which WAN interface applies. Select ANY WAN for general use.
DMZ Host	Enter the local IP address of the device to expose.
ALG Configuration	ALG helps certain applications (especially those using special ports or protocols) to work correctly through NAT.

2.5 Routing

If your network includes multiple routers and subnets, enable the routing function to allow communication between them. Routing determines the most efficient path for data to travel within the network.

2.5.1 Static Routing

Static Routing lets you manually set routing paths for specific devices or subnets. These routes are stored in the gateway's routing table and used to direct traffic accordingly.



■ IP Configuration

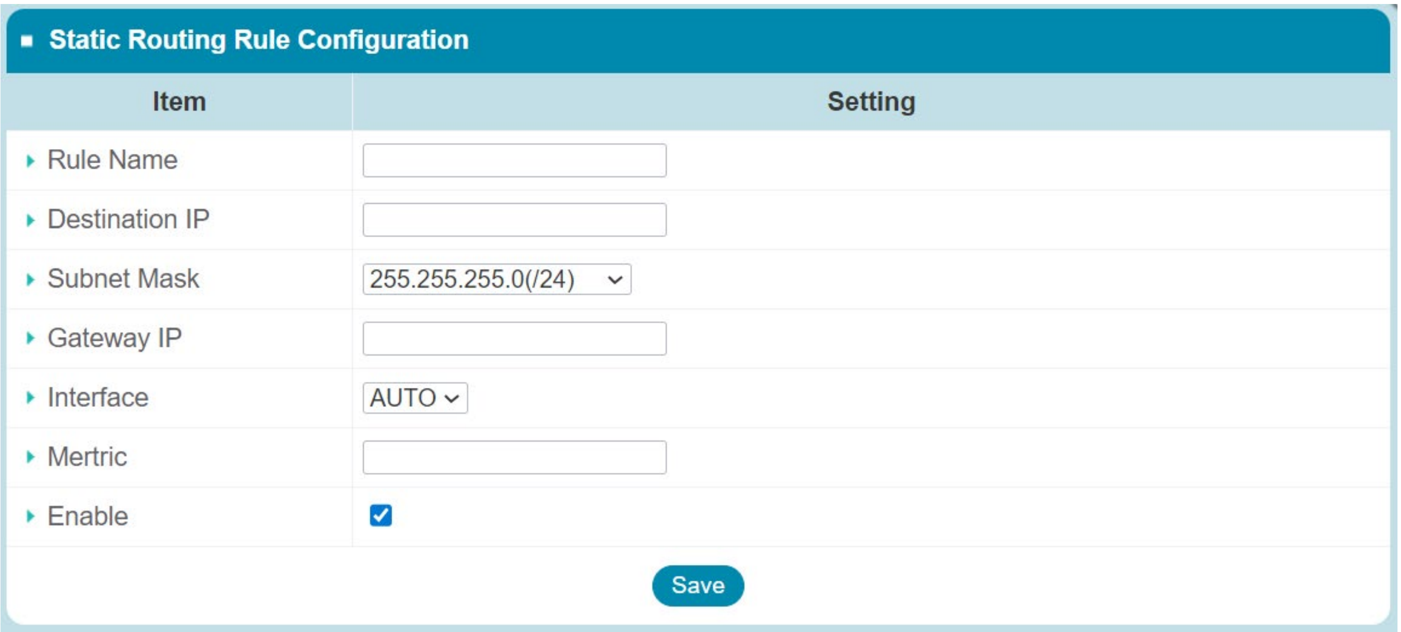
Item	Setting
IP Mode	IPv4

■ Configuration

Item	Setting
Static Routing	☑ Enable

■ Static Routing Rule List

ID	Rule Name	Destination IP	Subnet Mask	Gateway IP	Interface	Metric	Enable	Action



Static Routing Rule Configuration

Item	Setting
Rule Name	
Destination IP	
Subnet Mask	255.255.255.0(/24)
Gateway IP	
Interface	AUTO
Mertric	
Enable	☑

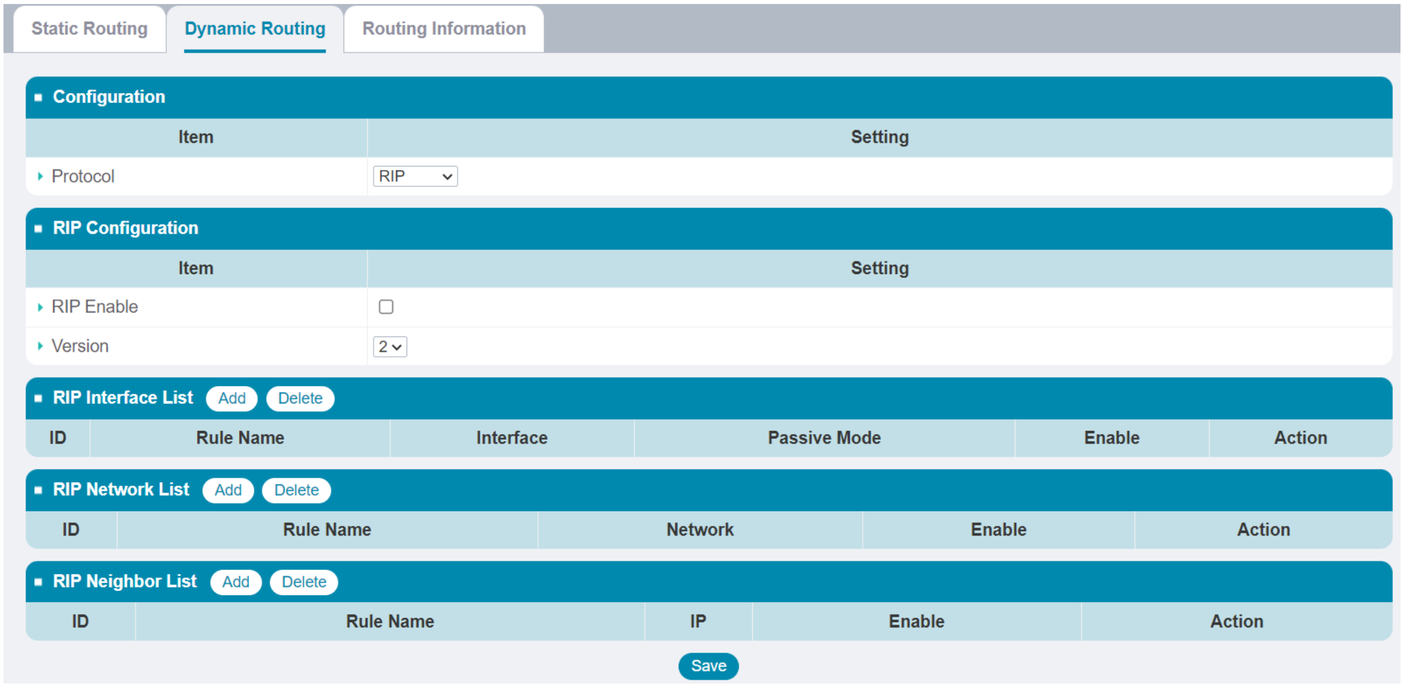
The fields available on this page are as follows:

Field	Description
Rule Name	A custom name to identify the routing rule.
Destination IP	The target network you want to reach.
Subnet Mask	Defines the size of the destination network.
Gateway IP	The next-hop router IP used to reach the destination.
Interface	Specifies the interface to use for routing.
Metric	Determines the priority of this route. Lower values mean higher priority.

2.5.2 Dynamic Routing

Dynamic Routing, also known as adaptive routing, enables the system to automatically update route paths in response to network changes such as congestion or outages. Common dynamic routing protocols include RIP (Routing Information Protocol) and OSPFv2 (Open Shortest Path First version 2).

2.5.2.1 RIP



Configuration

Item	Setting
Protocol	RIP

RIP Configuration

Item	Setting
RIP Enable	□
Version	2

RIP Interface List

ID	Rule Name	Interface	Passive Mode	Enable	Action

RIP Network List

ID	Rule Name	Network	Enable	Action

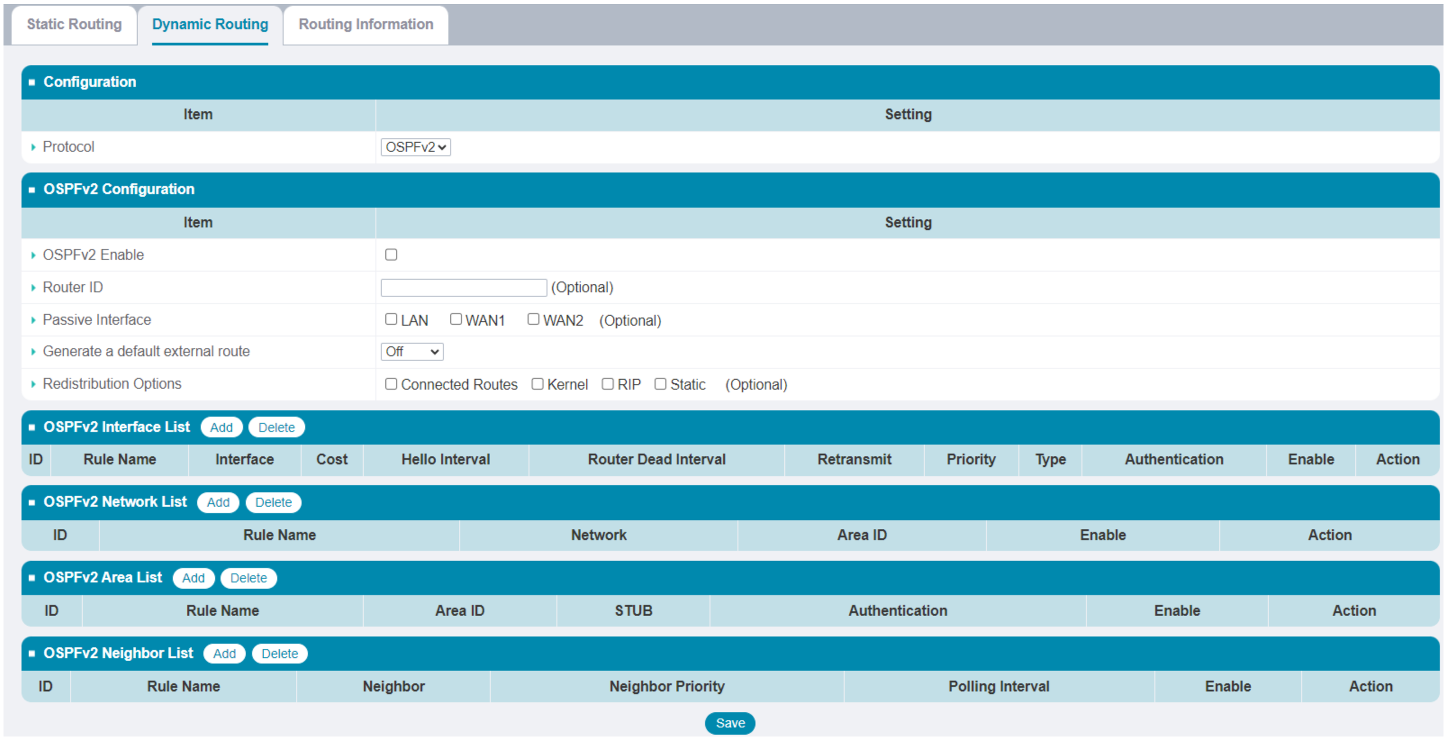
RIP Neighbor List

ID	Rule Name	IP	Enable	Action

The fields available on this page are as follows:

Field	Description
Version	Select the RIP version to use. RIP v2 is typically preferred due to support for subnet masks and authentication. **Version 1**: Supports only classful routing (no subnet masks). **Version 2**: Supports classless routing (CIDR), subnet masks, and multicast updates.
RIP Interface List	
RIP Interface List	Specifies which interfaces participate in RIP route advertisement and learning.
Rule Name	A custom name for the interface rule.
Interface	Select the interface on which RIP should operate.
Passive Mode	When enabled, RIP listens but does not send routing updates on this interface.
RIP Network List	
RIP Network List	Defines the internal IP networks to be advertised through RIP.
Rule Name	A custom name for the network rule.
Network	The IP network to be advertised (e.g., 192.168.1.0/24).
RIP Neighbor List	
RIP Neighbor List	Allows manual configuration of RIP neighbors (used in point-to-point or non-broadcast networks).
Rule Name	A custom name for identifying the neighbor rule.
IP	IP address of the neighboring RIP router.

2.5.2.2 OSPFv2



Configuration

Item	Setting
Protocol	OSPFv2

OSPFv2 Configuration

Item	Setting
OSPFv2 Enable	□
Router ID	(Optional)
Passive Interface	□ LAN □ WAN1 □ WAN2 (Optional)
Generate a default external route	Off
Redistribution Options	□ Connected Routes □ Kernel □ RIP □ Static (Optional)

OSPFv2 Interface List

ID	Rule Name	Interface	Cost	Hello Interval	Router Dead Interval	Retransmit	Priority	Type	Authentication	Enable	Action

OSPFv2 Network List

ID	Rule Name	Network	Area ID	Enable	Action

OSPFv2 Area List

ID	Rule Name	Area ID	STUB	Authentication	Enable	Action

OSPFv2 Neighbor List

ID	Rule Name	Neighbor	Neighbor Priority	Polling Interval	Enable	Action

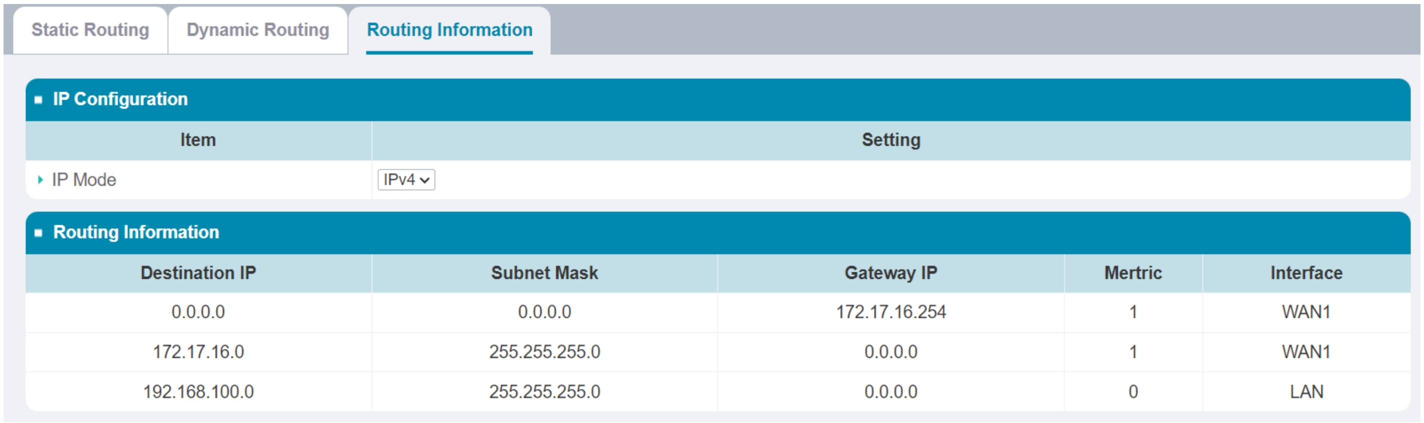
The fields available on this page are as follows:

Field	Description
Protocol	Selects the dynamic routing protocol to use.
OSPFv2 Configuration	
Router ID	Manually set the OSPF router ID. If left blank, the highest IP address of the active interfaces is used.
Passive Interface	Designates interfaces that will not send OSPF hello packets, but still advertise routes.
Generate a default external route	Determines whether to advertise a default route (0.0.0.0/0) to other OSPF routers.
Redistribution Options	Selects which route types will be redistributed into OSPF.
OSPFv2 Interface List	
OSPFv2 Interface List	Configures OSPF parameters on a per-interface basis. This section allows detailed control over how OSPF operates on each network port.
Rule Name	A custom name for the interface rule.
Interface	Specifies the physical or logical interface.
Cost	Sets the OSPF cost for the interface, used in route metric calculation. Lower values are preferred.
Hello Interval	Time (in seconds) between Hello packets sent by OSPF.
Router Dead Interval	Time before a neighbor is declared inactive after missing Hello packets.

Retransmit	Interval for retransmitting Link State Advertisements (LSAs).
Priority	Used to influence DR/BDR elections. A higher value increases the chance of becoming DR.
Type	Defines the OSPF network type (e.g., broadcast, non-broadcast).
Authentication	Enables authentication (plain text or cryptographic) for this interface.
OSPFv2 Network List	
OSPFv2 Network List	Defines which IP networks should be included in OSPF advertisements and maps them to their respective OSPF areas.
Rule Name	A custom name for the area rule.
Area ID	Identifies the OSPF area (e.g., 0.0.0.0 for backbone).
STUB	Marks the area as a stub, reducing routing overhead by limiting external routes.
Authentication	Enables authentication for the area.
OSPFv2 Neighbor List	
OSPFv2 Neighbor List	Allows for manual configuration of OSPF neighbors, primarily used in NBMA (Non-Broadcast Multi-Access) or point-to-multipoint environments where dynamic discovery is not available.
Rule Name	A custom name for identifying the neighbor rule.
Neighbor	IP address of the OSPF neighbor router
Neighbor Priority	DR/BDR election priority for the specified neighbor.
Polling Interval	Time interval (in seconds) for polling the neighbor.

2.5.3 Routing information

The routing information allows user to view the routing table and policy routing information.



IP Configuration

Item	Setting
IP Mode	IPv4

Routing Information

Destination IP	Subnet Mask	Gateway IP	Mertric	Interface
0.0.0.0	0.0.0.0	172.17.16.254	1	WAN1
172.17.16.0	255.255.255.0	0.0.0.0	1	WAN1
192.168.100.0	255.255.255.0	0.0.0.0	0	LAN

The fields available on this page are as follows:

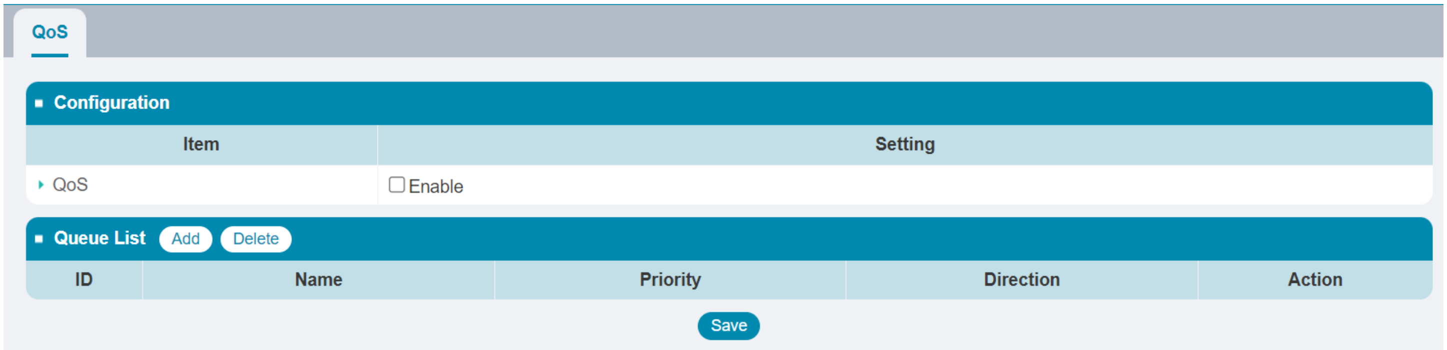
Field	Description
Destination IP	Routing record of Destination IP. IPv4 Format.
Subnet Mask	Routing record of Subnet Mask. IPv4 Format.
Gateway IP	Routing record of Gateway IP. IPv4 Format.
Metric	Routing record of Metric. Numeric String Format.
Interface	Routing record of Interface Type. String Format.

2.6 QoS

This gateway offers a wide range of flexible rules for configuring QoS (Quality of Service) policies. Before creating a policy, you should first identify three key elements:

1. **Who** needs to be managed? (e.g., specific devices, IP addresses, or user groups)
2. **What** type of service or traffic requires control? (e.g., video streaming, VoIP, gaming)
3. **How** should the traffic be prioritized? (e.g., high, medium, or low priority)

Once you have defined these elements, you can proceed to explore and configure the features available in this section in greater detail.



QoS

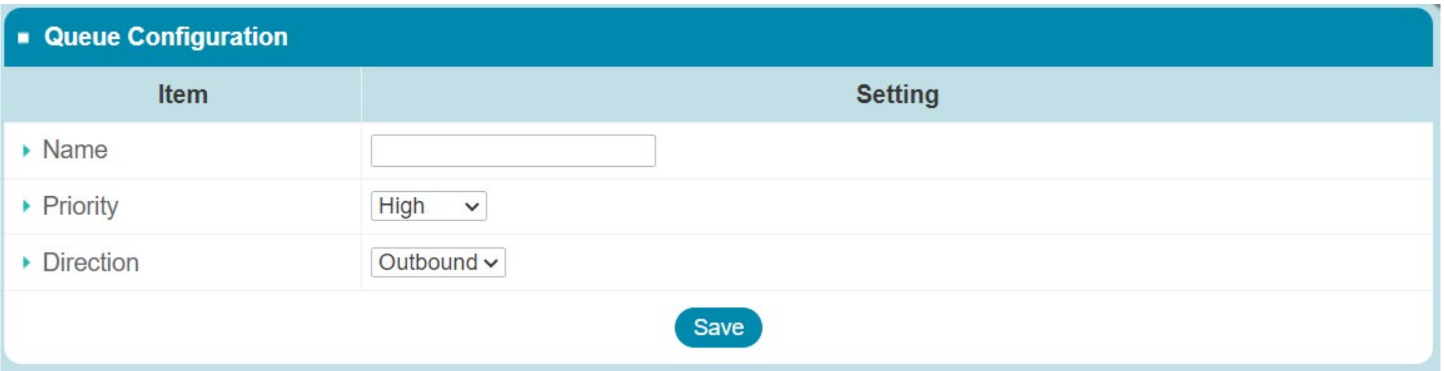
Configuration

Item	Setting
QoS	□ Enable

Queue List Add Delete

ID	Name	Priority	Direction	Action

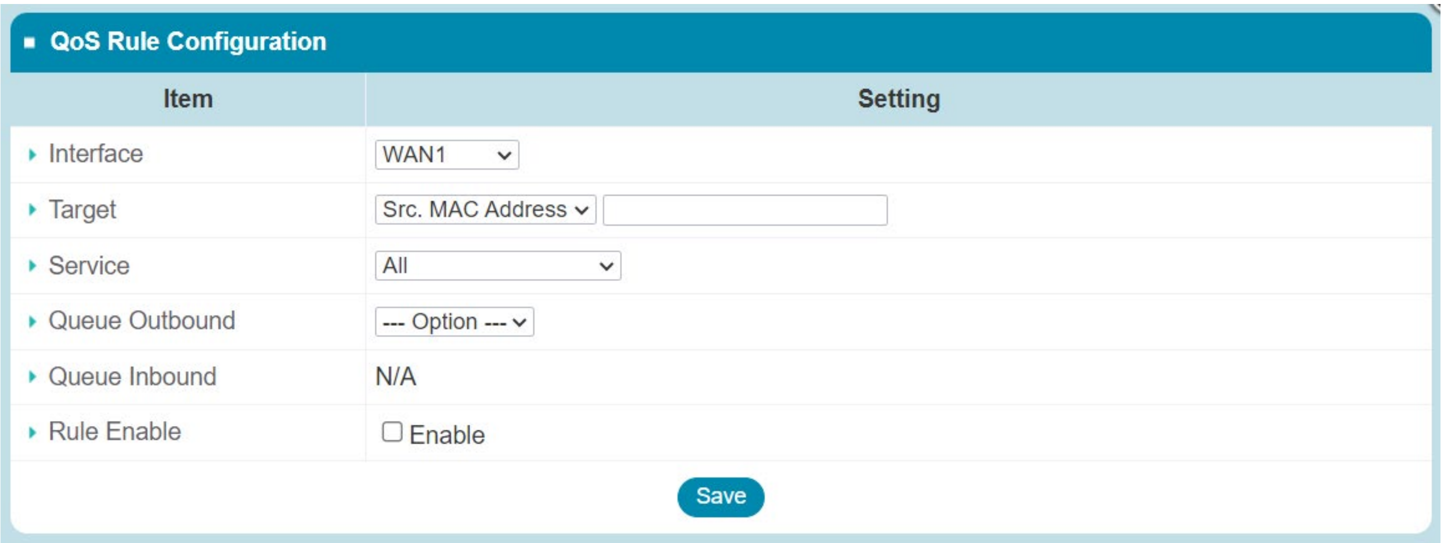
Save



Queue Configuration

Item	Setting
Name	
Priority	High
Direction	Outbound

Save



QoS Rule Configuration

Item	Setting
Interface	WAN1
Target	Src. MAC Address
Service	All
Queue Outbound	--- Option ---
Queue Inbound	N/A
Rule Enable	□ Enable

Save

The fields available on this page are as follows:

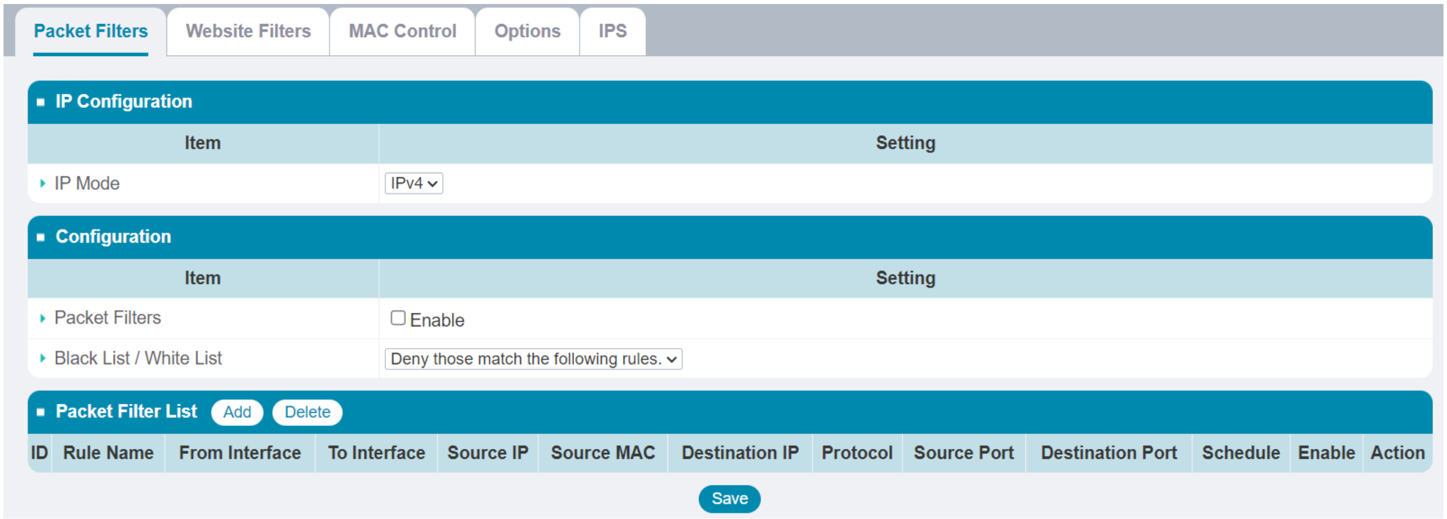
Field	Description
Queue List	
Queue List	Queues define how traffic is managed and prioritized. You can create multiple queues with different priorities to ensure critical services receive proper bandwidth.
Name	Specifies a unique name for the queue. Used for identification and management purposes.
Priority	Determines the priority level of the queue. High-priority queues are processed first.
Direction	Defines the traffic flow direction this queue applies to: - Outbound for upload traffic - Inbound for download traffic.
QoS Rule List	
QoS Rule List	These rules let you associate specific traffic types or devices with defined queues, ensuring that network resources are allocated based on your prioritization strategy.
Interface	Specifies the network interface (e.g., WAN1) to which the QoS rule will be applied.
Target	Defines the traffic target. The rule applies to the specified source MAC address.
Service	Specifies the type of service or protocol (e.g., HTTP, FTP) to be managed by the rule.
Queue Outbound	Assigns outbound traffic to a specific QoS queue to control priority or bandwidth.
Queue Inbound	Indicates that inbound queuing is not applicable or configurable on this device.

Chapter 3 Security

3.1 Firewall

The firewall functions include Packet Filter, URL Blocking, MAC Control, IPS and Certificates.

3.1.1 Packet Filters



■ IP Configuration

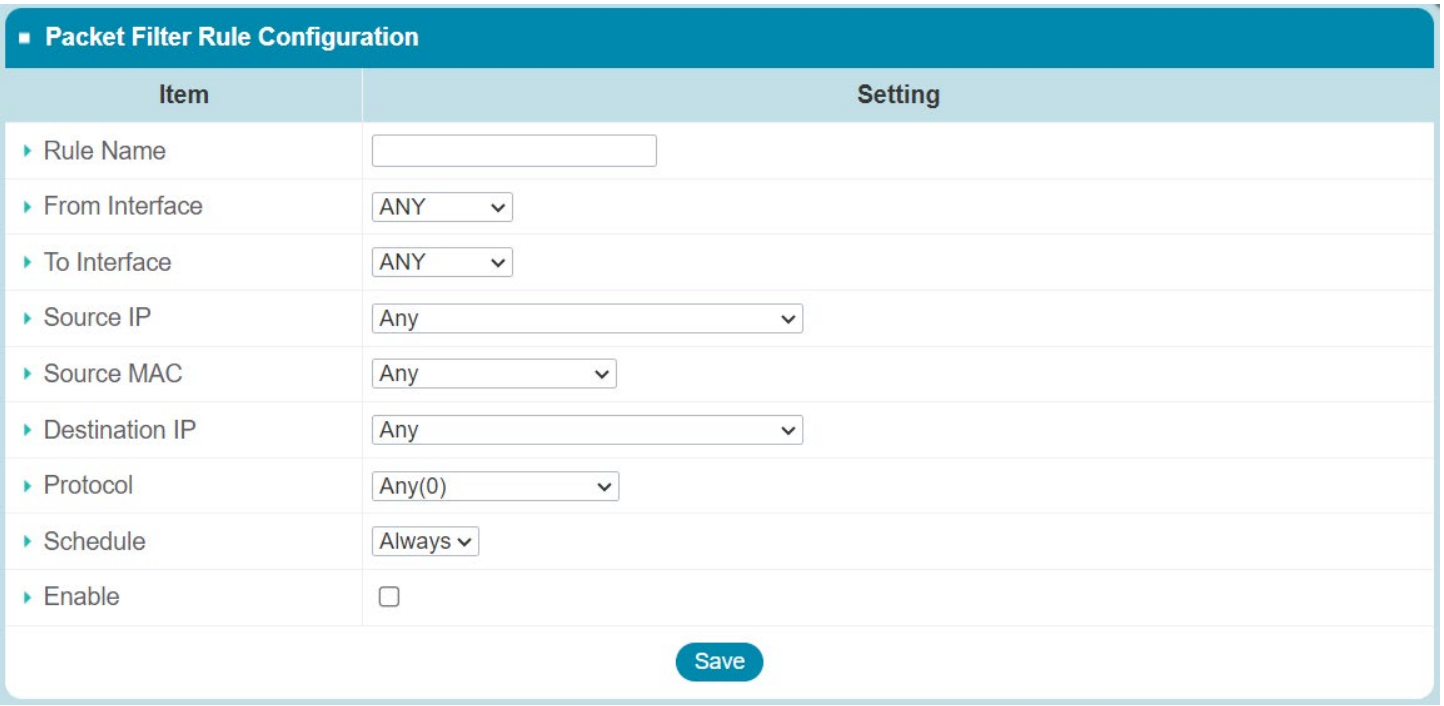
Item	Setting
IP Mode	IPv4

■ Configuration

Item	Setting
Packet Filters	☐ Enable
Black List / White List	Deny those match the following rules.

■ Packet Filter List

ID	Rule Name	From Interface	To Interface	Source IP	Source MAC	Destination IP	Protocol	Source Port	Destination Port	Schedule	Enable	Action


■ Packet Filter Rule Configuration

Item	Setting
Rule Name	
From Interface	ANY
To Interface	ANY
Source IP	Any
Source MAC	Any
Destination IP	Any
Protocol	Any(0)
Schedule	Always
Enable	☐

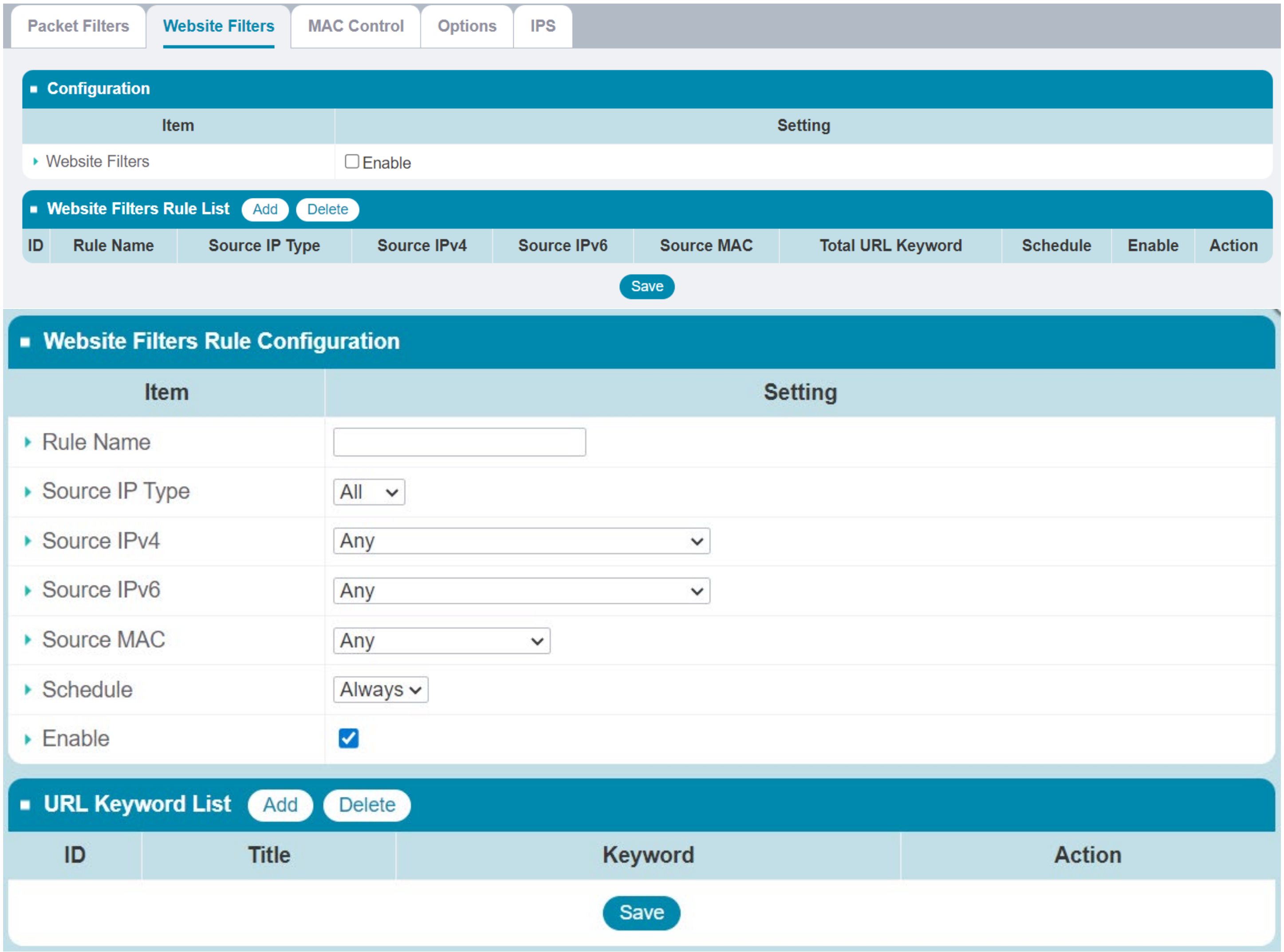
The fields available on this page are as follows:

Field	Description
Configuration	
Black List / White List	When Deny those match the following rules is selected, as the name suggest, packets specified in the rules will be blocked –black listed. In contrast, with Allow those match the following rules, you can specifically white list the packets to pass and the rest will be blocked.
Packet Filter List	
Rule Name	Specifies a unique name for the filtering rule for easier identification and

	management.
From Interface	Select the incoming network interface where the rule applies.
To Interface	Selects the outgoing network interface where the rule applies.
Source IP	Defines the source IP address to match packets from a specific sender.
Source MAC	Filters traffic based on the originating MAC address (layer 2 filtering).
Destination IP	Defines the destination IP address for traffic filtering
Protocol	Filters packets based on protocol type, e.g., TCP, UDP, or ICMP.
Schedule	Sets when the rule is active, allowing for time-based filtering (e.g., during work hours).

3.1.2 Website Filters

URL Blocking allows you to create rules to permit or block web requests based on full URLs, partial domain names, or specific keywords. You can filter traffic using domain suffixes (e.g., .com, .org) or keywords (e.g., “bct”, “mpe”). Each rule can include a target port and optional time schedule to control when the rule is active.



■ Configuration

Item	Setting
Website Filters	□ Enable

■ Website Filters Rule List

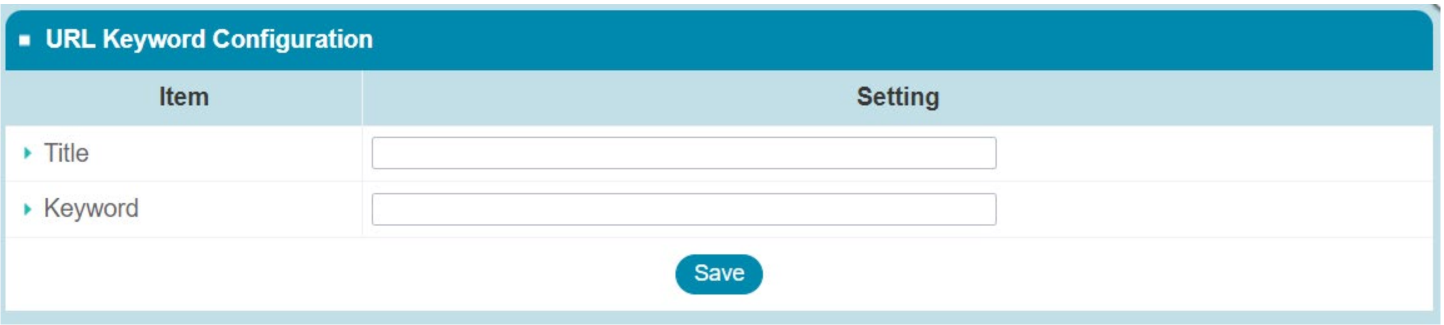
ID	Rule Name	Source IP Type	Source IPv4	Source IPv6	Source MAC	Total URL Keyword	Schedule	Enable	Action

■ Website Filters Rule Configuration

Item	Setting
Rule Name	
Source IP Type	All
Source IPv4	Any
Source IPv6	Any
Source MAC	Any
Schedule	Always
Enable	☑

■ URL Keyword List

ID	Title	Keyword	Action



URL Keyword Configuration

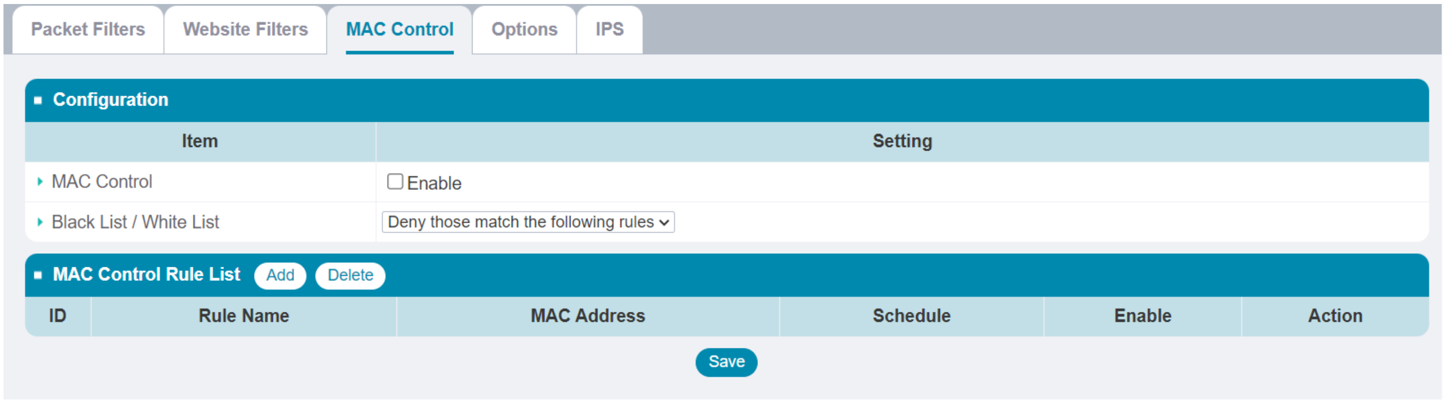
Item	Setting
Title	
Keyword	

The fields available on this page are as follows:

Field	Description
Website Filters Rule List	
Rule Name	A user-defined name to identify and manage the filter rule.
Source IP Type	Selects the type of source IP address the rule applies to.
Source IPv4	Filters requests based on the source IPv4 address.
Source IPv6	Filters requests based on the source IPv6 address.
Source MAC	This field is to specify the Source MAC address. ● Select Any to filter packets coming from any MAC addresses. ● Select Specific MAC Address to filter packets coming from a MAC address.
Schedule	Determines when the rule is active.
URL Keyword List	
Title	A user-defined label for the keyword rule, for easy identification.
Keyword	A keyword, partial domain, or URL string to be matched against web requests. applied.

3.1.3 MAC control

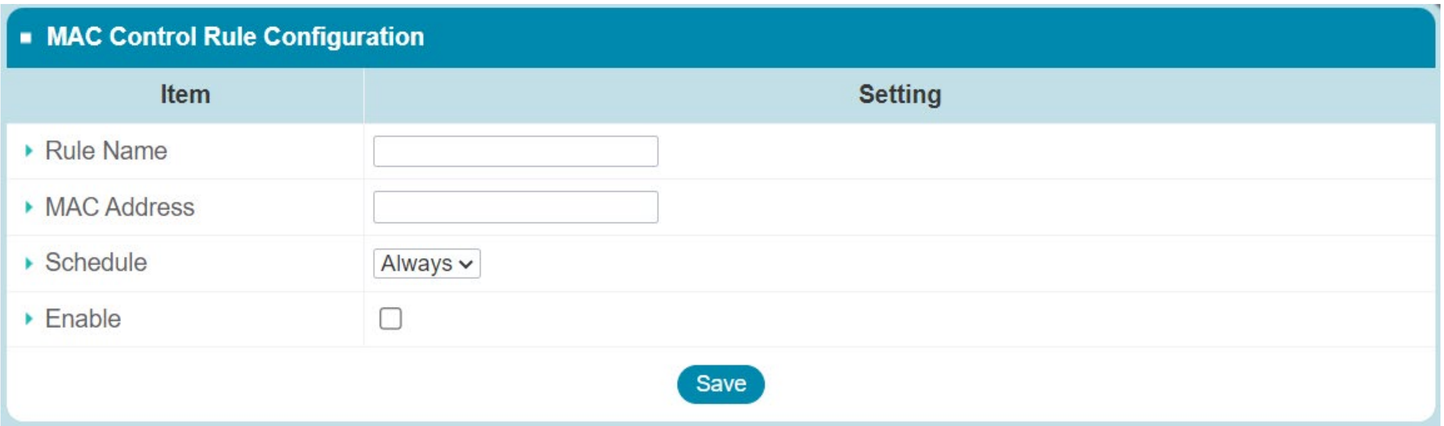
MAC Control allows the administrator to manage access to the gateway based on device MAC addresses.



Configuration

Item	Setting
MAC Control	☐ Enable
Black List / White List	Deny those match the following rules

ID	Rule Name	MAC Address	Schedule	Enable	Action



MAC Control Rule Configuration

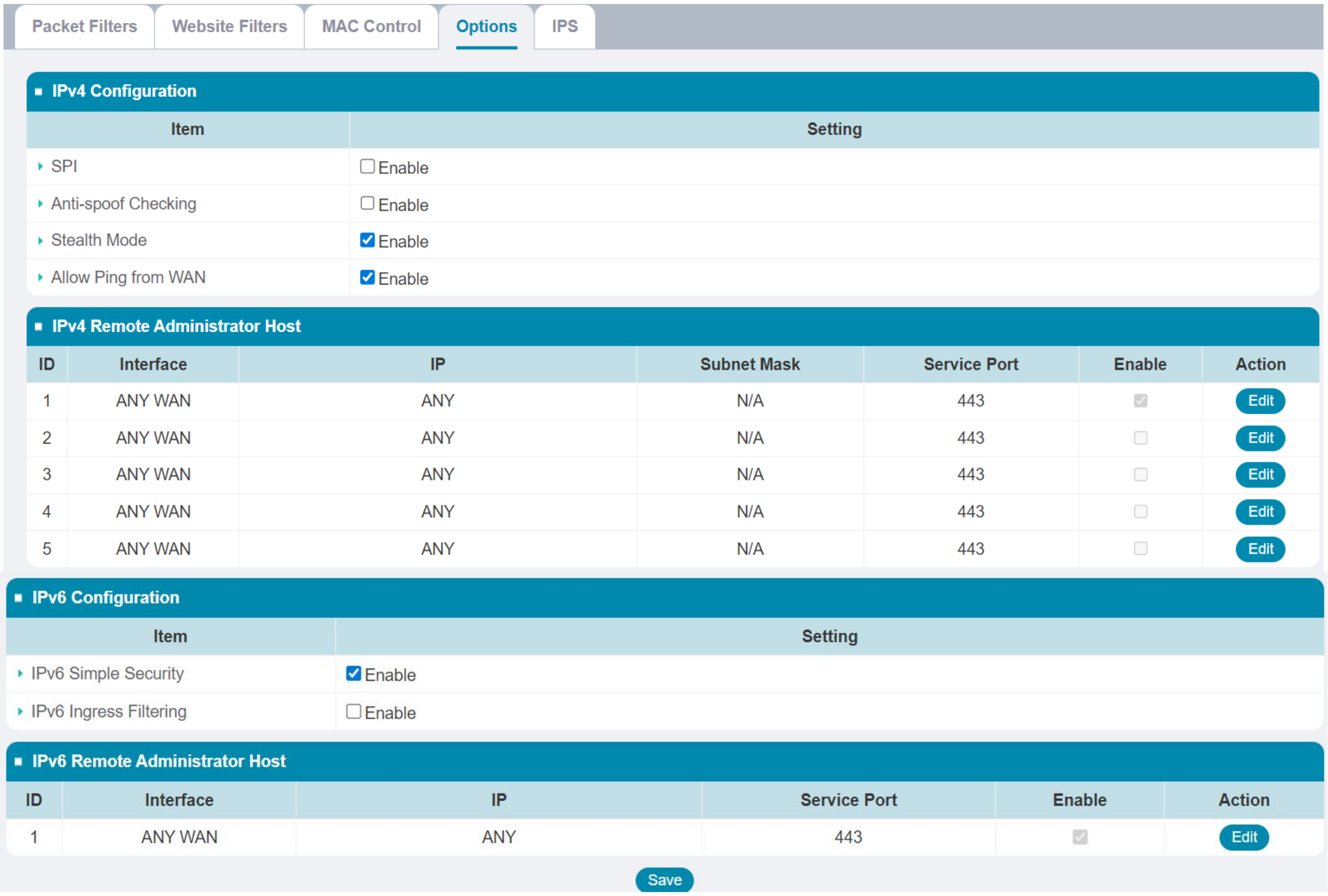
Item	Setting
Rule Name	
MAC Address	
Schedule	Always
Enable	□

The fields available on this page are as follows:

Field	Description
Black List / White List	Selects filtering mode: use rules to either deny (blacklist) or allow (whitelist) specific devices.
MAC Control Rule List	
Rule Name	User-defined name for identifying the rule.
MAC Address	Specifies the MAC address of the device to be allowed or denied network access.
Schedule	Defines the time interval during which the rule is active

3.1.4 Optional

SPI (Stateful Packet Inspection) monitors and verifies incoming packets based on connection state and packet information to ensure they are legitimate.



IPv4 Configuration

Item	Setting
SPI	□ Enable
Anti-spoof Checking	□ Enable
Stealth Mode	☑ Enable
Allow Ping from WAN	☑ Enable

IPv4 Remote Administrator Host

ID	Interface	IP	Subnet Mask	Service Port	Enable	Action
1	ANY WAN	ANY	N/A	443	☑	Edit
2	ANY WAN	ANY	N/A	443	□	Edit
3	ANY WAN	ANY	N/A	443	□	Edit
4	ANY WAN	ANY	N/A	443	□	Edit
5	ANY WAN	ANY	N/A	443	□	Edit

IPv6 Configuration

Item	Setting
IPv6 Simple Security	☑ Enable
IPv6 Ingress Filtering	□ Enable

IPv6 Remote Administrator Host

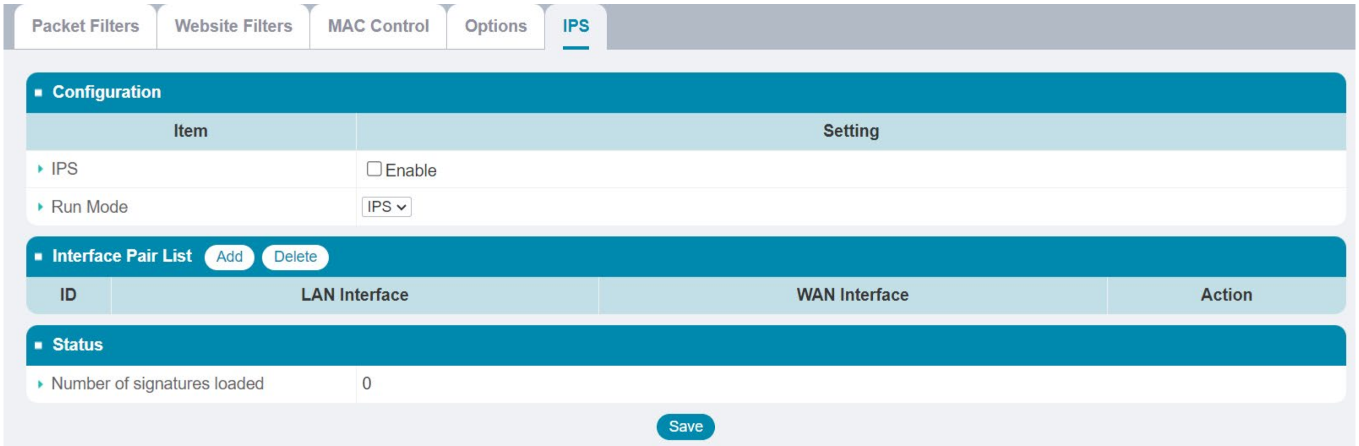
ID	Interface	IP	Service Port	Enable	Action
1	ANY WAN	ANY	443	☑	Edit

The fields available on this page are as follows:

Field	Description
IPv4 Configuration	
SPI	Enables Stateful Packet Inspection (SPI) to filter incoming packets and enhance security.
Anti-spoof Checking	Verifies the source IP address of incoming packets to prevent IP spoofing attacks.
Stealth Mode	Prevents the router from responding to unsolicited connection attempts (e.g., port scans).
Allow Ping from WAN	Allows the router to respond to ICMP ping requests from external WAN sources.
IPv4 Remote Administrator Host	
Interface	Specifies which WAN interface allows remote admin access.
IP	Specifies the remote IP address allowed to access the device for administration.
Subnet Mask	Defines the subnet for the allowed IP (not used when IP is set to ANY).
Service Port	Defines the port number used for remote access (e.g., HTTPS over port 443).
IPv6 Configuration	
IPv6 Simple Security	Enables basic protection for IPv6 connections by blocking unsolicited inbound traffic.
IPv6 Ingress Filtering	Filters incoming IPv6 traffic to ensure packets are from legitimate sources.
IPv6 Remote Administrator Host	

Interface	Specifies which WAN interface accepts remote admin access.
IP	Specifies the remote IPv6 address allowed to access the device for administration.
Service Port	Indicates the port used for remote access (commonly HTTPS port 443).

3.1.5 IPS



Configuration

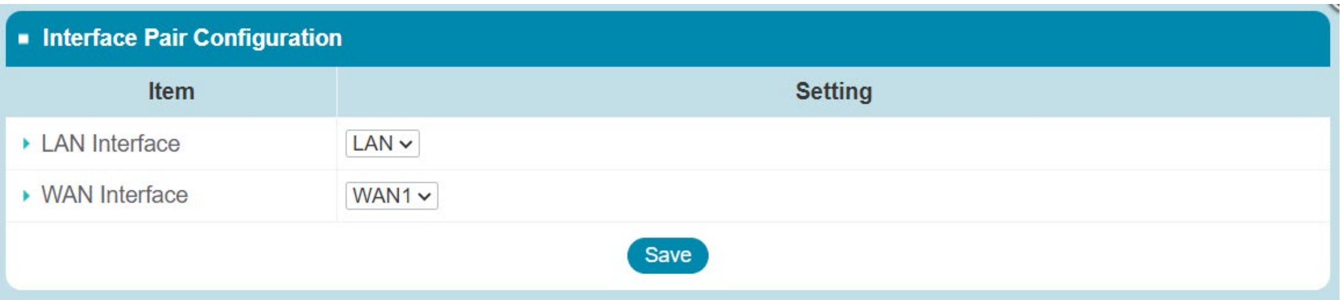
Item	Setting
IPS	☐ Enable
Run Mode	IPS

Interface Pair List

ID	LAN Interface	WAN Interface	Action

Status

Number of signatures loaded	0



Interface Pair Configuration

Item	Setting
LAN Interface	LAN
WAN Interface	WAN1

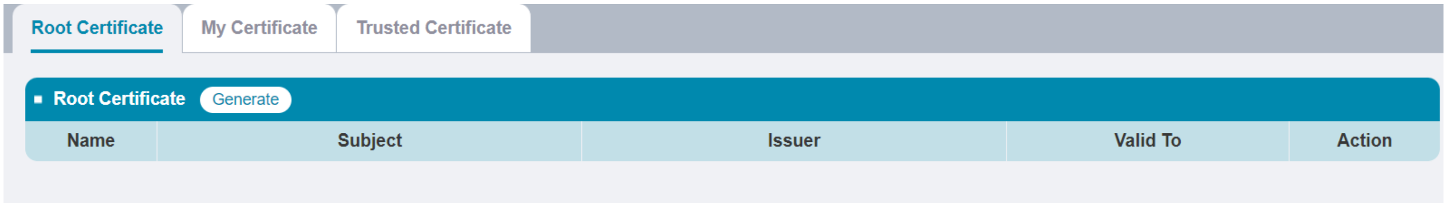
The fields available on this page are as follows:

Field	Description
Run Mode	Specifies the operation mode: IPS (Intrusion Prevention) actively blocks, IDS (Detection only) logs alerts but does not block.
Interface Pair List	
LAN Interface	Specifies the internal network interface for monitoring (e.g., LAN1, VLAN).
WAN Interface	Specifies the external interface that connects to the Internet (e.g., WAN1, WAN2).
Number of signatures loaded	Shows how many IPS signatures have been successfully loaded into the system for detection.

3.2 Certification

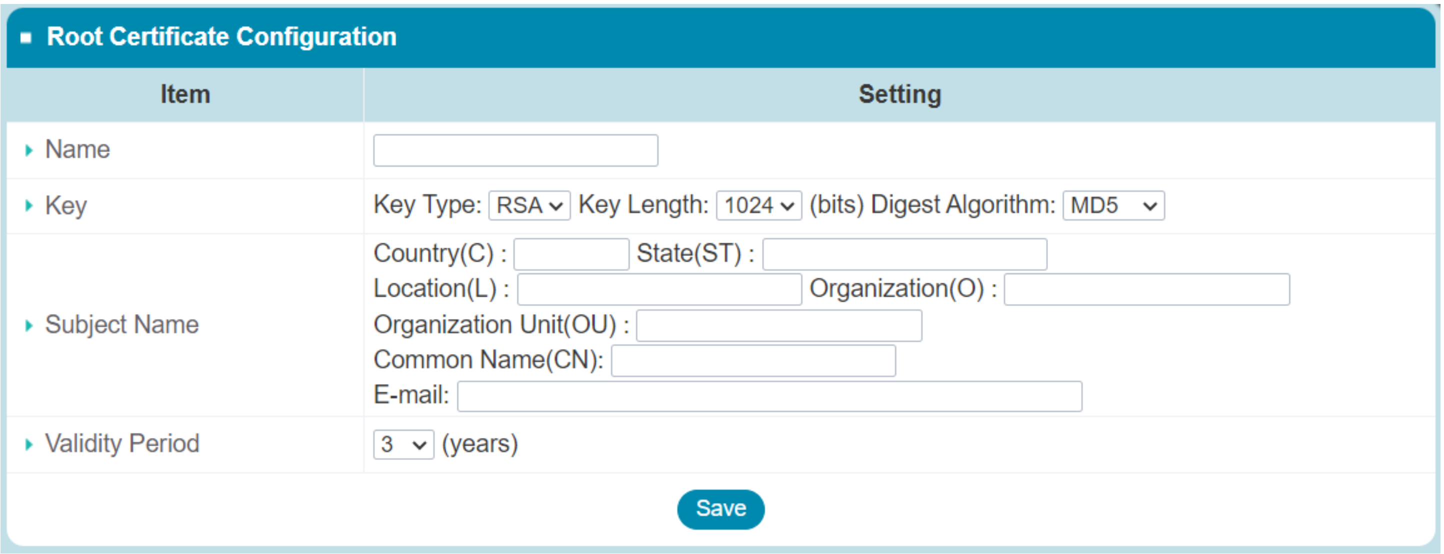
The certificate feature is used to enable secure communication and identity verification between devices or users. It allows the system to prove its authenticity and establish trust using digital certificates.

3.2.1 Root Certificate



▪ Root Certificate

Name	Subject	Issuer	Valid To	Action



▪ Root Certificate Configuration

Item	Setting
Name	
Key	Key Type: RSA Key Length: 1024 (bits) Digest Algorithm: MD5

Subject Name	Country(C) : State(ST) :
	Location(L) : Organization(O) :
	Organization Unit(OU) :
	Common Name(CN):
	E-mail:

Validity Period	3 (years)

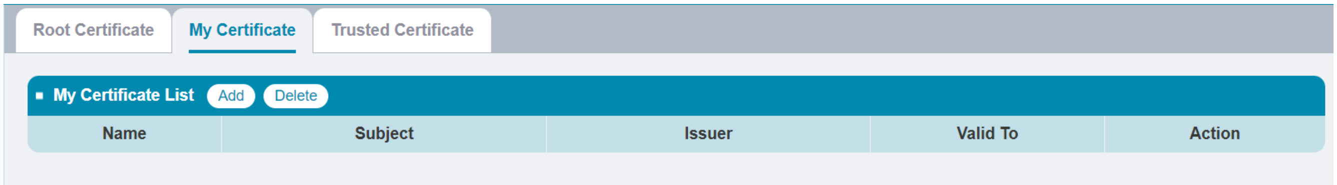
The fields available on this page are as follows:

Field	Description
Name	Selects filtering mode: use rules to either deny (blacklist) or allow (whitelist) specific devices.
Key Type	Specifies the cryptographic algorithm for key generation. RSA is the most common.
Key Length	Defines the strength of the key. Higher values offer stronger security but slower performance.
Digest Algorithm	Determines the hash algorithm used to sign the certificate. SHA-256 is recommended for modern security.
Country (C)	ISO code representing the country where the organization is located.
State (ST)	The full name of the state or province.
Location (L)	The city or locality where the organization is based.
Organization (O)	The legal name of the organization issuing the certificate.
Organizational Unit (OU)	A department or division within the organization (e.g., IT Department).
Common Name (CN)	Usually the domain name (e.g., www.example.com) or server name for which the certificate is issued.

E-mail	Email address of the certificate administrator or contact person.
Validity Period	Duration the certificate will be valid before expiration.

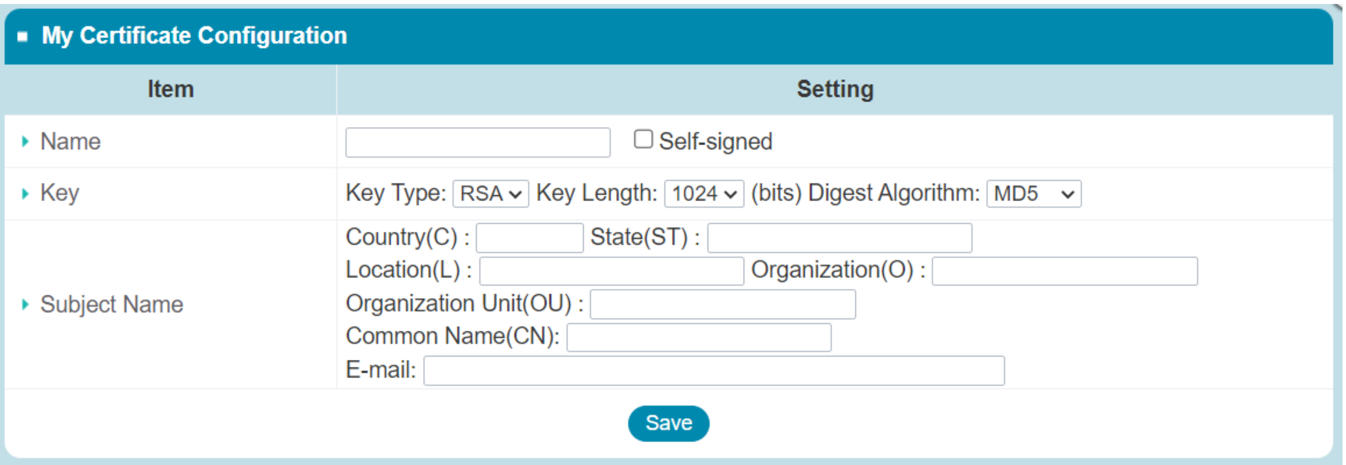
3.2.2 My Certificate

The My Certificate List displays all certificates generated by the gateway's built-in Root Certificate Authority (CA). It also stores Certificate Signing Requests (CSRs) that have been created for submission to external CAs. Once signed by an external CA, these certificates can be imported and recognized as local certificates on the gateway.



My Certificate List

Name	Subject	Issuer	Valid To	Action



My Certificate Configuration

Item	Setting
Name	□ Self-signed
Key	Key Type: RSA Key Length: 1024 (bits) Digest Algorithm: MD5

Subject Name	Country(C) : State(ST) :
	Location(L) : Organization(O) :
	Organization Unit(OU) :
	Common Name(CN):
	E-mail:

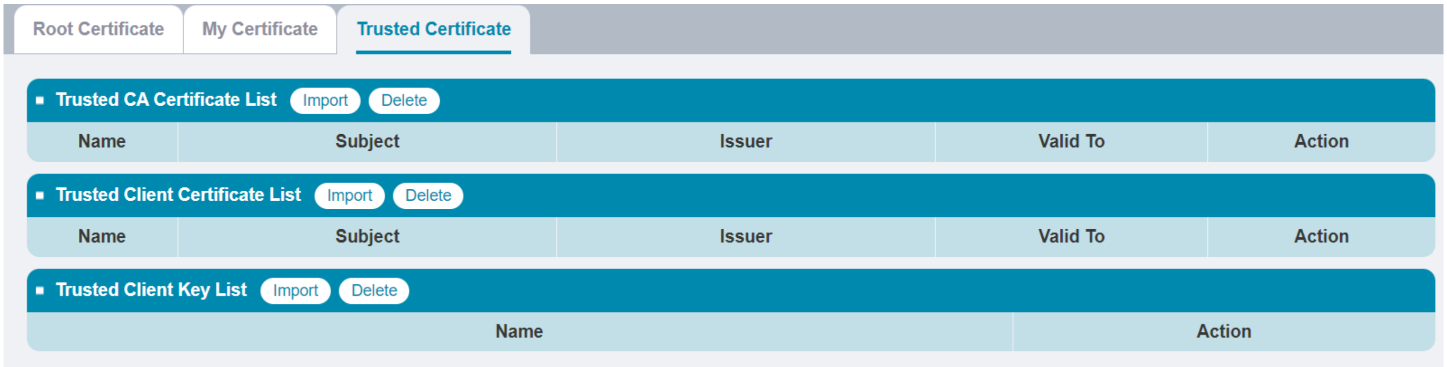
The fields available on this page are as follows:

Field	Description
Name	Selects filtering mode: use rules to either deny (blacklist) or allow (whitelist) specific devices.
Self-signed	If checked, the certificate will be self-signed (signed by itself), typically used for internal or testing purposes.
Key Type	Specifies the cryptographic algorithm for key generation. RSA is the most common.
Key Length	Defines the strength of the key. Higher values offer stronger security but slower performance.
Digest Algorithm	Determines the hash algorithm used to sign the certificate. SHA-256 is recommended for modern security.
Country (C)	ISO code representing the country where the organization is located.
State (ST)	The full name of the state or province.
Location (L)	The city or locality where the organization is based.
Organization (O)	The legal name of the organization issuing the certificate.
Organizational Unit (OU)	A department or division within the organization (e.g., IT Department).
Common Name (CN)	Usually the domain name (e.g., www.example.com) or server name for which

	the certificate is issued.
E-mail	Email address of the certificate administrator or contact person.

3.2.3 Trusted Certificate

The Trusted Certificate section allows you to manage certificates that your system recognizes as trustworthy. These include certificates from trusted Certificate Authorities (CAs) and trusted client certificates for mutual authentication. It also manages associated client keys used for identity verification.



Name	Subject	Issuer	Valid To	Action

Name	Subject	Issuer	Valid To	Action

Name	Action

The fields available on this page are as follows:

Field	**Description**
Trusted CA Certificate List	
Import	Upload a trusted CA certificate in PEM or DER format. These are used to validate server or client certificates signed by this CA.
Delete	Remove selected CA certificates from the trusted list.
Name	Internal reference name for the CA certificate.
Subject	The distinguished name (DN) of the CA that owns the certificate.
Issuer	The entity that issued the certificate (often the same as the subject if self-signed).
Valid To	Expiration date of the certificate.
Trusted Client Certificate List	
Import	Upload client certificates to enable mutual authentication (e.g., in VPN or secure management).
Delete	Remove selected client certificates from the trusted list.
Name	Identifier for the client certificate.
Subject	Identity of the client (Distinguished Name).
Issuer	The authority that signed the client certificate.
Valid To	Expiration date of the certificate.
Trusted Client Key List	
Import	Upload private key files corresponding to trusted client certificates. Required for authentication.
Delete	Remove selected private keys.

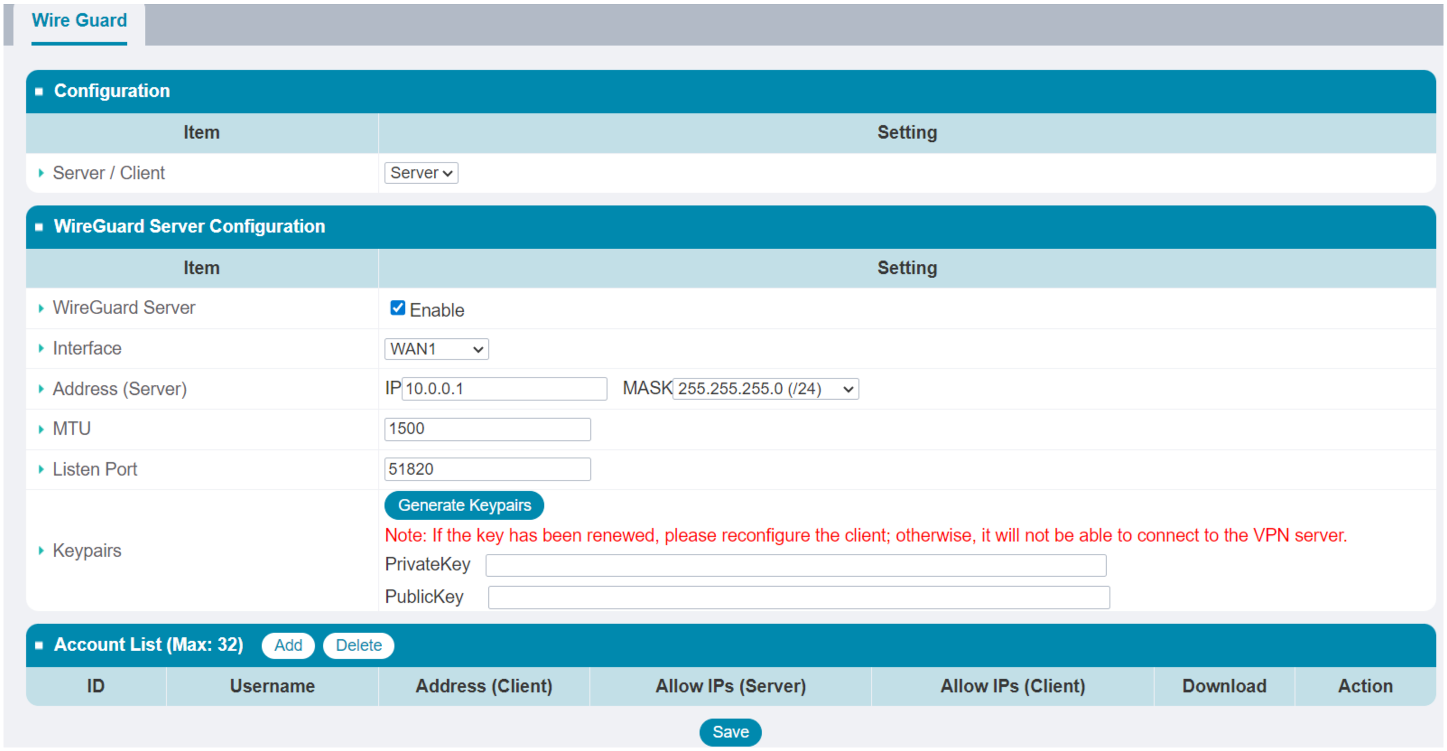
Name	Name or label for the private key.

Chapter 4 VPN

A Virtual Private Network (VPN) allows devices to securely connect to a private network over a public network like the Internet. It enables data to be transmitted as if the devices were physically connected to the same private network.

4.1 WireGuard

4.1.1 WireGuard Server



Wire Guard

■ Configuration

Item	Setting
Server / Client	Server

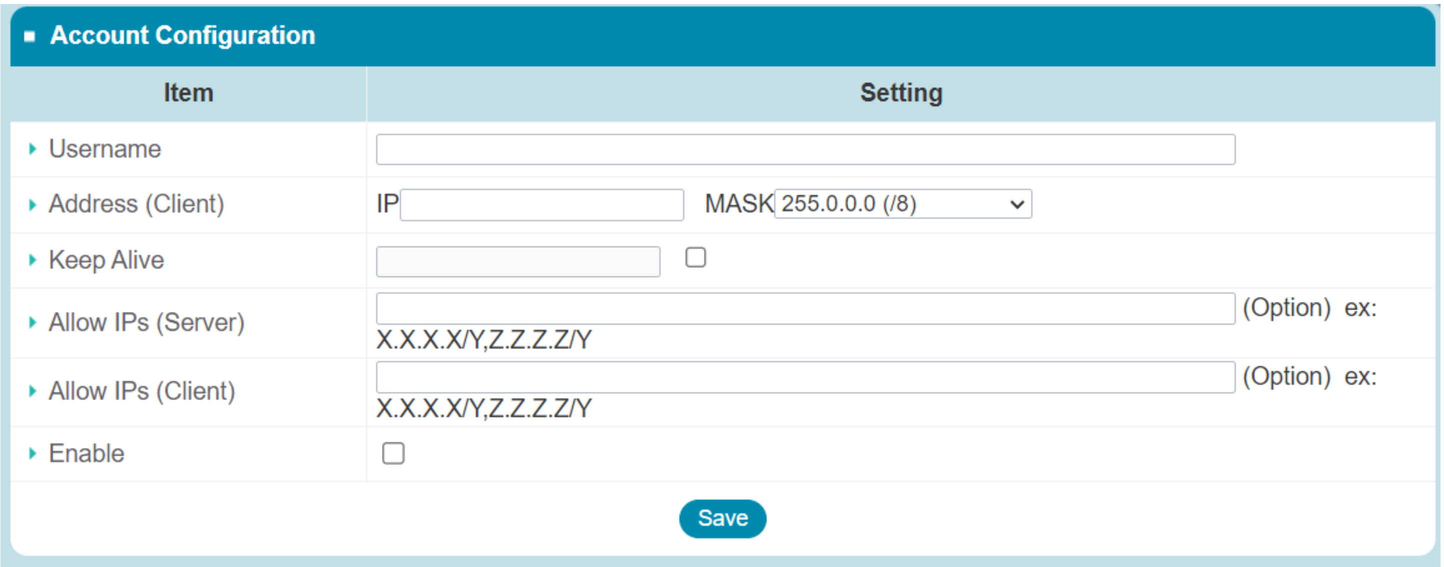
■ WireGuard Server Configuration

Item	Setting
WireGuard Server	☑ Enable
Interface	WAN1
Address (Server)	IP 10.0.0.1 MASK 255.255.255.0 (/24)
MTU	1500
Listen Port	51820
Keypairs	Generate Keypairs Note: If the key has been renewed, please reconfigure the client; otherwise, it will not be able to connect to the VPN server. PrivateKey PublicKey

■ Account List (Max: 32) Add Delete

ID	Username	Address (Client)	Allow IPs (Server)	Allow IPs (Client)	Download	Action

Save



Account Configuration

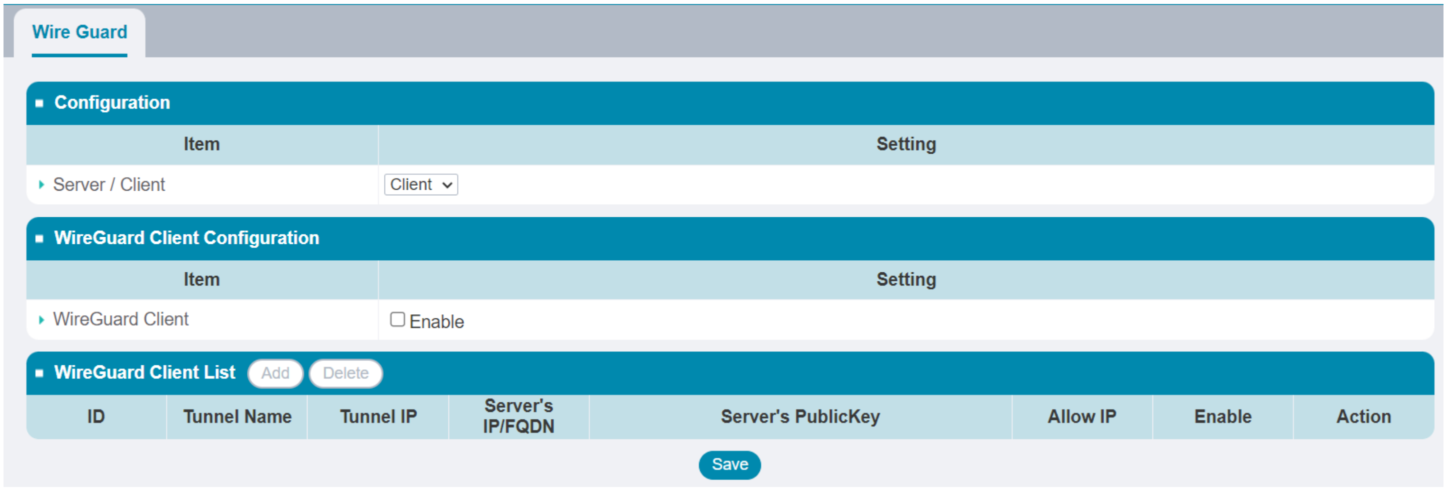
Item	Setting
Username	
Address (Client)	IP MASK 255.0.0.0 (/8)
Keep Alive	□
Allow IPs (Server)	(Option) ex: X.X.X.X/Y,Z.Z.Z.Z/Y
Allow IPs (Client)	(Option) ex: X.X.X.X/Y,Z.Z.Z.Z/Y
Enable	□

The fields available on this page are as follows:

Field	Description
Server / Client	Select the role of the device. Set to Server to host a WireGuard VPN for incoming client connections.
Interface	Selects the WAN interface that the server listens on for incoming VPN connections.
Address (Server)	Internal reference name for the CA certificate.
MTU	Sets the Maximum Transmission Unit size for VPN packets. Usually defaults to 1420–1500.
Listen Port	Specifies the UDP port on which the WireGuard server listens for connections.
Keypairs	Generated key pair used for encrypting VPN traffic. Clients must use the public key. (Changing the key pair requires reconfiguration on the client side.)
Account List	
Username	Name assigned to each client account.
Address (Client)	The static VPN IP address assigned to this client.
Keep Alive	Sets an optional interval (in seconds) for persistent keep-alive messages to maintain NAT traversal.
Allow IPs (Server)	Understanding AllowedIPs: **Routing:** When a peer sends a packet, WireGuard checks if the destination IP address is in the peer's "AllowedIPs" list. If it is, the packet is routed through the WireGuard tunnel. **Access Control:** When a peer receives a packet, the "AllowedIPs" list ensures that the source IP address is authorized to communicate with that peer. **Allowed IPS (Server):** Specifies the Client’s VPN and LAN subnets that the Server

	uses to route traffic to that client. By default, the server should set the client’s VPN IP (e.g. 10.0.0.2/24). If you also want to route traffic to the Client’s local network (e.g. 192.168.11.0/24), you should include that subnet as well. Allowed IPs (Server)= 10.0.0.2/24, 192.168.11.0/24.
Allow IPs (Client)	Specifies which destination IPs or subnets the Client will route through the VPN tunnel to the Server. By default, the Allowed IPs (Client) is set to 0.0.0.0/0, which enables **full tunnel mode**, meaning all traffic is routed through the VPN. If you only want to route traffic to the server’s specific local networks, such as 192.168.100.0/24, 192.168.200.0/24, use a **split tunnel** configuration like: Allowed IPs (Client)= 192.168.100.0/24, 192.168.200.0/24.
Download	Option to export the client configuration file.

4.1.2 WireGuard Client



Configuration

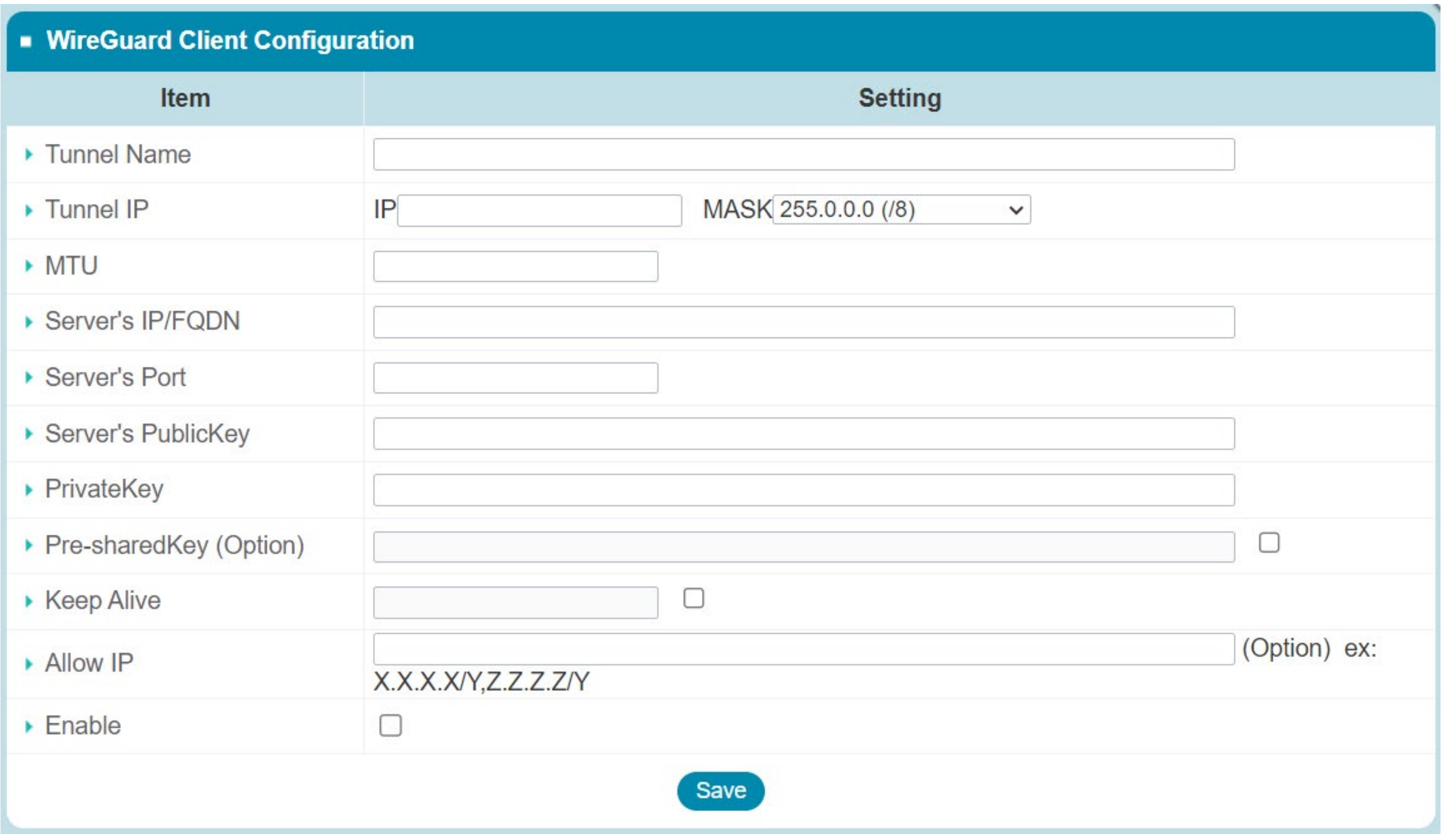
Item	Setting
Server / Client	Client

WireGuard Client Configuration

Item	Setting
WireGuard Client	☐ Enable

WireGuard Client List

ID	Tunnel Name	Tunnel IP	Server's IP/FQDN	Server's PublicKey	Allow IP	Enable	Action



WireGuard Client Configuration

Item	Setting
Tunnel Name	
Tunnel IP	IP MASK 255.0.0.0 (/8)
MTU	
Server's IP/FQDN	
Server's Port	
Server's PublicKey	
PrivateKey	
Pre-sharedKey (Option)	□
Keep Alive	□
Allow IP	(Option) ex: X.X.X.X/Y,Z.Z.Z.Z/Y
Enable	□

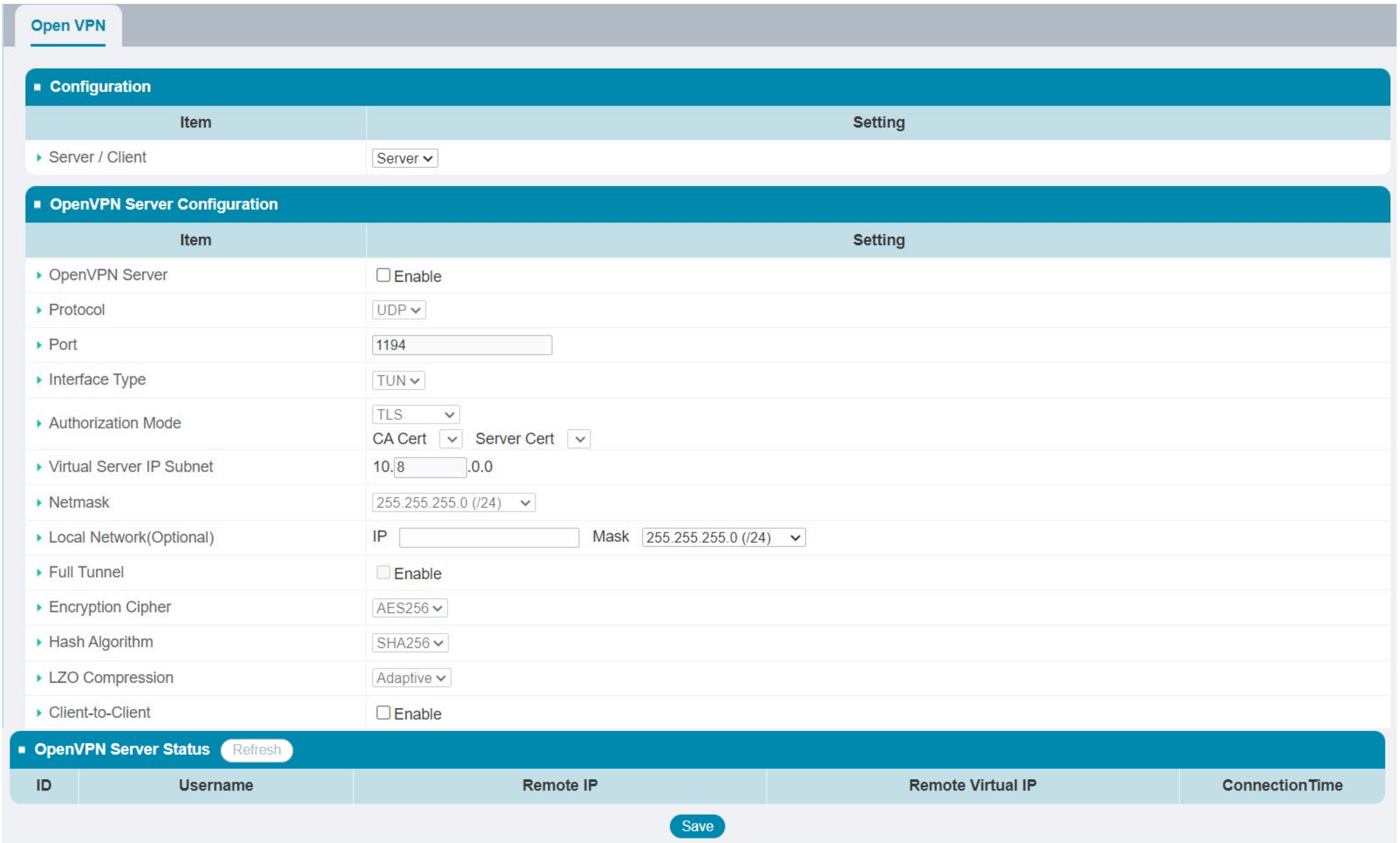
The fields available on this page are as follows:

Field	Description
Tunnel Name	User-defined name for the VPN tunnel for easy identification.
Tunnel IP	Specifies the internal IP address and subnet mask used for the VPN tunnel.
Server's IP/FQDN	The IP address or Fully Qualified Domain Name of the remote WireGuard server.
Server's Port	The port number on which the server listens for incoming WireGuard connections. Default is usually 51820.
Server's PublicKey	The public key of the remote server. Required for secure encrypted communication.
PrivateKey	The private key of the local client. Automatically generated or manually entered. Keep it secure.
Pre-shared Key (Optional)	An additional layer of encryption using a shared key. Improves security.
Keep Alive	Sends periodic messages to keep the connection alive. Recommended for NAT traversal.
Allow IP	Understanding AllowedIPs: **Routing:** When a peer sends a packet, WireGuard checks if the destination IP address is in the peer's "AllowedIPs" list. If it is, the packet is routed through the WireGuard tunnel.

	Access Control: When a peer receives a packet, the "AllowedIPs" list ensures that the source IP address is authorized to communicate with that peer.

4.2 OpenVPN

4.2.1 OpenVPN Server



■ Configuration

Item	Setting
Server / Client	Server

■ OpenVPN Server Configuration

Item	Setting
OpenVPN Server	□ Enable
Protocol	UDP
Port	1194
Interface Type	TUN
Authorization Mode	TLS CA Cert Server Cert
Virtual Server IP Subnet	10.8.0.0
Netmask	255.255.255.0 (/24)
Local Network(Optional)	IP Mask 255.255.255.0 (/24)
Full Tunnel	□ Enable
Encryption Cipher	AES256
Hash Algorithm	SHA256
LZO Compression	Adaptive
Client-to-Client	□ Enable

■ OpenVPN Server Status

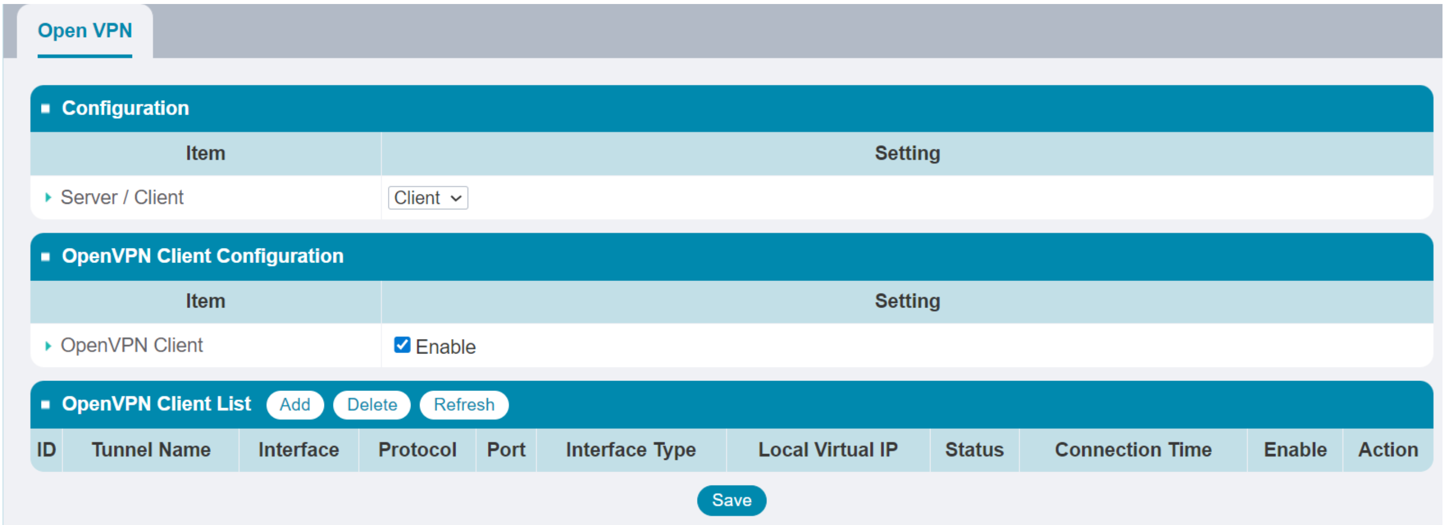
ID	Username	Remote IP	Remote Virtual IP	ConnectionTime

The fields available on this page are as follows:

Field	Description
Protocol	Specifies the transport protocol for OpenVPN communication.
Port	Defines the port number the OpenVPN server will listen on.
Interface Type	Sets the type of virtual network interface. TUN is for routed VPN; TAP for bridged.
Authorization Mode	Selects the authentication method. TLS uses certificates for secure connections.
CA Cert	Selects the Certificate Authority used for validating client certificates.
Server Cert	Selects the server certificate used for TLS authentication.
Virtual Server IP	Defines the virtual IP subnet assigned to VPN clients.

Subnet	
Netmask	Sets the subnet mask for the virtual IP range.
Local Network (Optional)	Specifies internal LAN to be accessible through VPN if required.
Full Tunnel	Forces all client traffic (including Internet access) through the VPN tunnel.
Encryption Cipher	Sets the cipher used to encrypt VPN traffic.
Hash Algorithm	Defines the algorithm used for message integrity verification.
LZO Compression	Configures compression for VPN traffic to improve performance.
Client-to-Client	Allows communication between connected VPN clients.

4.2.2 OpenVPN Client



■ Configuration

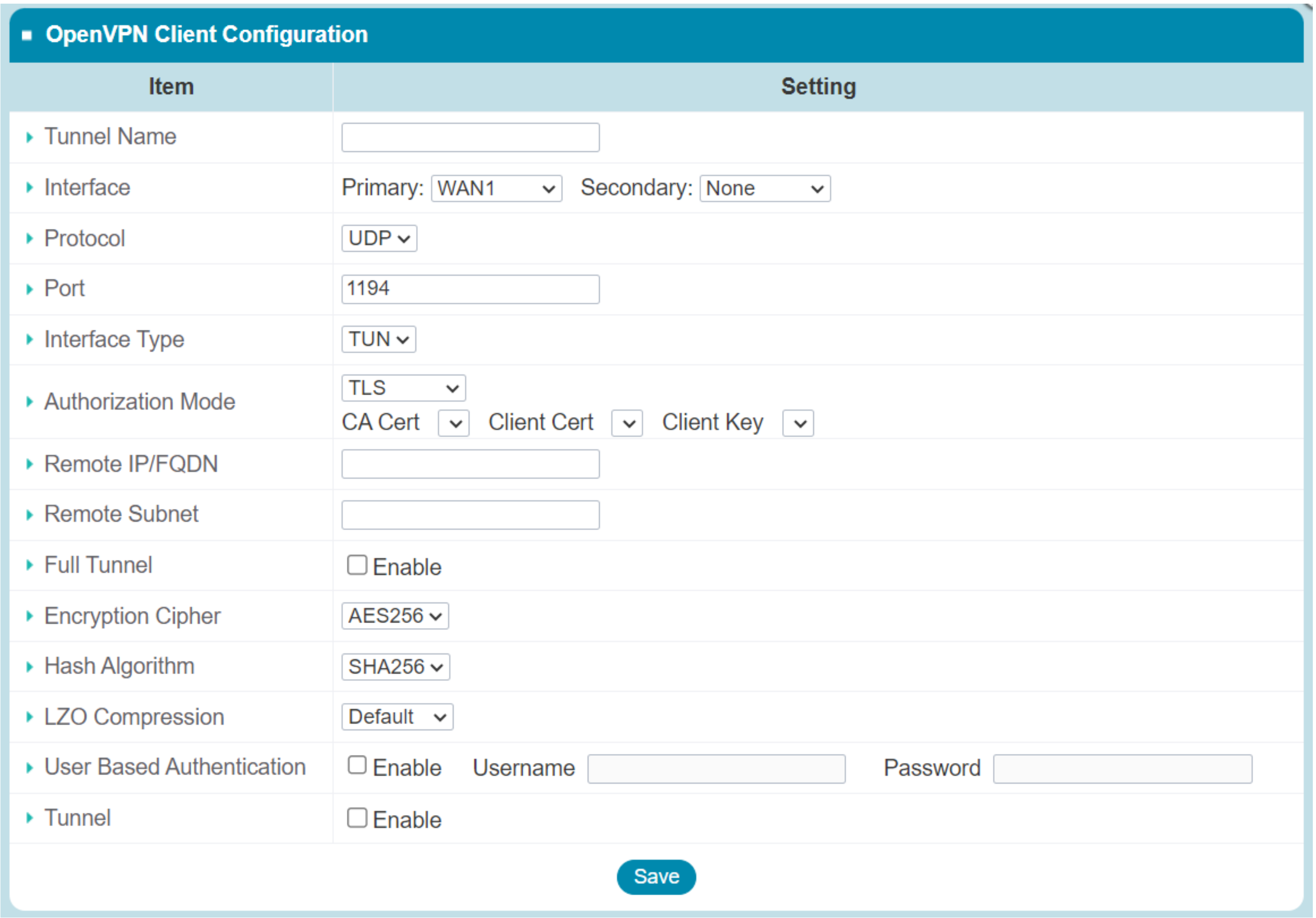
Item	Setting
Server / Client	Client

■ OpenVPN Client Configuration

Item	Setting
OpenVPN Client	☑ Enable

■ OpenVPN Client List

ID	Tunnel Name	Interface	Protocol	Port	Interface Type	Local Virtual IP	Status	Connection Time	Enable	Action



■ OpenVPN Client Configuration

Item	Setting
Tunnel Name	
Interface	Primary: WAN1 ⌄ Secondary: None ⌄
Protocol	UDP ⌄
Port	1194
Interface Type	TUN ⌄
Authorization Mode	TLS ⌄ CA Cert ⌄ Client Cert ⌄ Client Key ⌄
Remote IP/FQDN	
Remote Subnet	
Full Tunnel	□ Enable
Encryption Cipher	AES256 ⌄
Hash Algorithm	SHA256 ⌄
LZO Compression	Default ⌄
User Based Authentication	□ Enable Username Password
Tunnel	□ Enable

The fields available on this page are as follows:

Field	Description
Tunnel Name	Name the VPN tunnel for identification.
Interface	Select the outgoing network interface for VPN connection.
Protocol	Choose the VPN transport protocol. UDP is faster; TCP is more reliable.
Port	Specify the port number used by the VPN server. Default is 1194.
Interface Type	Sets the type of virtual network interface. TUN is for routed VPN; TAP for bridged.
Authorization Mode	Selects the authentication method. TLS uses certificates for secure connections.
CA Cert / Client Cert / Client Key	Select certificate and key files for authentication.
Remote IP/FQDN	Enter the VPN server's IP address or domain name.
Remote Subnet	Specify the remote network accessible through the VPN.
Full Tunnel	If enabled, all traffic goes through VPN.
Encryption Cipher	Sets the cipher used to encrypt VPN traffic.
Hash Algorithm	Defines the algorithm used for message integrity verification.
LZO Compression	Configures compression for VPN traffic to improve performance.

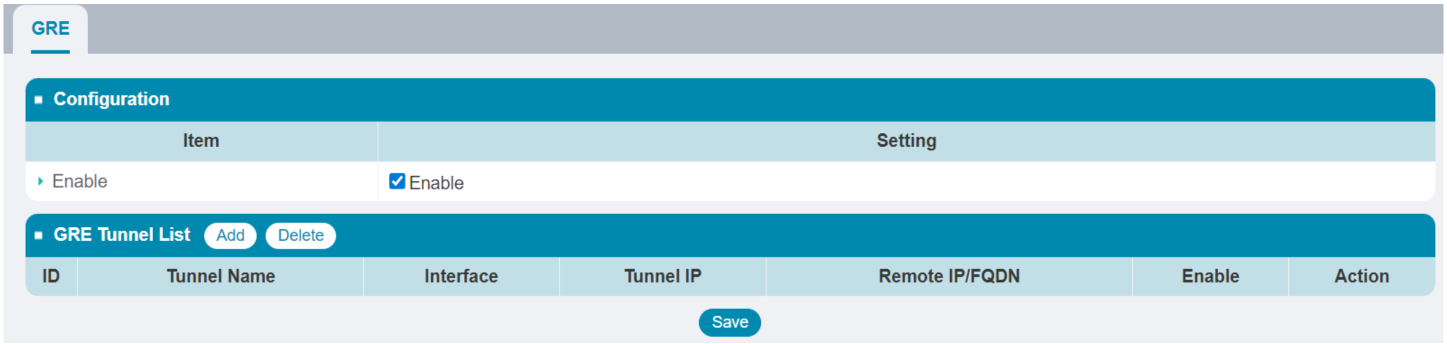
User Based Authentication	Add extra layer of authentication with username and password.

4.3 GRE

GRE (Generic Routing Encapsulation) is a tunneling protocol that encapsulates a wide variety of network layer protocols inside point-to-point IP tunnels. It is commonly used for:

- Creating point-to-point links between remote networks.
- Transporting multicast, broadcast, or routing protocols (e.g., OSPF).
- Supporting legacy protocols over IP networks.

⚠ **Note**: GRE does not provide encryption.

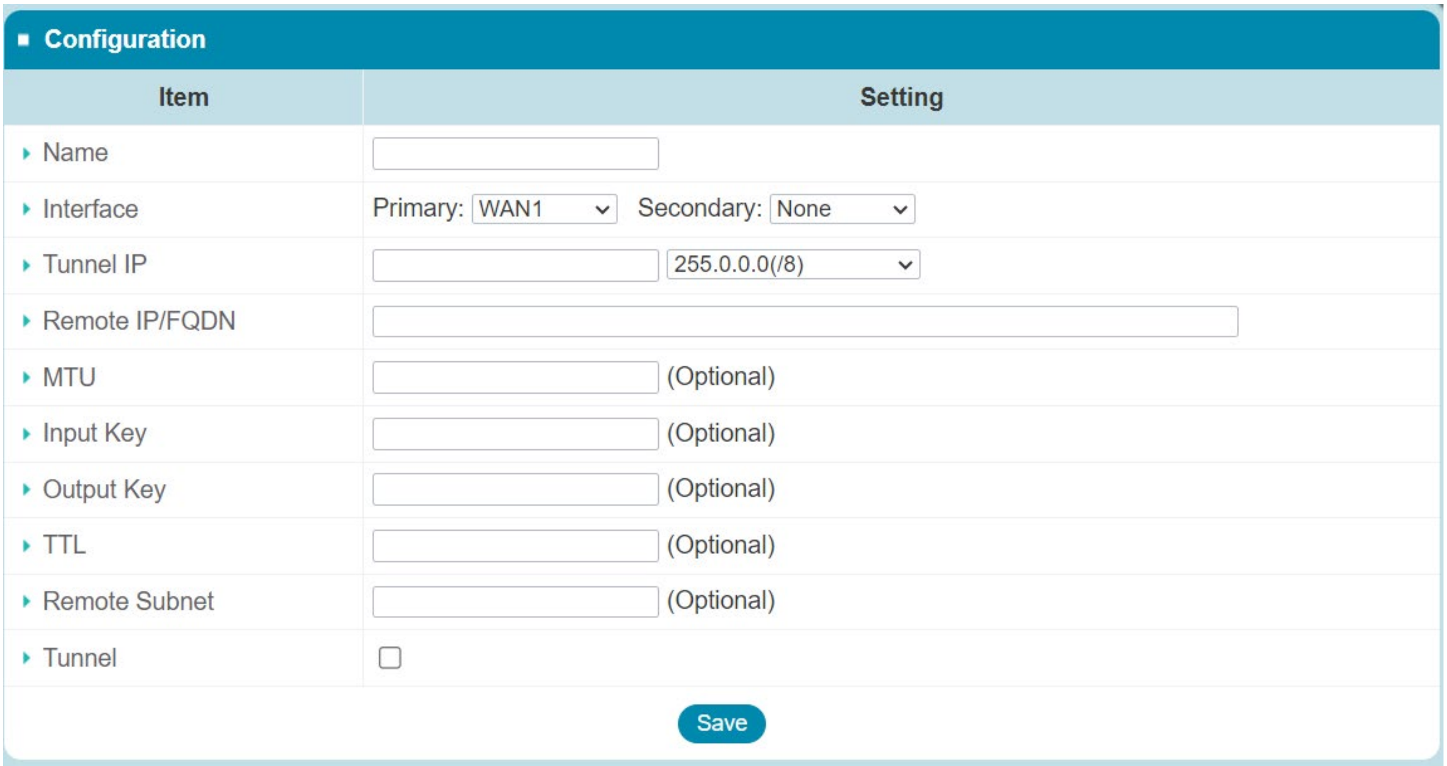


Configuration

Item	Setting
Enable	☑ Enable

GRE Tunnel List

ID	Tunnel Name	Interface	Tunnel IP	Remote IP/FQDN	Enable	Action



Configuration

Item	Setting
Name	
Interface	Primary: WAN1 Secondary: None
Tunnel IP	255.0.0.0(/8)
Remote IP/FQDN	
MTU	(Optional)
Input Key	(Optional)
Output Key	(Optional)
TTL	(Optional)
Remote Subnet	(Optional)
Tunnel	☐

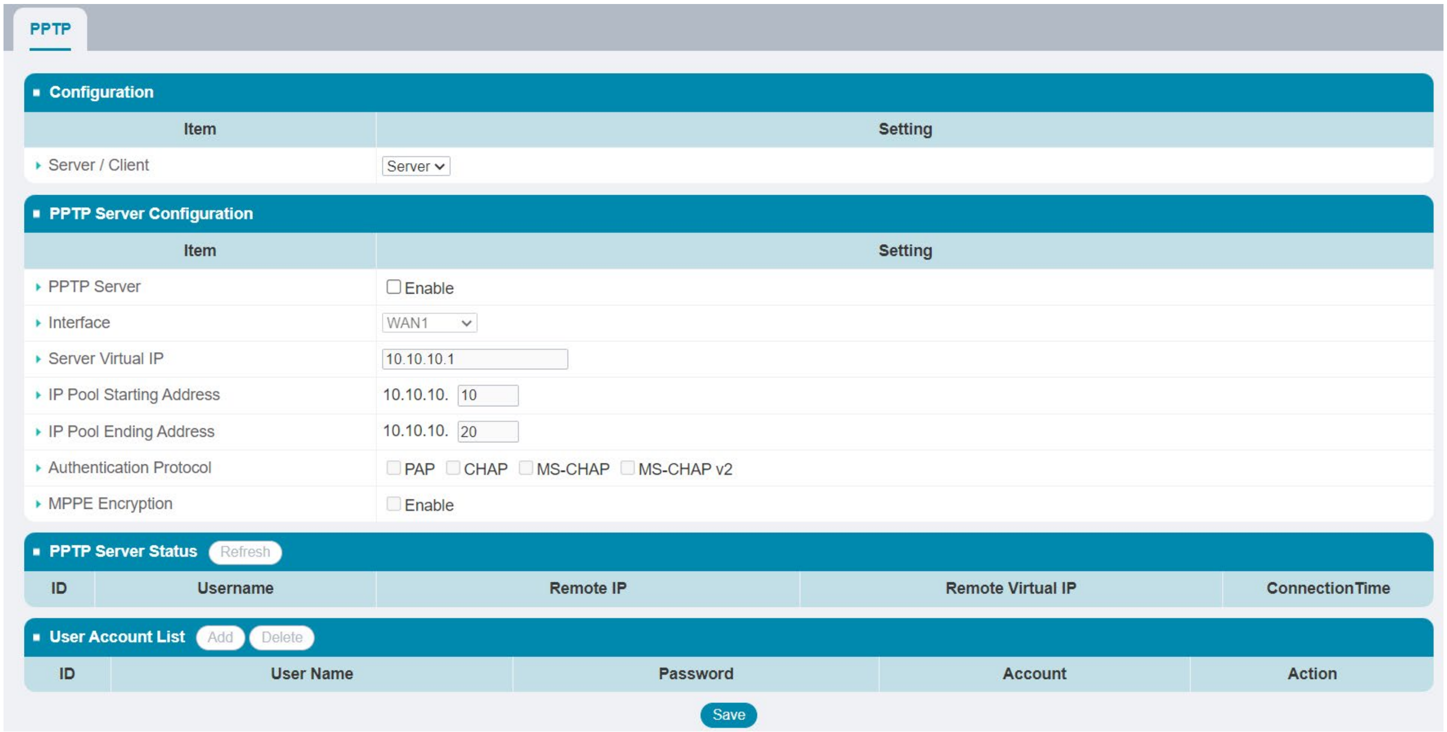
The fields available on this page are as follows:

Field	Description
Name	Name used to identify the GRE tunnel.
Interface	Select the primary and optional secondary WAN interface to establish the tunnel.
Tunnel IP	Local endpoint IP address used in the GRE tunnel.
Port	Specify the port number used by the VPN server. Default is 1194.
Remote IP/FQDN	Specifies the remote GRE tunnel peer.
Authorization Mode	Selects the authentication method. TLS uses certificates for secure connections.
MTU	Maximum Transmission Unit for GRE packets. Leave blank to use default (typically 1476).
Remote IP/FQDN	Enter the VPN server's IP address or domain name.
Input Key	Key used to authenticate incoming GRE packets.
Output Key	Key used for authenticating outgoing GRE packets.
TTL	Time To Live value for GRE packets. Default is usually 255.
Remote Subnet	Defines the destination network reachable via the GRE tunnel. Useful for routing.
Tunnel	Activates the tunnel when checked.

4.4 PPTP

Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating to encapsulate PPP packets. It is a client-server based technology.

4.4.1 PPTP Server



PPTP

Configuration

Item	Setting
Server / Client	Server

PPTP Server Configuration

Item	Setting
PPTP Server	□ Enable
Interface	WAN1
Server Virtual IP	10.10.10.1
IP Pool Starting Address	10.10.10. 10
IP Pool Ending Address	10.10.10. 20
Authentication Protocol	□ PAP □ CHAP □ MS-CHAP □ MS-CHAP v2
MPPE Encryption	□ Enable

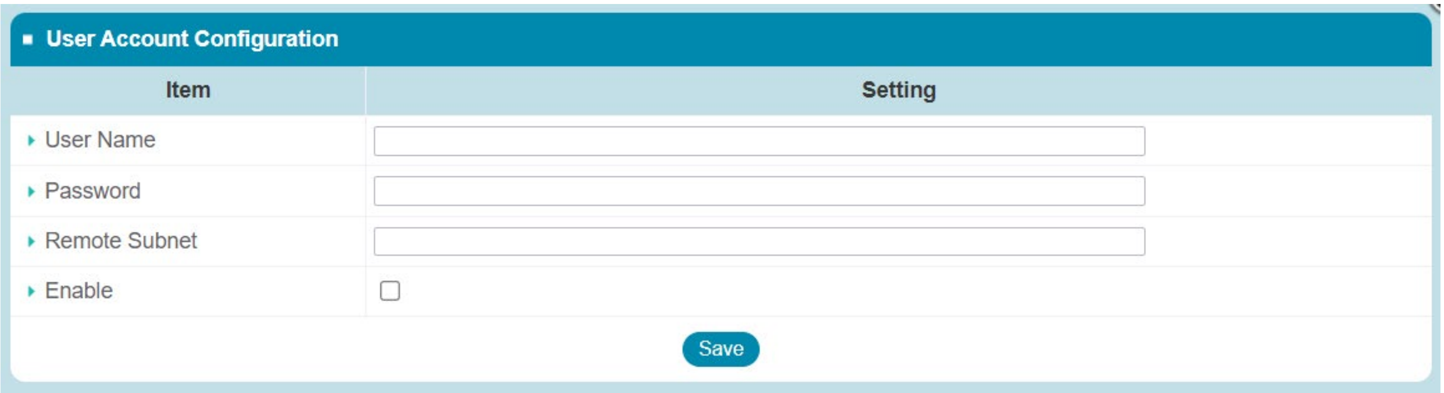
PPTP Server Status Refresh

ID	Username	Remote IP	Remote Virtual IP	ConnectionTime

User Account List Add Delete

ID	User Name	Password	Account	Action

Save



User Account Configuration

Item	Setting
User Name	
Password	
Remote Subnet	
Enable	□

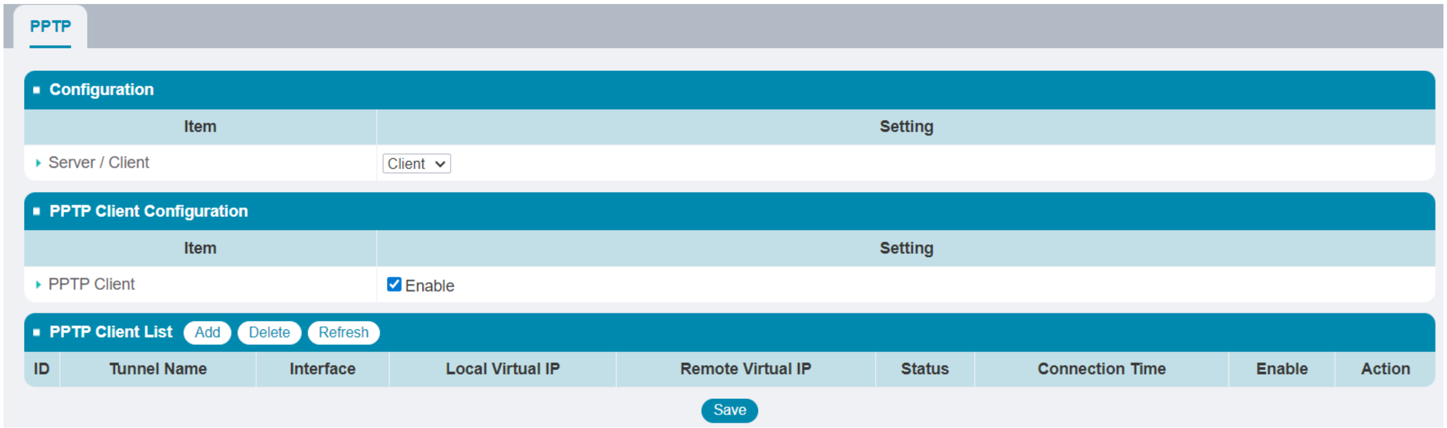
Save

The fields available on this page are as follows:

Field	Description
Interface	Specifies the WAN interface used for PPTP connection.
Server Virtual IP	The virtual IP address of the PPTP server.
IP Pool Starting Address	Beginning of the IP address range assigned to PPTP clients.
IP Pool Ending Address	End of the IP address range assigned to PPTP clients.
Authentication Protocol	Defines the method of authentication for PPTP clients. - **PAP**: Basic password-based authentication. - **CHAP**: Uses challenge-response for better security. - **MS-CHAP / v2**: Microsoft versions with improved encryption.
MPPE Encryption	Enables Microsoft Point-to-Point Encryption (MPPE) for secure data

	transmission.
PPTP Server Status	
Username	Displays the name of the connected PPTP client.
Remote IP	Shows the public IP address of the client device connected to the PPTP server.
Remote Virtual IP	Indicates the virtual IP address assigned to the client by the PPTP server.
Connection Time	Displays the duration of the current PPTP session for the user.
User Account List	
User Name	Specifies the username used for PPTP VPN authentication.
Password	Sets the password associated with the PPTP VPN user account.
Remote Subnet	Defines the remote network accessible through the VPN tunnel for this user.

4.4.2 PPTP Client



PPTP

Configuration

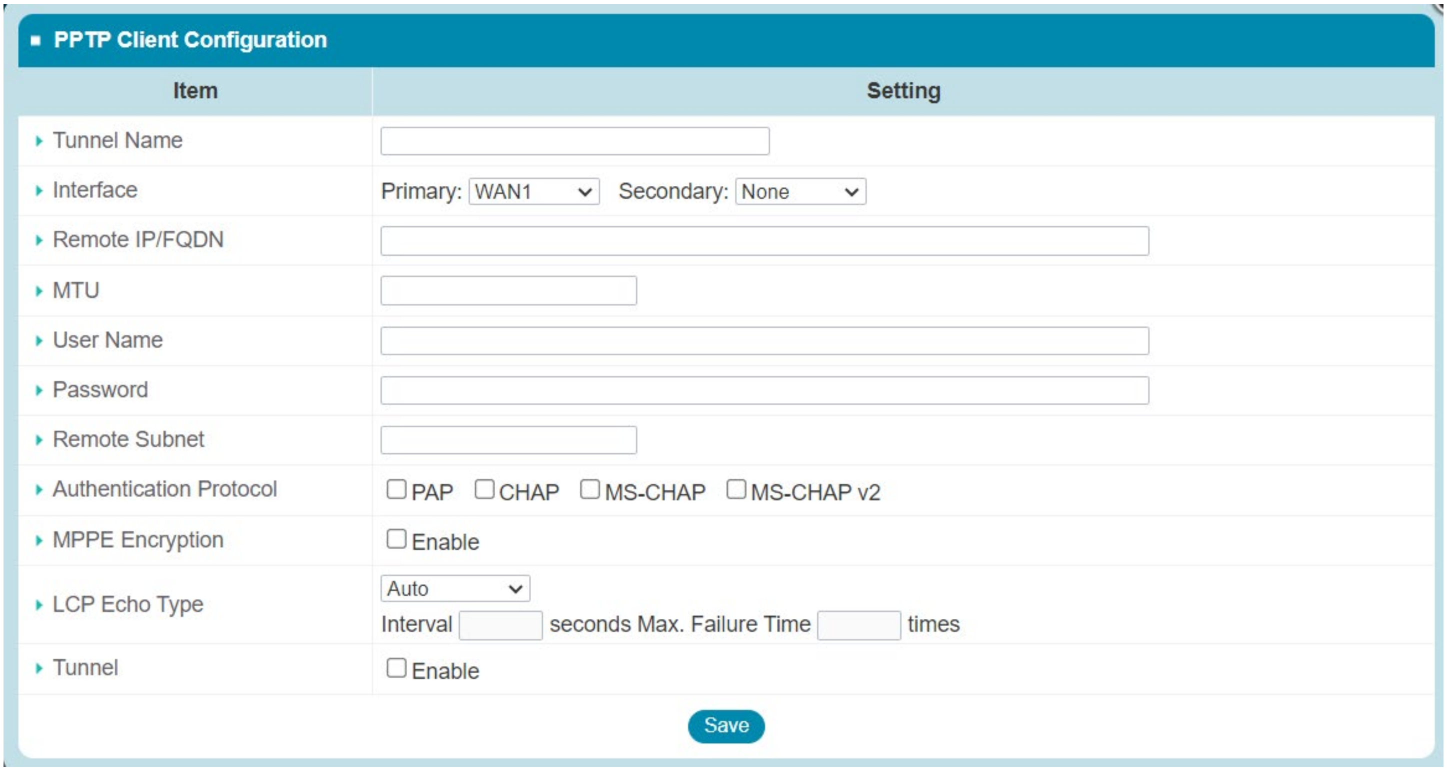
Item	Setting
Server / Client	Client

PPTP Client Configuration

Item	Setting
PPTP Client	☑ Enable

PPTP Client List

ID	Tunnel Name	Interface	Local Virtual IP	Remote Virtual IP	Status	Connection Time	Enable	Action



▪ PPTP Client Configuration

Item	Setting
‣ Tunnel Name	
‣ Interface	Primary: WAN1 ⌄ Secondary: None ⌄
‣ Remote IP/FQDN	
‣ MTU	
‣ User Name	
‣ Password	
‣ Remote Subnet	
‣ Authentication Protocol	□ PAP □ CHAP □ MS-CHAP □ MS-CHAP v2
‣ MPPE Encryption	□ Enable
‣ LCP Echo Type	Auto ⌄ Interval ___ seconds Max. Failure Time ___ times
‣ Tunnel	□ Enable

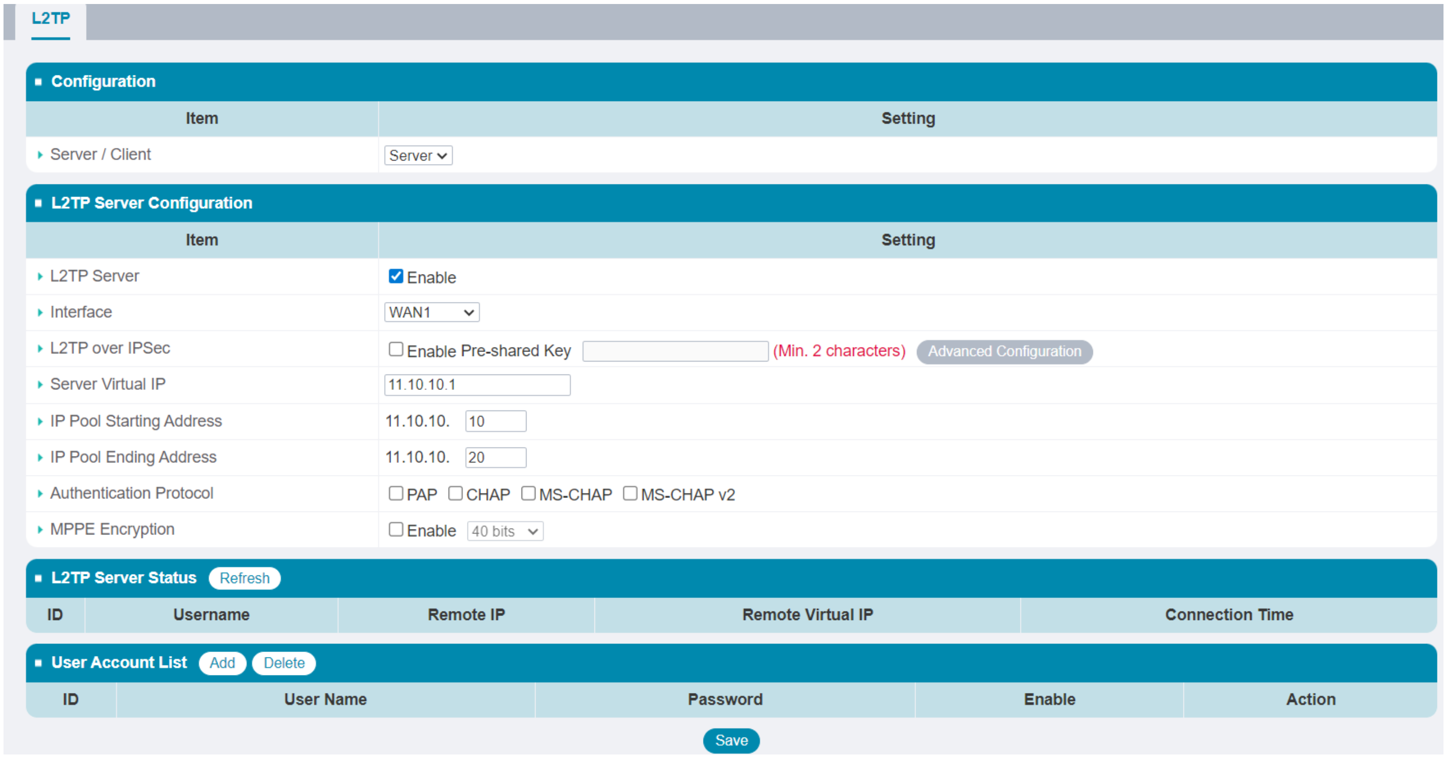
The fields available on this page are as follows:

Field	Description
Tunnel Name	Sets a unique name for this PPTP VPN tunnel configuration. Used for identification.
Interface	Specifies which WAN interface to use as the primary and (optionally) secondary for the VPN connection.
Remote IP/FQDN	Specifies the IP address or domain name of the remote PPTP server to connect to.
MTU	Sets the Maximum Transmission Unit size for the tunnel.
User Name	Username for PPTP VPN authentication.
Password	Password associated with the PPTP user account.
Remote Subnet	Defines the subnet accessible through the VPN tunnel.
Authentication Protocol	Selects the authentication method. Multiple options may be checked depending on server settings.
MPPE Encryption	Enables Microsoft Point-to-Point Encryption to secure the tunnel traffic.
LCP Echo Type	Controls LCP echo requests for connection health checks. **Interval**: Time between echos. **Max. Failure Time**: How many missed echoes before marking the tunnel as down.
Tunnel	Enables or disables the tunnel configuration. When checked, the client attempts to connect.

4.5 L2TP

L2TP is a tunneling protocol for VPNs. It does not encrypt data on its own but can be used with IPSec for secure communication. This gateway supports both L2TP server and client modes at the same time.

4.5.1 L2TP Server



L2TP

Configuration

Item	Setting
Server / Client	Server

L2TP Server Configuration

Item	Setting
L2TP Server	☑ Enable
Interface	WAN1
L2TP over IPSec	□ Enable Pre-shared Key (Min. 2 characters) Advanced Configuration
Server Virtual IP	11.10.10.1
IP Pool Starting Address	11.10.10. 10
IP Pool Ending Address	11.10.10. 20
Authentication Protocol	□ PAP □ CHAP □ MS-CHAP □ MS-CHAP v2
MPPE Encryption	□ Enable 40 bits

L2TP Server Status Refresh

ID	Username	Remote IP	Remote Virtual IP	Connection Time

User Account List Add Delete

ID	User Name	Password	Enable	Action

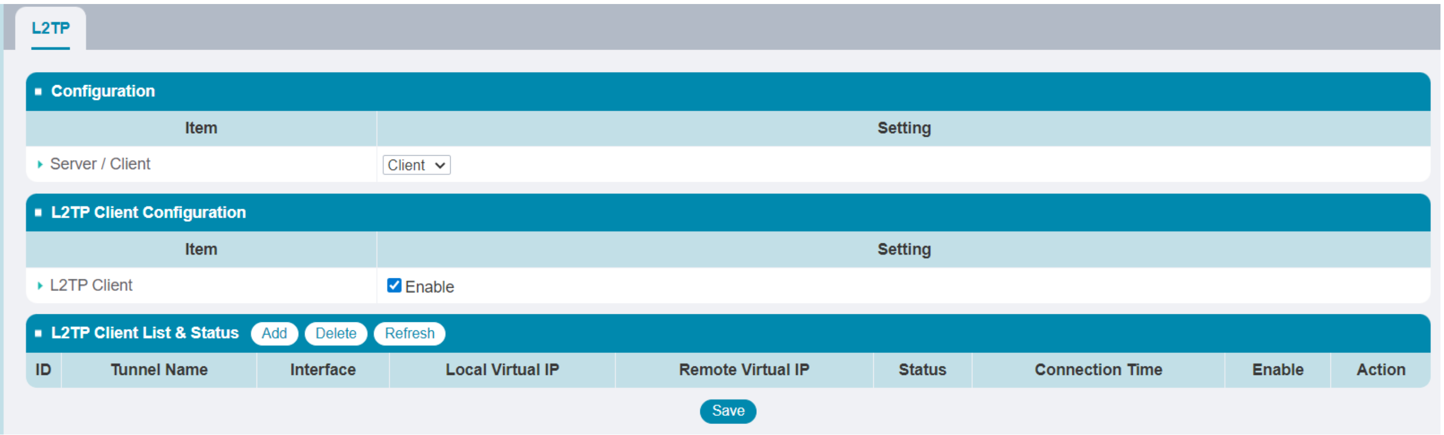
Save

The fields available on this page are as follows:

Field	Description
Interface	Select the network interface for the L2TP server.
L2TP over IPSec	Optional: Enable L2TP over IPSec with a pre-shared key for encryption.
Server Virtual IP	The virtual IP address of the L2TP server.
IP Pool Starting Address	Beginning of the IP address range assigned to L2TP clients.
IP Pool Ending Address	End of the IP address range assigned to L2TP clients.
Authentication Protocol	Defines the method of authentication for L2TP clients. - **PAP**: Basic password-based authentication. - **CHAP**: Uses challenge-response for better security. - **MS-CHAP / v2**: Microsoft versions with improved encryption.
MPPE Encryption	Enables Microsoft Point-to-Point Encryption (MPPE) for secure data transmission.

PPTP Server Status	
Username	Displays the name of the connected L2TP client.
Remote IP	Shows the public IP address of the client device connected to the L2TP server.
Remote Virtual IP	Indicates the virtual IP address assigned to the client by the L2TP server.
Connection Time	Displays the duration of the current L2TP session for the user.
User Account List	
User Name	Specifies the username used for L2TP VPN authentication.
Password	Sets the password associated with the L2TP VPN user account.
Remote Subnet	Defines the remote network accessible through the VPN tunnel for this user.

4.5.2 L2TP Client



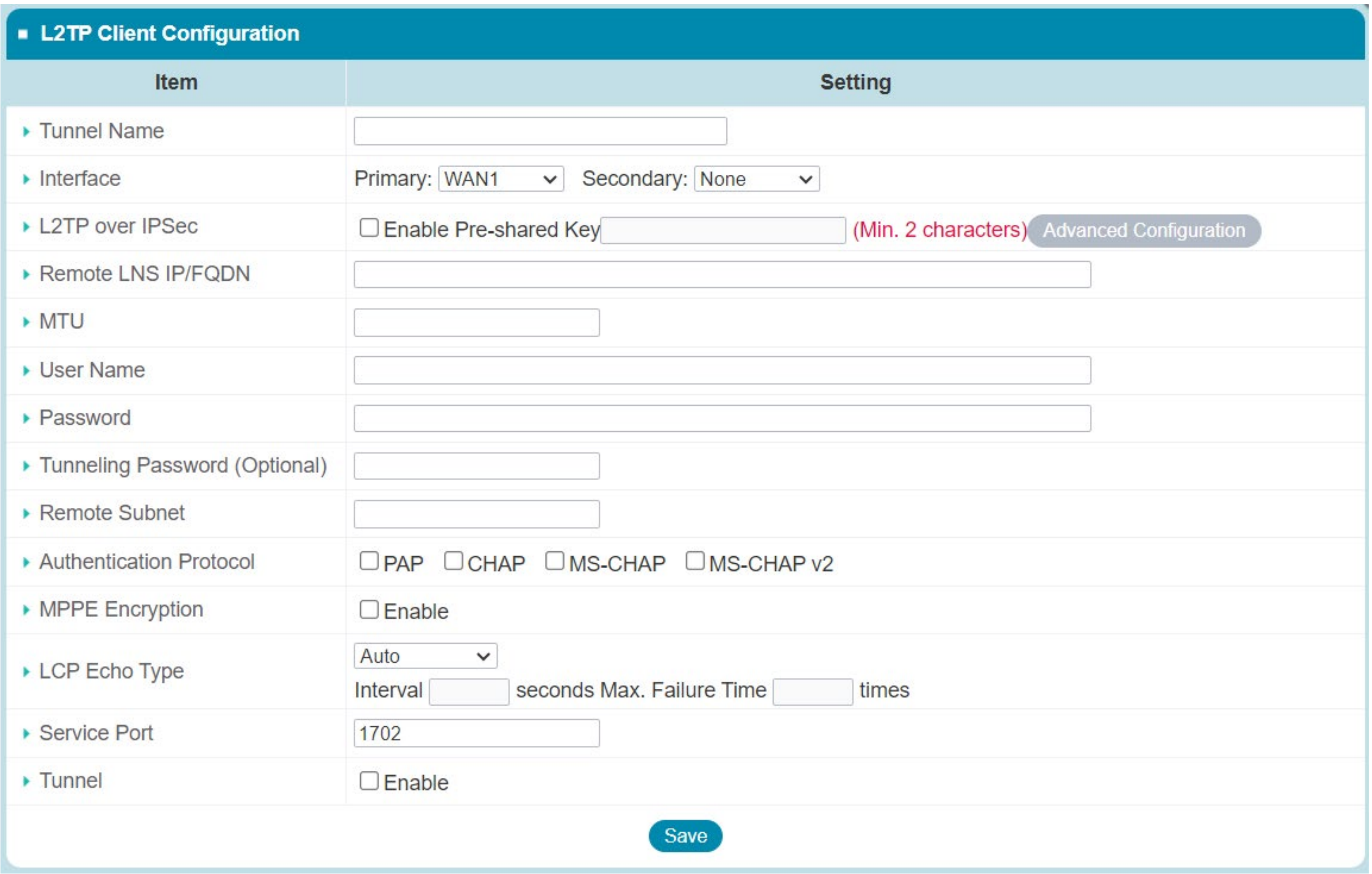
Configuration

Item	Setting
Server / Client	Client

L2TP Client Configuration

Item	Setting
L2TP Client	☑ Enable

ID	Tunnel Name	Interface	Local Virtual IP	Remote Virtual IP	Status	Connection Time	Enable	Action



■ L2TP Client Configuration

Item	Setting
Tunnel Name	
Interface	Primary: WAN1 ⌄ Secondary: None ⌄
L2TP over IPSec	□ Enable Pre-shared Key (Min. 2 characters) Advanced Configuration
Remote LNS IP/FQDN	
MTU	
User Name	
Password	
Tunneling Password (Optional)	
Remote Subnet	
Authentication Protocol	□ PAP □ CHAP □ MS-CHAP □ MS-CHAP v2
MPPE Encryption	□ Enable
LCP Echo Type	Auto ⌄ Interval seconds Max. Failure Time times
Service Port	1702
Tunnel	□ Enable

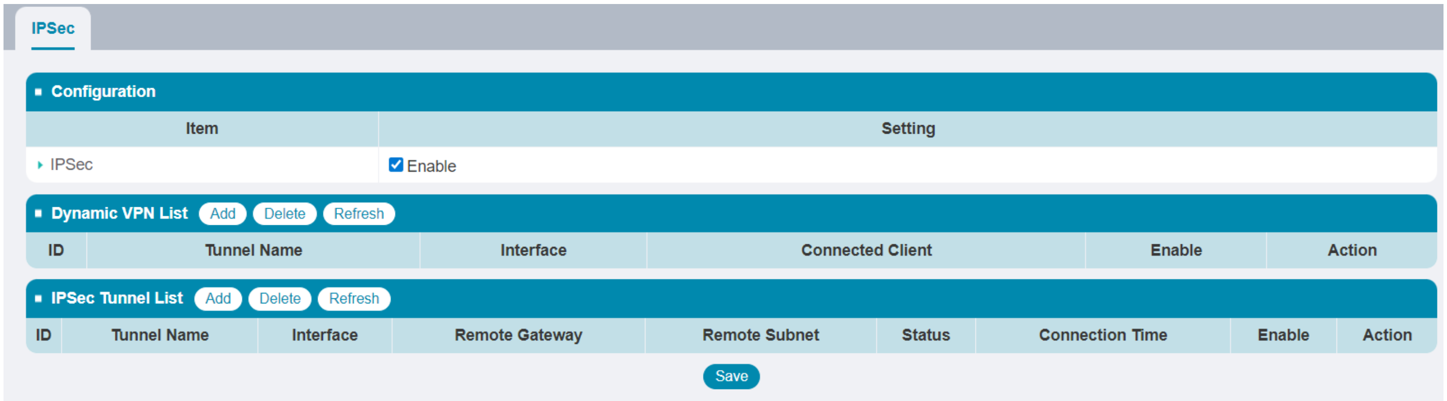
The fields available on this page are as follows:

Field	Description
Tunnel Name	Sets a unique name for this L2TP VPN tunnel configuration. Used for identification.
Interface	Specifies which WAN interface to use as the primary and (optionally) secondary for the VPN connection.
L2TP over IPSec	Enable L2TP over IPSec with a pre-shared key for encryption.
Remote IP/FQDN	Specifies the IP address or domain name of the remote L2TP server to connect to.
MTU	Sets the Maximum Transmission Unit size for the tunnel.
User Name	Username for L2TP VPN authentication.
Password	Password associated with the L2TP user account.
Remote Subnet	Defines the subnet accessible through the VPN tunnel.
Authentication Protocol	Selects the authentication method. Multiple options may be checked depending on server settings.
MPPE Encryption	Enables Microsoft Point-to-Point Encryption to secure the tunnel traffic.
LCP Echo Type	Controls LCP echo requests for connection health checks. **Interval**: Time between echos. **Max. Failure Time**: How many missed echoes before marking the tunnel as

	down.
Service Port	Specify the port number used by the VPN server. Default is 1702
Tunnel	Enables or disables the tunnel configuration. When checked, the client attempts to connect.

4.6 IPSec

I PSec VPN (Internet Protocol Security Virtual Private Network) is a secure communication method that encrypts and authenticates IP traffic between devices over the Internet. It is commonly used for creating secure site-to-site or remote access connections.



Configuration

Item	Setting
IPSec	☑ Enable

Dynamic VPN List

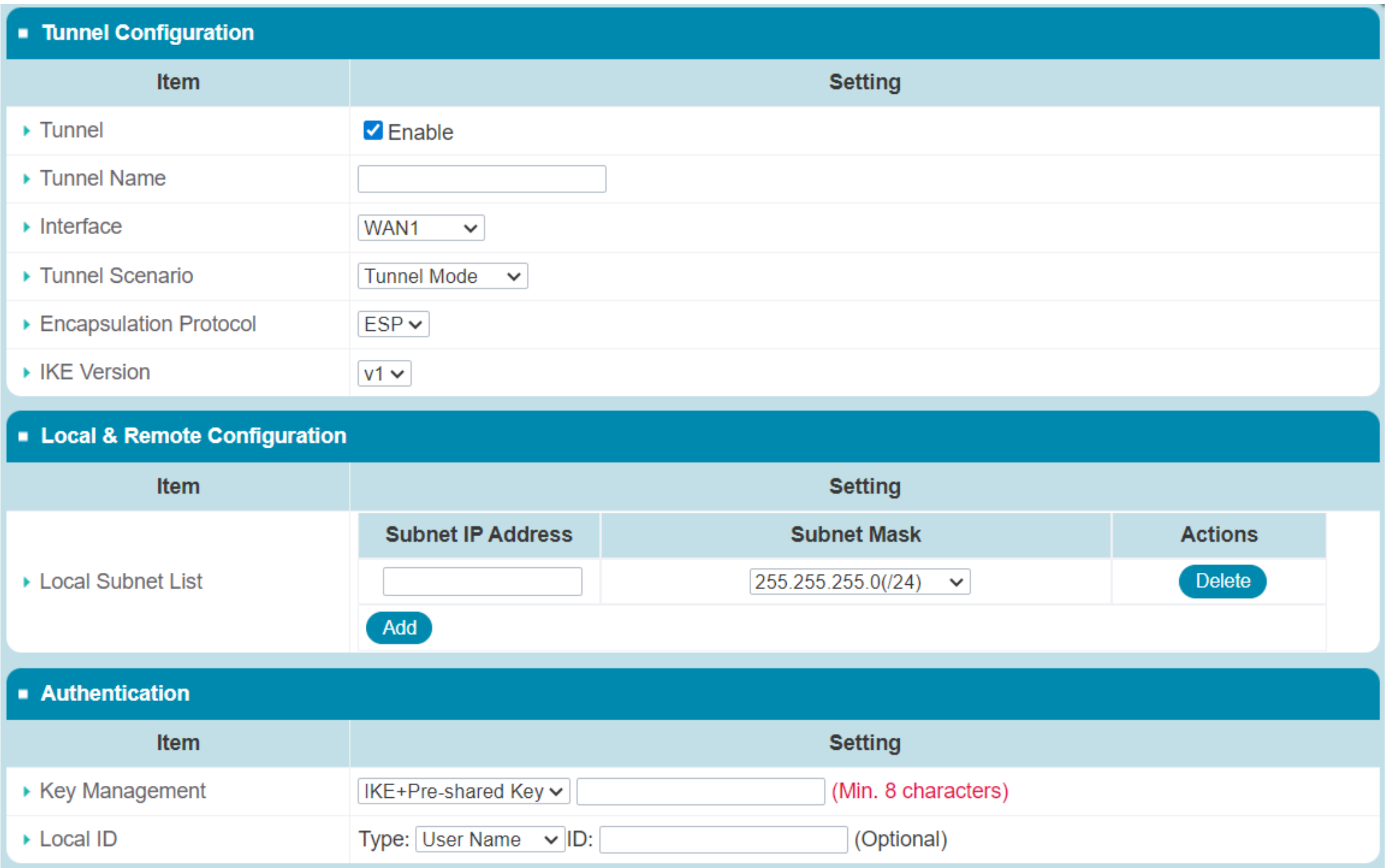
ID	Tunnel Name	Interface	Connected Client	Enable	Action

IPSec Tunnel List

ID	Tunnel Name	Interface	Remote Gateway	Remote Subnet	Status	Connection Time	Enable	Action

4.6.1 Dynamic VPN

This section allows the user to manage dynamic VPN tunnels for connecting remote clients with dynamically assigned IPs.



■ Tunnel Configuration

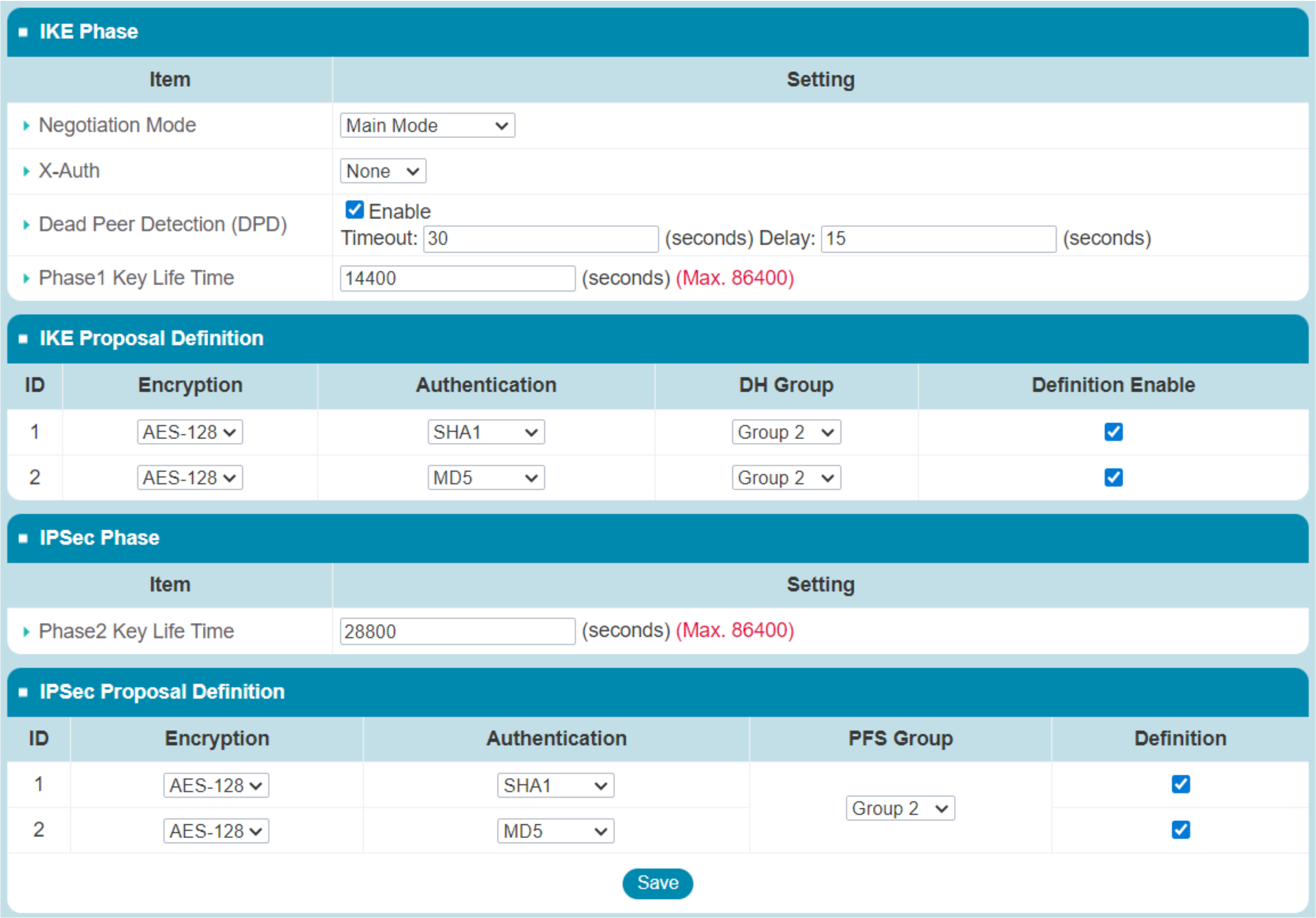
Item	Setting
Tunnel	☑ Enable
Tunnel Name	
Interface	WAN1
Tunnel Scenario	Tunnel Mode
Encapsulation Protocol	ESP
IKE Version	v1

■ Local & Remote Configuration

Item	Setting		
	Subnet IP Address	Subnet Mask	Actions
Local Subnet List		255.255.255.0(/24)	Delete
	Add		

■ Authentication

Item	Setting
Key Management	IKE+Pre-shared Key (Min. 8 characters)
Local ID	Type: User Name ID: (Optional)



▪ IKE Phase

Item	Setting
Negotiation Mode	Main Mode
X-Auth	None
Dead Peer Detection (DPD)	☑ Enable Timeout: 30 (seconds) Delay: 15 (seconds)
Phase1 Key Life Time	14400 (seconds) (Max. 86400)

▪ IKE Proposal Definition

ID	Encryption	Authentication	DH Group	Definition Enable
1	AES-128	SHA1	Group 2	☑
2	AES-128	MD5	Group 2	☑

▪ IPSec Phase

Item	Setting
Phase2 Key Life Time	28800 (seconds) (Max. 86400)

▪ IPSec Proposal Definition

ID	Encryption	Authentication	PFS Group	Definition
1	AES-128	SHA1	Group 2	☑
2	AES-128	MD5		☑

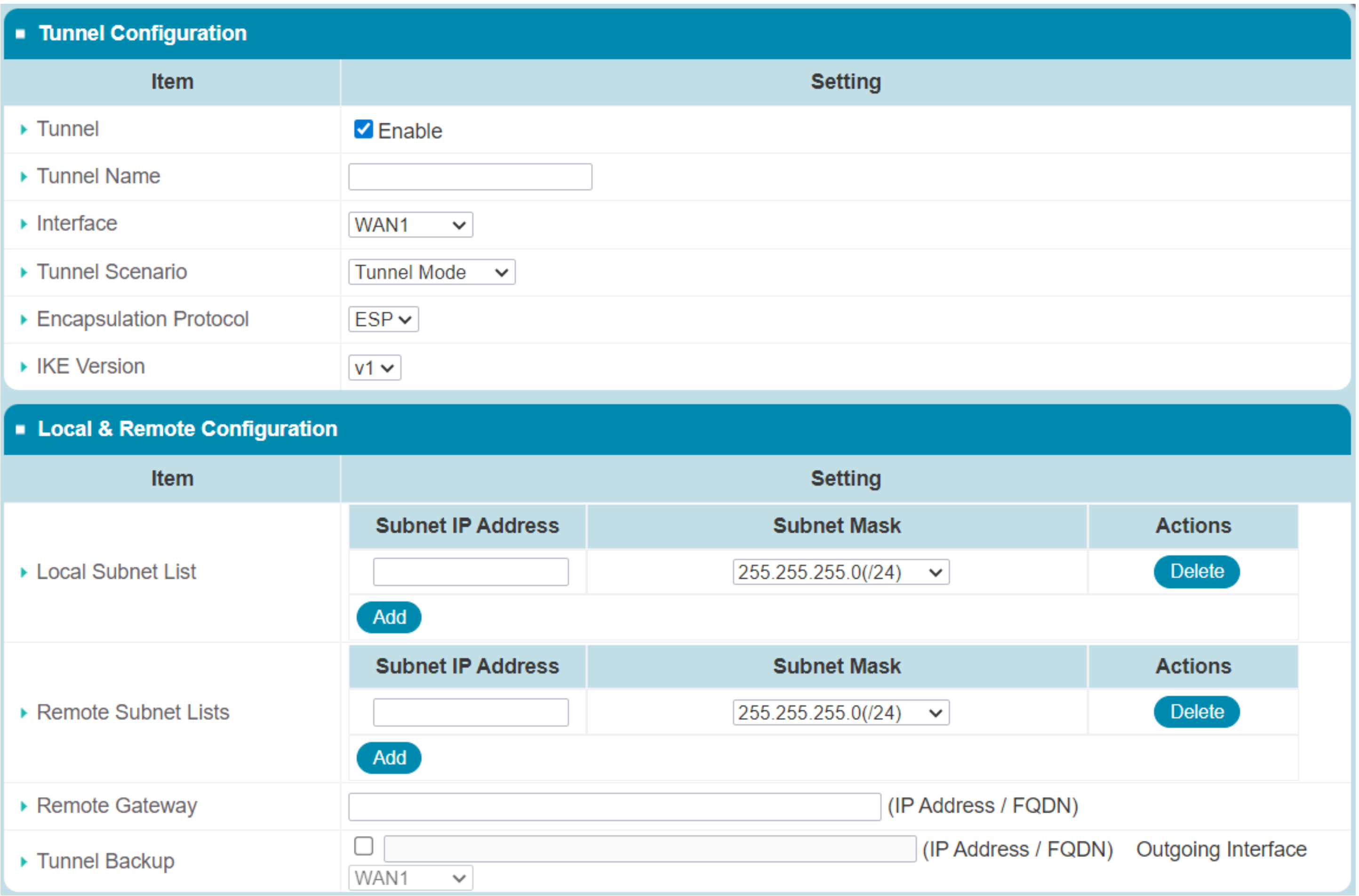
The fields available on this page are as follows:

Field	Description
Tunnel Configuration	
Tunnel Name	User-defined name to identify the tunnel.
Interface	Selects the WAN interface used for the IPSec tunnel.
Tunnel Scenario	Defines the operational mode of the tunnel.
Encapsulation Protocol	Specifies the type of encapsulation used for IPSec (ESP is typical for encrypted transport).
IKE Version	Sets the Internet Key Exchange version (v1 or v2) for tunnel negotiation.
Local & Remote Configuration	
Local Subnet List	Defines the internal (local) subnet(s) to be included in the VPN tunnel. These are typically the networks behind the local router.
Authentication	
Key Management	Selects the key management method and inputs the pre-shared key (minimum 8 characters).
Local ID	Sets the local identity used for authentication during tunnel negotiation. This can be a username or other identifier. The ID field is optional.

IKE Phase	
Negotiation Mode	Determines the mode for IKE Phase 1 negotiation. Main Mode is typically more secure.
X-Auth	Specifies if extended authentication (e.g. username/password) is used.
Dead Peer Detection (DPD)	Keeps the connection alive by detecting if the peer is unreachable.
Phase1 Key Life Time	Duration for which the Phase 1 key is valid before it needs re-negotiation.
IKE Proposal Definition	
Encryption	Algorithm used for encrypting IKE Phase 1 traffic.
Authentication	Hashing method for IKE authentication.
DH Group	Defines the Diffie-Hellman group for key exchange.
Definition Enable	Indicates whether the proposal is active.

4.6.2 IPsec Tunnel

This section allows the user to configure IPSec VPN tunnels, defining encryption, authentication, and key exchange parameters for secure site-to-site or remote access communication over the Internet.

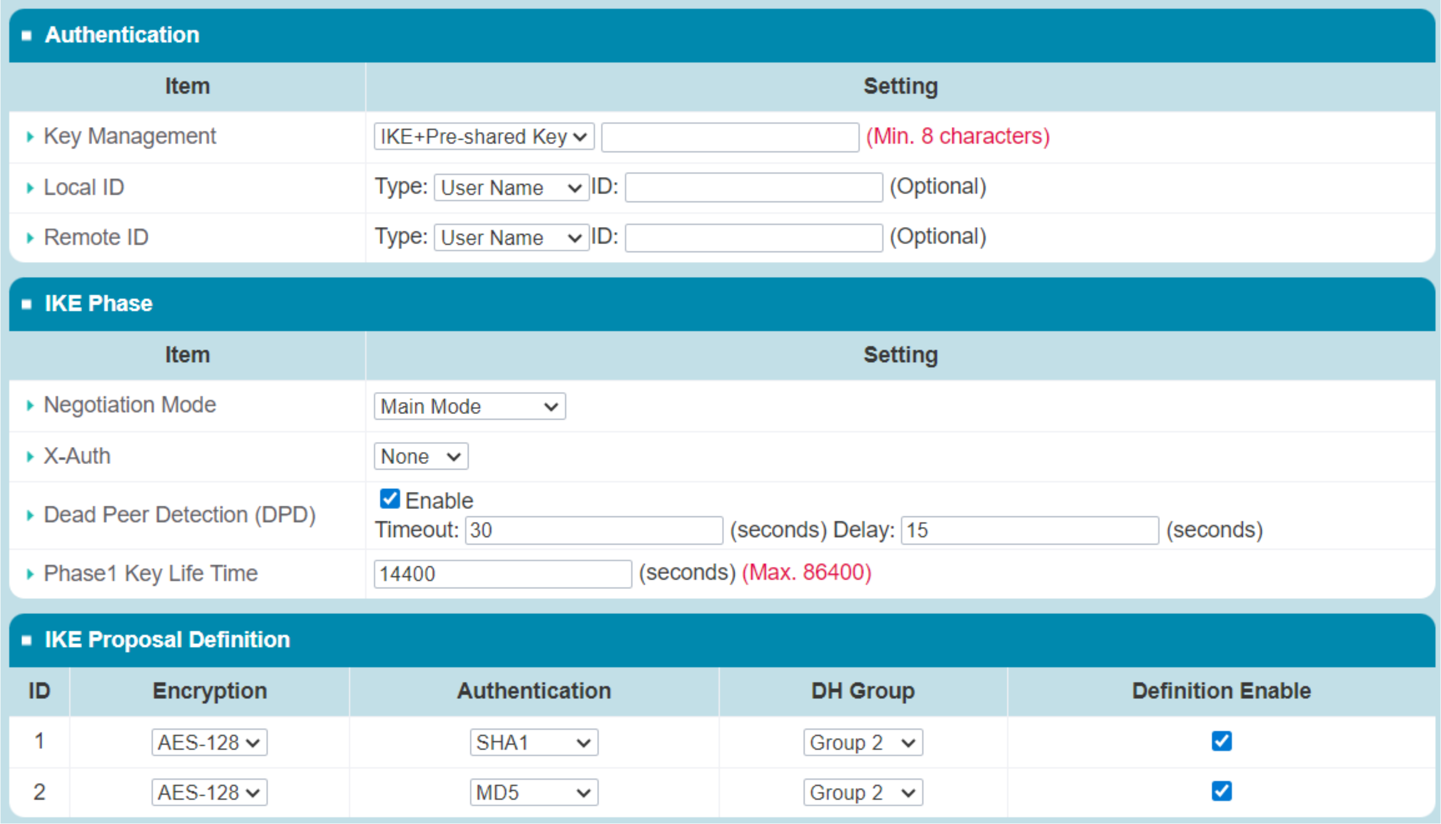


Tunnel Configuration

Item	Setting
Tunnel	☑ Enable
Tunnel Name	
Interface	WAN1
Tunnel Scenario	Tunnel Mode
Encapsulation Protocol	ESP
IKE Version	v1

Local & Remote Configuration

Item	Setting		
	Subnet IP Address	Subnet Mask	Actions
Local Subnet List		255.255.255.0(/24)	Delete
	Add		
	Subnet IP Address	Subnet Mask	Actions
Remote Subnet Lists		255.255.255.0(/24)	Delete
	Add		
Remote Gateway	(IP Address / FQDN)		
Tunnel Backup	□ (IP Address / FQDN) Outgoing Interface WAN1		



Authentication

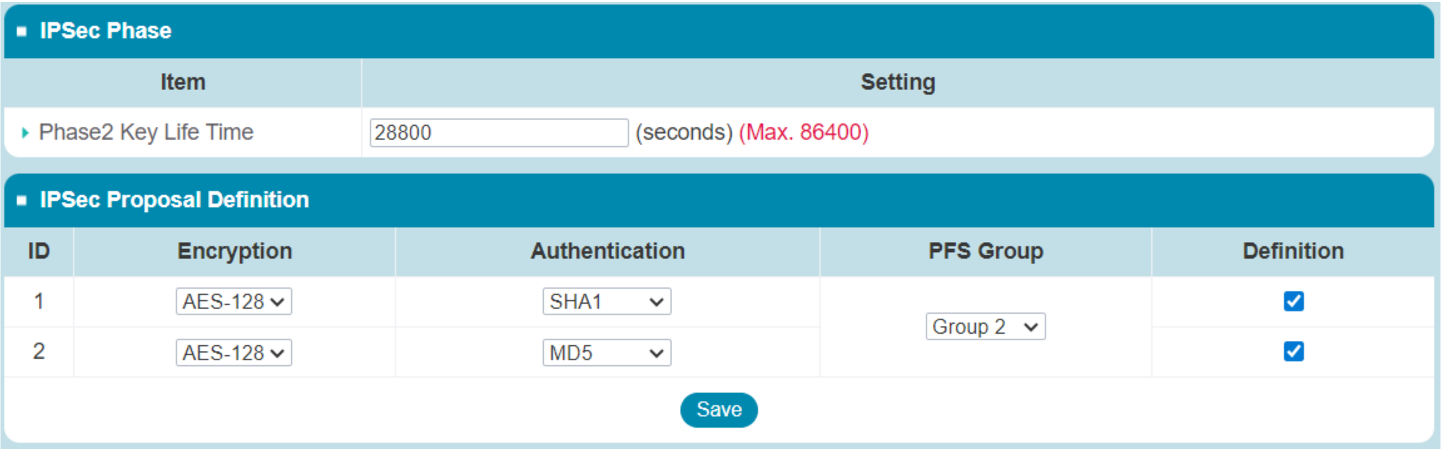
Item	Setting
Key Management	IKE+Pre-shared Key ⌄ (Min. 8 characters)
Local ID	Type: User Name ⌄ ID: (Optional)
Remote ID	Type: User Name ⌄ ID: (Optional)

IKE Phase

Item	Setting
Negotiation Mode	Main Mode ⌄
X-Auth	None ⌄
Dead Peer Detection (DPD)	☑ Enable Timeout: 30 (seconds) Delay: 15 (seconds)
Phase1 Key Life Time	14400 (seconds) (Max. 86400)

IKE Proposal Definition

ID	Encryption	Authentication	DH Group	Definition Enable
1	AES-128 ⌄	SHA1 ⌄	Group 2 ⌄	☑
2	AES-128 ⌄	MD5 ⌄	Group 2 ⌄	☑



IPSec Phase

Item	Setting
Phase2 Key Life Time	28800 (seconds) (Max. 86400)

IPSec Proposal Definition

ID	Encryption	Authentication	PFS Group	Definition
1	AES-128 ⌄	SHA1 ⌄	Group 2 ⌄	☑
2	AES-128 ⌄	MD5 ⌄		☑

The fields available on this page are as follows:

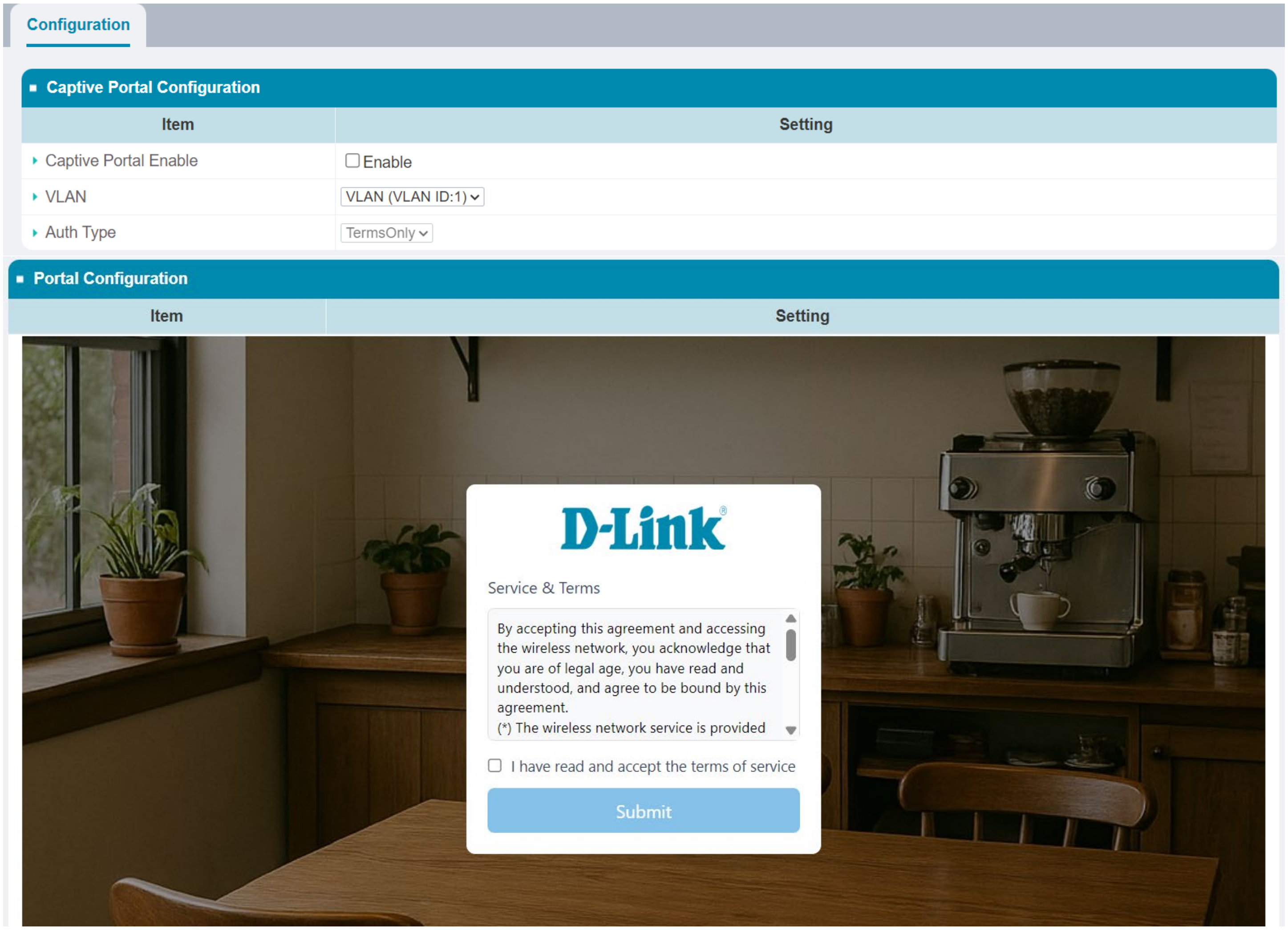
Field	Description
Tunnel Configuration	
Tunnel Name	Defines a unique name for identifying the VPN tunnel.
Interface	Selects the WAN interface used for the VPN tunnel.
Tunnel Scenario	Specifies the IPSec mode (e.g., Tunnel or Transport mode).
Encapsulation Protocol	Sets the protocol used to encapsulate IP packets (ESP or AH).
IKE Version	Sets the Internet Key Exchange version (v1 or v2) for tunnel negotiation.

Local & Remote Configuration	
Local Subnet List	Specifies the internal network(s) to be routed through the tunnel.
Remote Subnet Lists	Defines the remote network(s) accessible through the tunnel.
Remote Gateway	Sets the IP address or domain name of the remote VPN peer.
Tunnel Backup	Enables backup VPN path using another interface if the primary fails.
Authentication	
Key Management	Selects the key exchange method; commonly uses a shared secret for authentication.
Local ID	Specifies the identity of the local device (used during IKE negotiation).
Remote ID	Defines the identity of the remote peer
IKE Phase	
Negotiation Mode	Determines the mode for IKE Phase 1 negotiation. Main Mode is typically more secure.
X-Auth	Specifies if extended authentication (e.g. username/password) is used.
Dead Peer Detection (DPD)	Detects inactive peers and helps reestablish the tunnel if needed.
Phase1 Key Life Time	Specifies how long the IKE Phase 1 key is valid before renewal.
IKE Proposal Definition	
Encryption	Algorithm used for encrypting IKE Phase 1 traffic.
Authentication	Hashing method for IKE authentication.
DH Group	Defines the Diffie-Hellman group for key exchange.
Definition Enable	Indicates whether the proposal is active.
IPsec Phase	
Phase2 Key Life Time	Sets the lifetime of the Phase 2 Security Association (SA). After this time, the key will be renegotiated. Range: 1–86400 seconds.
IPSec Proposal Definition	
Encryption	Defines the encryption algorithm to protect data confidentiality.
Authentication	Specifies the hashing method for data integrity and authentication.
PFS Group	Sets the Perfect Forward Secrecy (PFS) Diffie-Hellman group used in key exchange.
Definition	Marks the proposal as active and valid for use in the IPSec VPN.

Chapter 5 Service

5.1 Captive Portal

The DBR-700 provides Captive Portal functionality for secure internet access control in public areas such as cafés, airports, and hotels. When paired with the DBR-X3000-AP, it supports VLAN-based user authentication for network segmentation and access control.
Note: DBR-700 supports only one Captive Portal service at a time.



Captive Portal Configuration

Item	Setting
Captive Portal Enable	□ Enable
VLAN	VLAN (VLAN ID:1)
Auth Type	TermsOnly

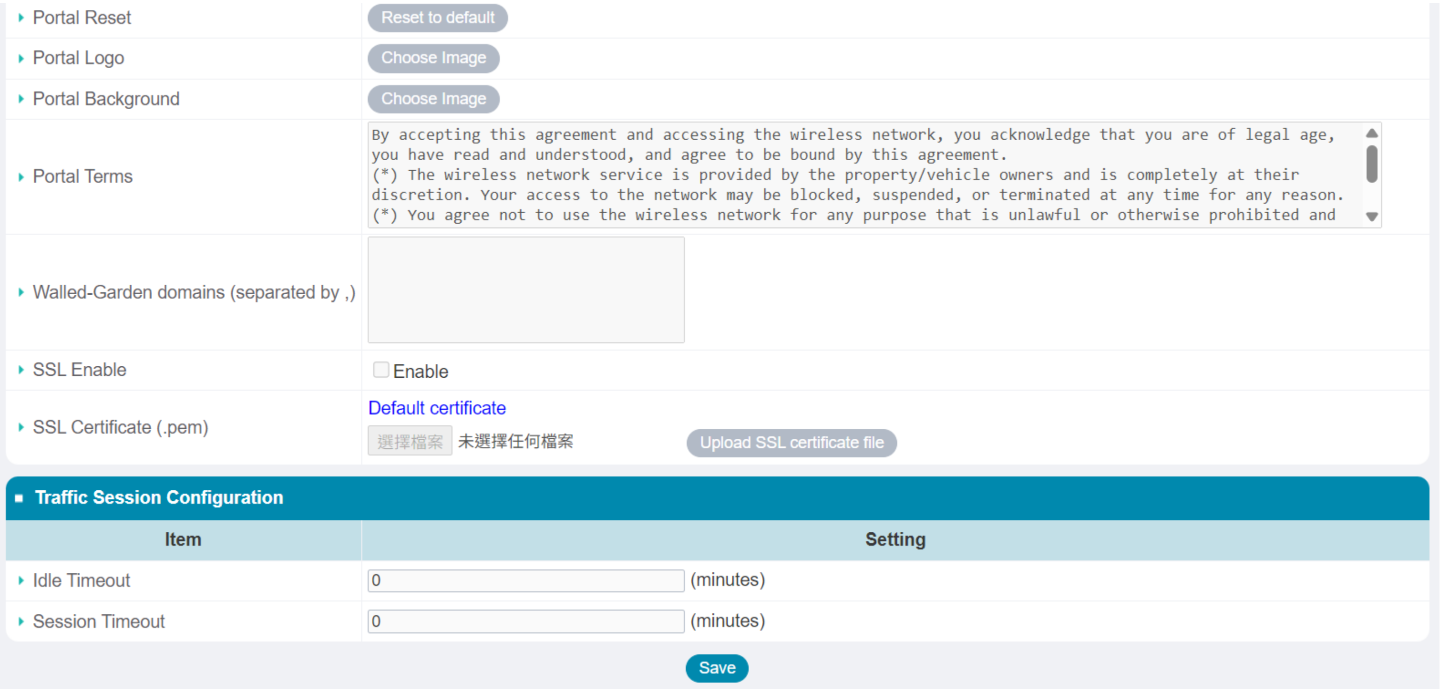
Portal Configuration

Item	Setting

Service & Terms

By accepting this agreement and accessing the wireless network, you acknowledge that you are of legal age, you have read and understood, and agree to be bound by this agreement.
(*) The wireless network service is provided

□ I have read and accept the terms of service



Portal Reset	Reset to default
Portal Logo	Choose Image
Portal Background	Choose Image
Portal Terms	By accepting this agreement and accessing the wireless network, you acknowledge that you are of legal age, you have read and understood, and agree to be bound by this agreement. (*) The wireless network service is provided by the property/vehicle owners and is completely at their discretion. Your access to the network may be blocked, suspended, or terminated at any time for any reason. (*) You agree not to use the wireless network for any purpose that is unlawful or otherwise prohibited and
Walled-Garden domains (separated by ,)	
SSL Enable	□ Enable
SSL Certificate (.pem)	Default certificate 選擇檔案 未選擇任何檔案 Upload SSL certificate file

Traffic Session Configuration

Item	Setting
Idle Timeout	0 (minutes)
Session Timeout	0 (minutes)

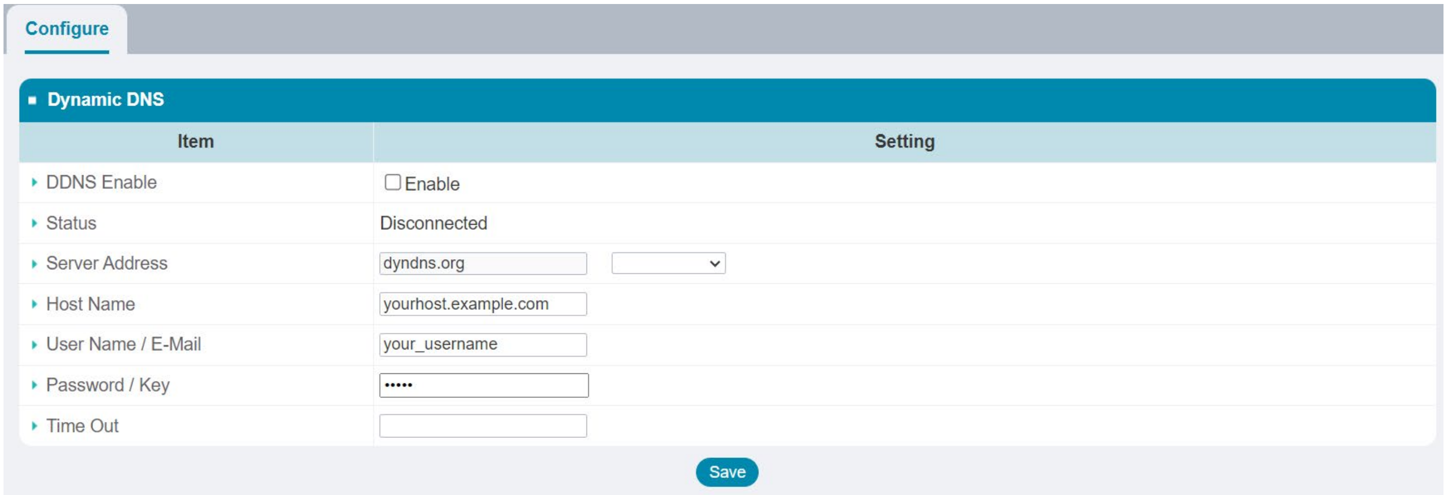
Save

The fields available on this page are as follows:

Field	Description
Captive Portal Enable	Activates or deactivates the Captive Portal feature.
VLAN	Selects the VLAN interface to bind the Captive Portal to.
Auth Type	Defines the authentication method.
Portal Configuration	
Portal Reset	Restores the portal page to its default settings.
Portal Logo	Sets a custom logo on the Captive Portal login page.
Portal Background	Sets the background image for the portal page.
Portal Terms	Displays terms and conditions users must accept before accessing the network.
Walled-Garden domains	Allows access to specific websites before login
SSL Enable	Enables HTTPS encryption for the portal login page.
SSL Certificate (.pem)	Uploads a custom SSL certificate to secure the Captive Portal page.
Traffic Session Configuration	
Idle Timeout	Disconnects the user session if no traffic is detected within the set time.
Session Timeout	Forces logout after the session duration, regardless of activity.

5.2 DDNS

DDNS (Dynamic Domain Name System) automatically updates your domain name to match your network's changing IP address. This ensures you can always access your device remotely, even with a dynamic IP.



Dynamic DNS

Item	Setting
DDNS Enable	□ Enable
Status	Disconnected
Server Address	dyndns.org
Host Name	yourhost.example.com
User Name / E-Mail	your_username
Password / Key	•••••
Time Out	

The fields available on this page are as follows:

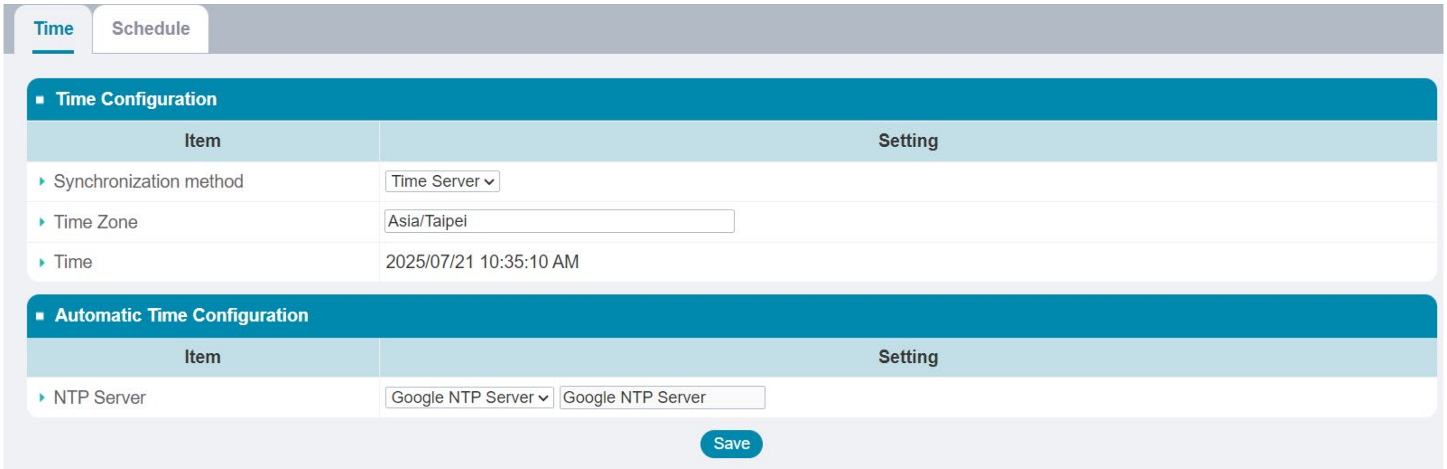
Field	Description
Tunnel Name	Sets a unique name for this L2TP VPN tunnel configuration. Used for identification.
Interface	Specifies which WAN interface to use as the primary and (optionally) secondary for the VPN connection.
L2TP over IPSec	Enable L2TP over IPSec with a pre-shared key for encryption.
Remote IP/FQDN	Specifies the IP address or domain name of the remote L2TP server to connect to.
MTU	Sets the Maximum Transmission Unit size for the tunnel.
User Name	Username for L2TP VPN authentication.
Password	Password associated with the L2TP user account.
Remote Subnet	Defines the subnet accessible through the VPN tunnel.
Authentication Protocol	Selects the authentication method. Multiple options may be checked depending on server settings.
MPPE Encryption	Enables Microsoft Point-to-Point Encryption to secure the tunnel traffic.

Chapter 6 Management

6.1 Time & Schedule

6.1.1 Time

This section allows you to configure the time zone and set up automatic time synchronization using NTP (Network Time Protocol).



Time Configuration

Item	Setting
Synchronization method	Time Server
Time Zone	Asia/Taipei
Time	2025/07/21 10:35:10 AM

Automatic Time Configuration

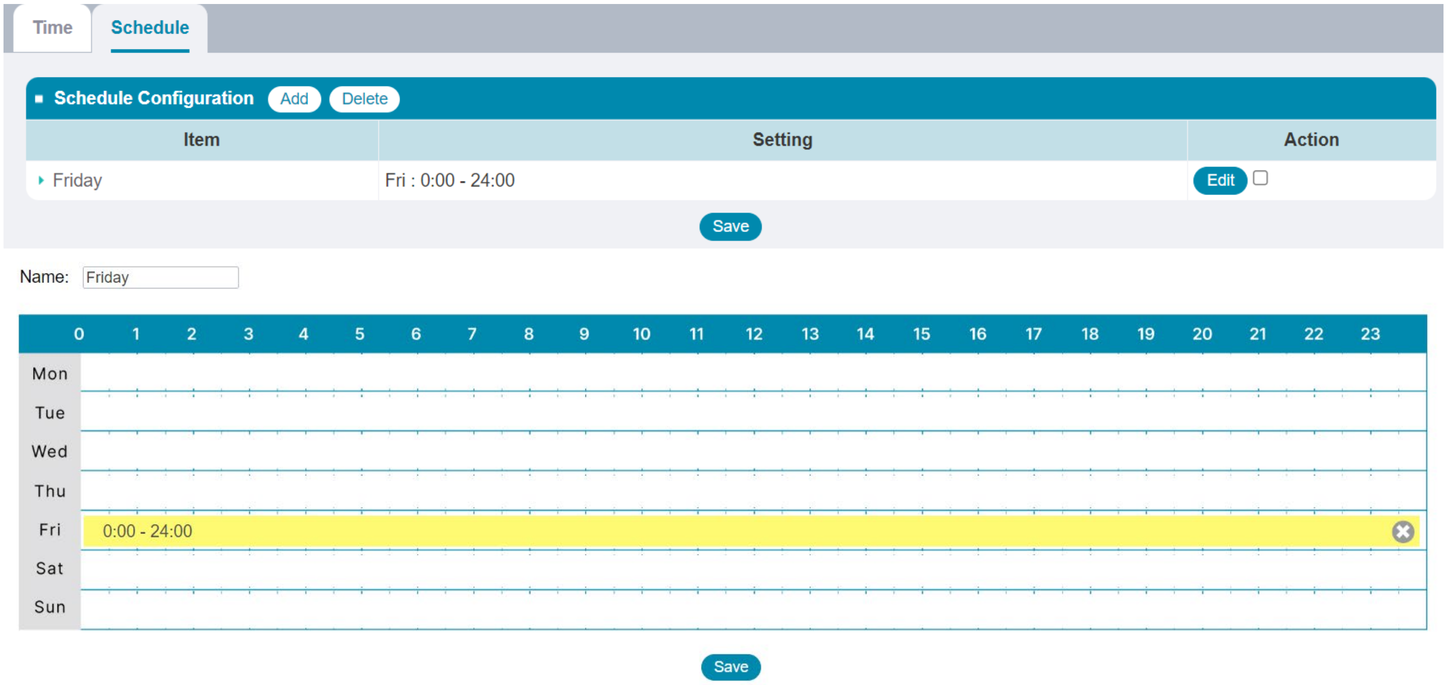
Item	Setting
NTP Server	Google NTP Server Google NTP Server

The fields available on this page are as follows:

Field	Description
Synchronization method	Specifies how the system time is synchronized. Selecting “Time Server” allows the device to automatically update time from a designated NTP (Network Time Protocol) server. Choosing "Manual" allows the user to input the time manually instead of syncing via a time server.
Time Zone	Sets the device's time zone, which affects how time is displayed across logs, schedules, and events.
Time	Displays the current system time.
MPPE Encryption	Enables Microsoft Point-to-Point Encryption to secure the tunnel traffic.

6.1.2 Schedule

This section allows you to configure specific days of the week and define time periods during which the schedule will be applied.



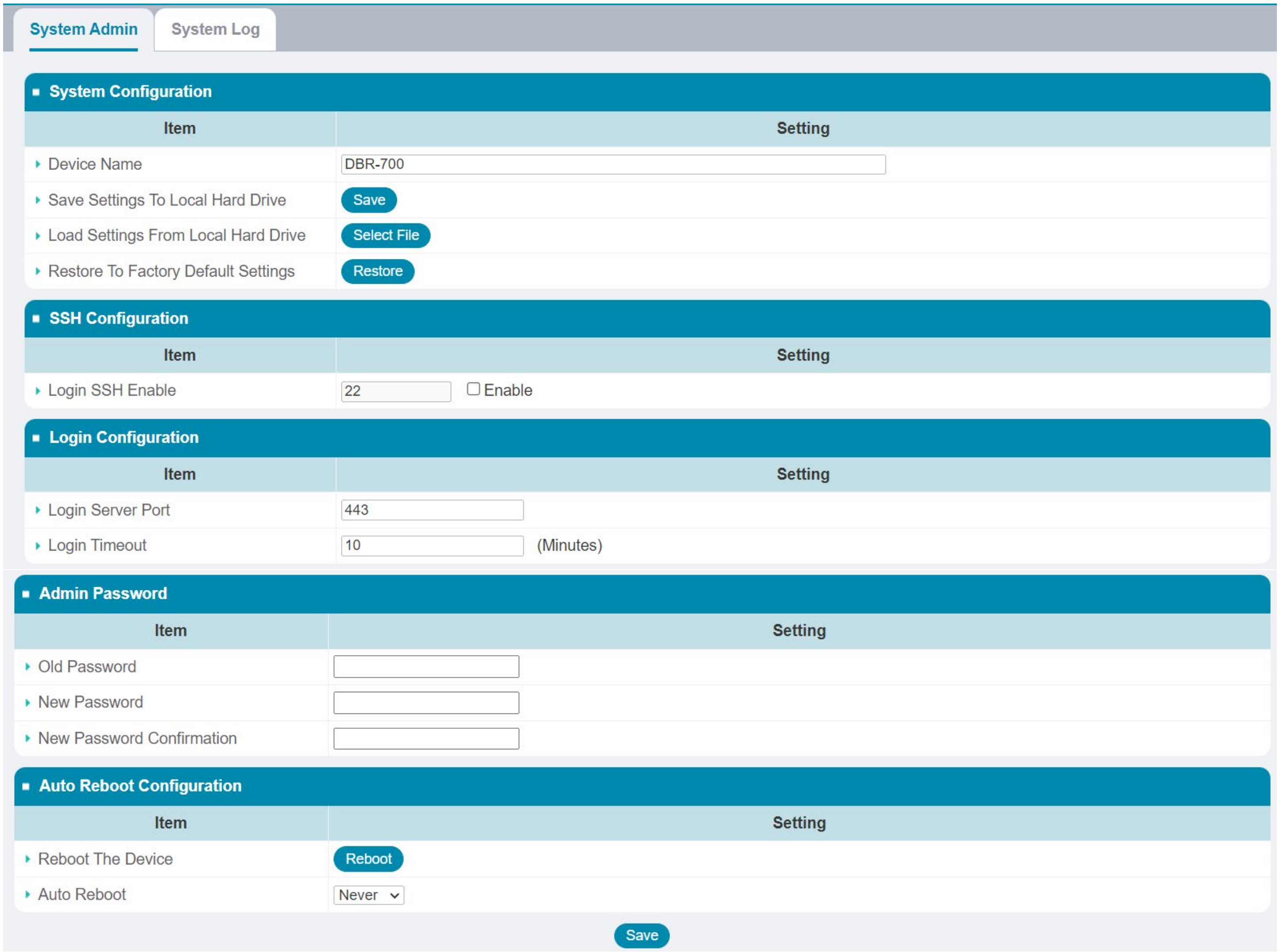
Item	Setting	Action
Friday	Fri : 0:00 - 24:00	Edit □

Name: Friday

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Mon																								
Tue																								
Wed																								
Thu																								
Fri	0:00 - 24:00																							
Sat																								
Sun																								

6.2 System Admin

6.2.1 System Admin



System Configuration

Item	Setting
Device Name	DBR-700
Save Settings To Local Hard Drive	Save
Load Settings From Local Hard Drive	Select File
Restore To Factory Default Settings	Restore

SSH Configuration

Item	Setting
Login SSH Enable	22 ☐ Enable

Login Configuration

Item	Setting
Login Server Port	443
Login Timeout	10 (Minutes)

Admin Password

Item	Setting
Old Password	
New Password	
New Password Confirmation	

Auto Reboot Configuration

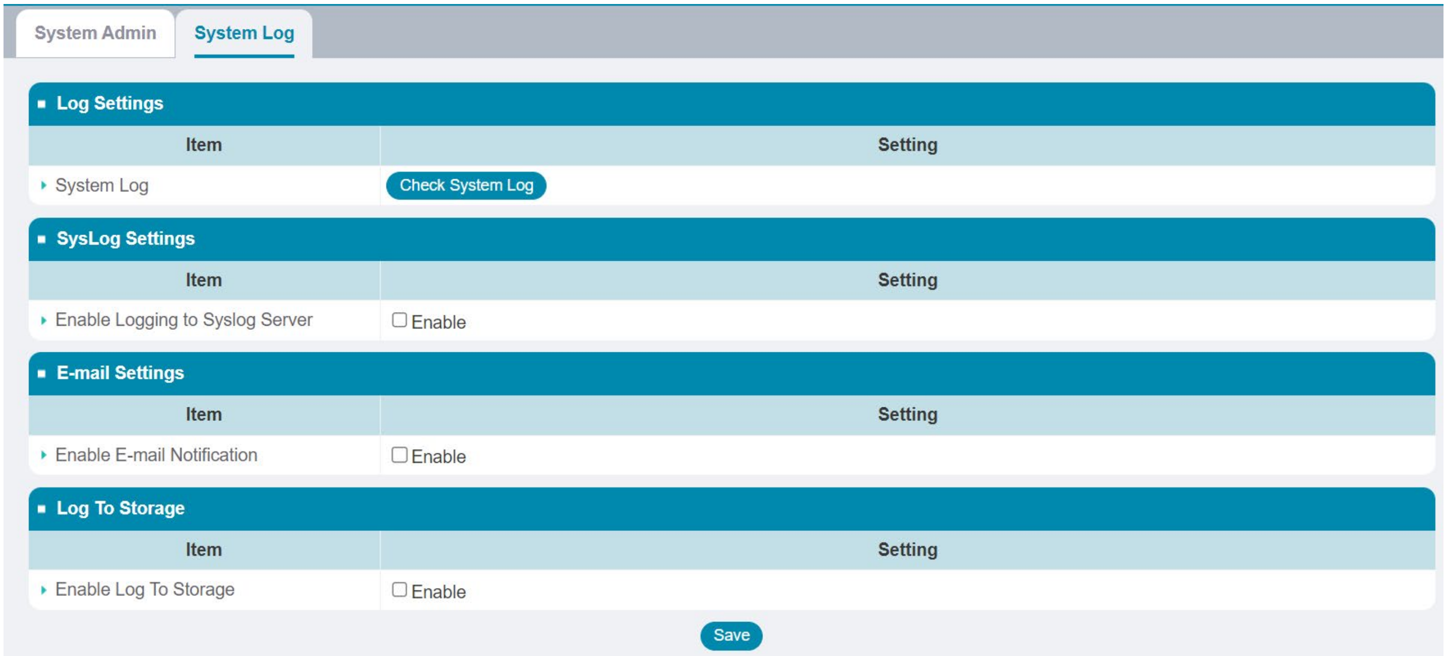
Item	Setting
Reboot The Device	Reboot
Auto Reboot	Never

The fields available on this page are as follows:

Field	Description
System Configuration	
Device Name	Sets the hostname or identifier of the device.
Save Settings To Local Hard Drive	Exports and saves current configuration to a file on the local PC.
Load Settings From Local Hard Drive	Uploads and restores configuration from a previously saved file.
Restore To Factory Default Settings	Resets the device to its original factory default settings.
Login Configuration	
Login Server Port	Sets the port number used for accessing the web management interface.
Login Timeout	Defines the inactivity timeout period before the user is logged out.
Admin Password	
Old Password	Enter the current admin password to authorize password change.

New Password	Enter the new password for the admin account.
New Password Confirmation	Re-enter the new password to confirm and avoid typos.
Auto Reboot Configuration	
Reboot The Device	Manually restarts the device immediately.
Auto Reboot	Configures automatic reboot schedule (e.g., daily, weekly, etc.). Default is Never.

6.2.2 System log



Log Settings

Item	Setting
System Log	Check System Log

SysLog Settings

Item	Setting
Enable Logging to Syslog Server	□ Enable

E-mail Settings

Item	Setting
Enable E-mail Notification	□ Enable

Log To Storage

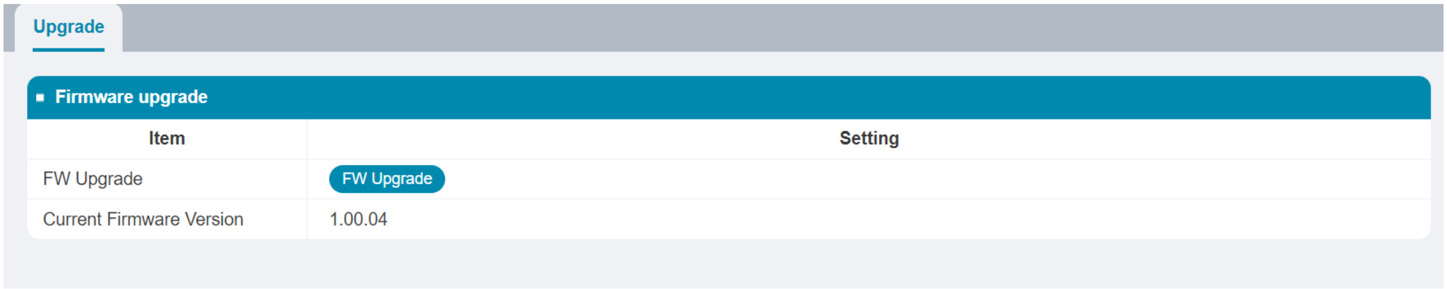
Item	Setting
Enable Log To Storage	□ Enable

The fields available on this page are as follows:

Field	Description
System Log	Allows the user to download system log file.
Enable Logging to Syslog Server	Enables sending logs to an external Syslog server for centralized log management.
Enable E-mail Notification	Enables the device to send alert or system notification emails.
Enable Log To Storage	Allows logs to be saved locally on the device’s storage (if storage is available).

6.3 Upgrade

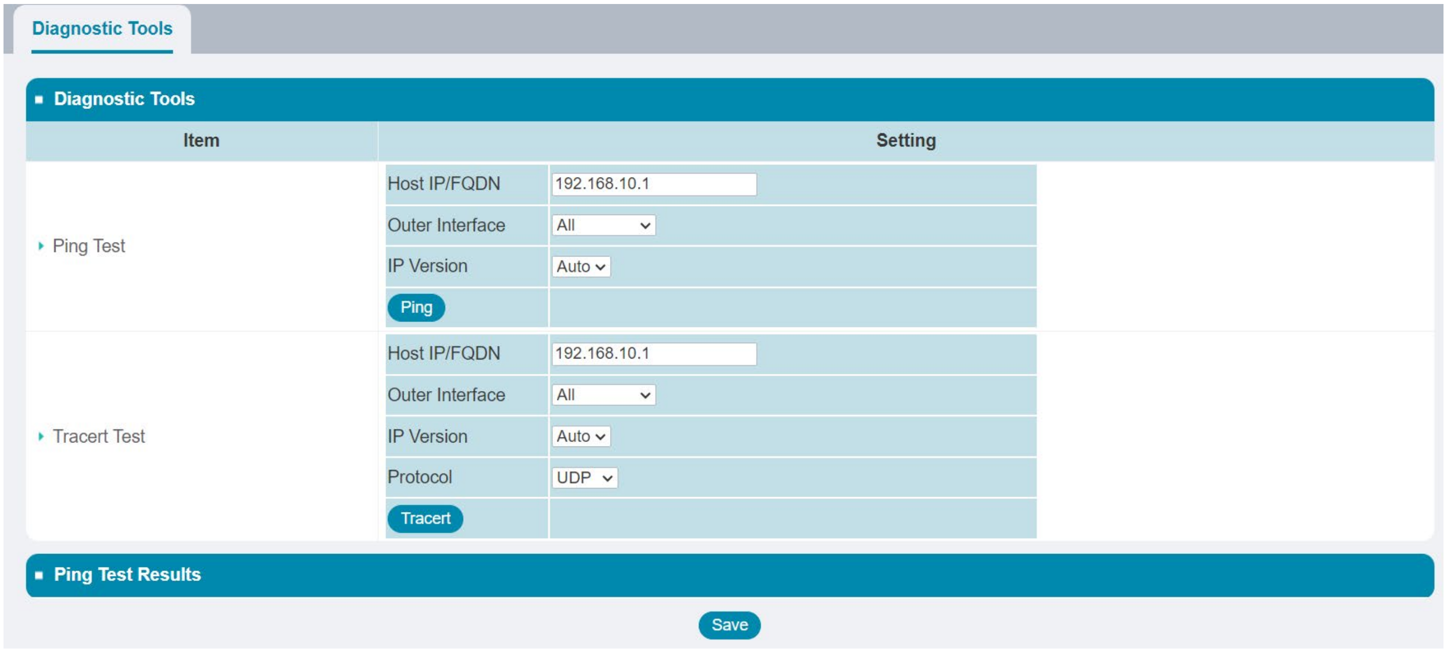
This section allows you to upgrade the device firmware.



Item	Setting
FW Upgrade	FW Upgrade
Current Firmware Version	1.00.04

6.4 Diagnostic Tools

Diagnostic Tools help users check network connectivity and routing. Use Ping Test to see if a device is reachable, and Tracert Test to trace the route packets take to a destination.



Item	Setting	
Ping Test	Host IP/FQDN	192.168.10.1
	Outer Interface	All
	IP Version	Auto
	Ping	
Tracert Test	Host IP/FQDN	192.168.10.1
	Outer Interface	All
	IP Version	Auto
	Protocol	UDP
	Tracert	

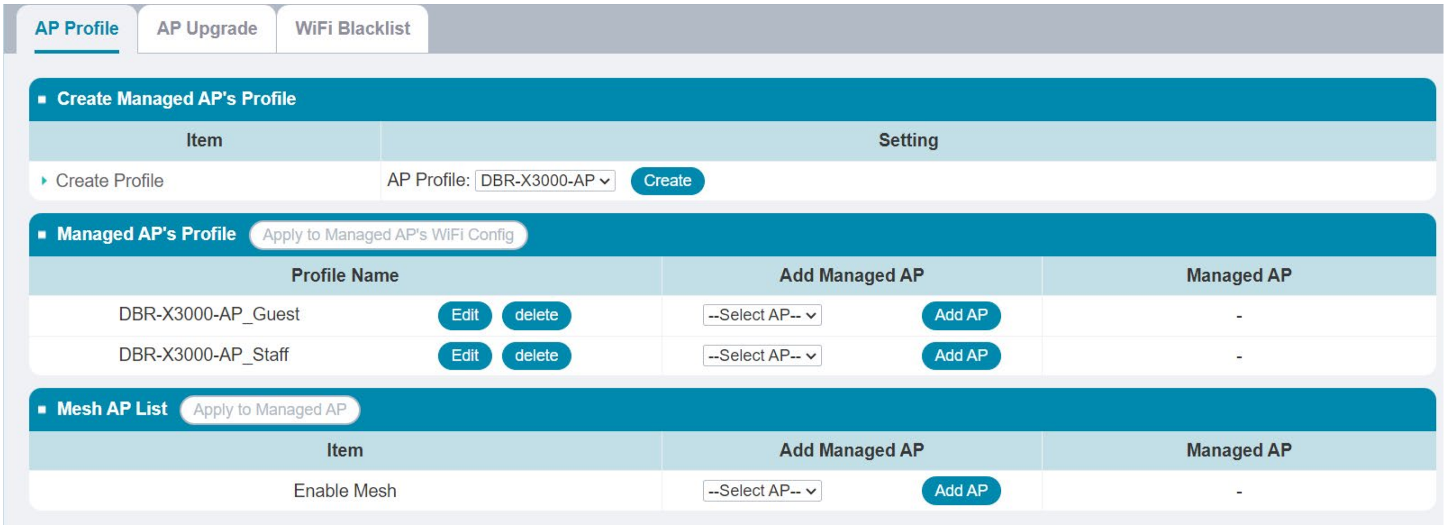
The fields available on this page are as follows:

Field	Description
Ping Test	
Host IP/FQDN	The destination IP address or Fully Qualified Domain Name to ping.
Outer Interface	Select the WAN interface to send the ping from.
IP Version	Select the IP protocol version to use.
Ping Button	Click to start the ping test.
Tracert Test	
Host IP/FQDN	The target IP address or domain to trace.
Outer Interface	Select the outgoing interface for the trace route.
IP Version	Select the IP protocol version to use.

Protocol	Select the protocol type used for traceroute packets.
Tracert Button	Click to initiate the traceroute.

6.5 AP Profile & Upgrade

This section allows you to create and configure the AP profile for the DBR-X3000-AP when it is managed by the DBR-700.



Create Managed AP's Profile

Item	Setting
Create Profile	AP Profile: DBR-X3000-AP

Managed AP's Profile

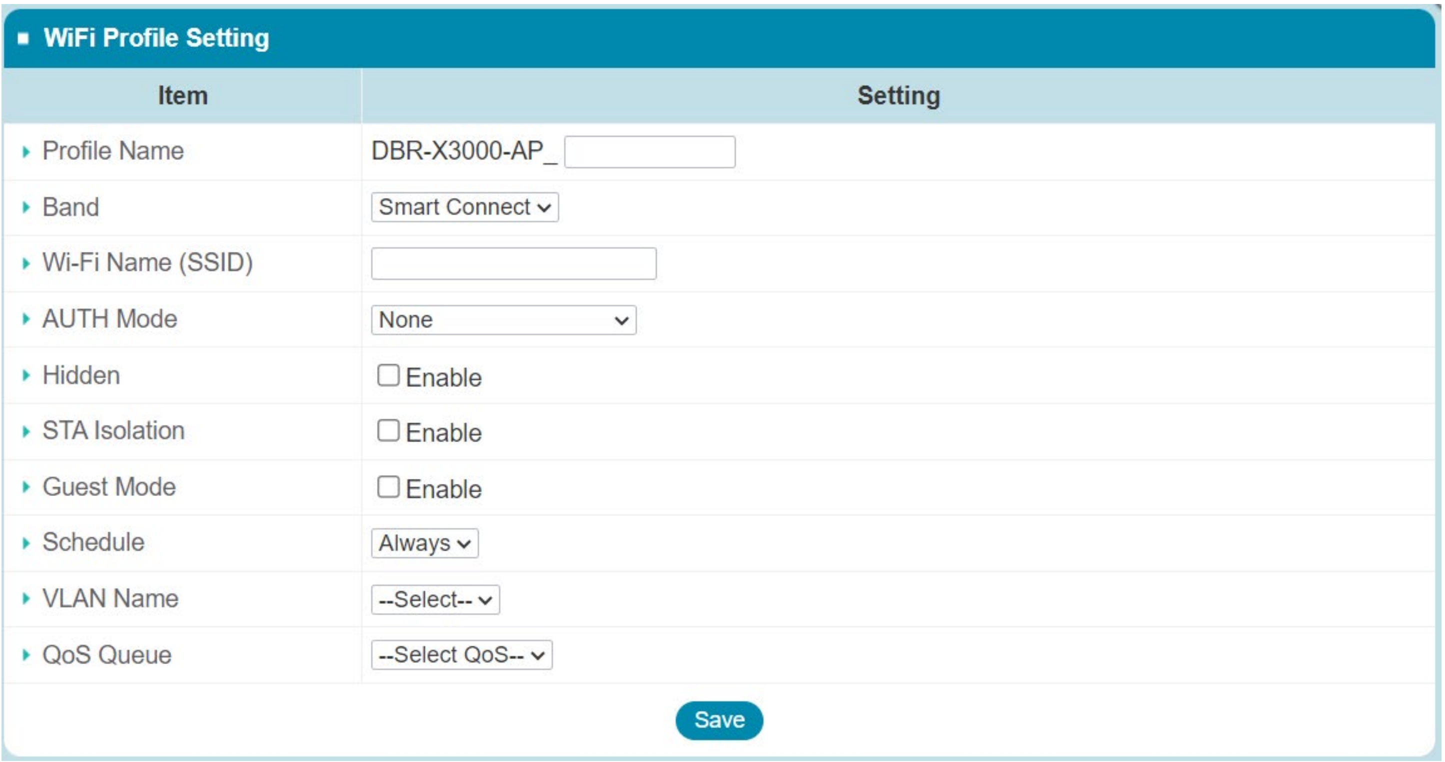
Profile Name	Add Managed AP	Managed AP
DBR-X3000-AP_Guest	--Select AP--	-
DBR-X3000-AP_Staff	--Select AP--	-

Mesh AP List

Item	Add Managed AP	Managed AP
Enable Mesh	--Select AP--	-

6.5.1 AP Profile

Create Profile



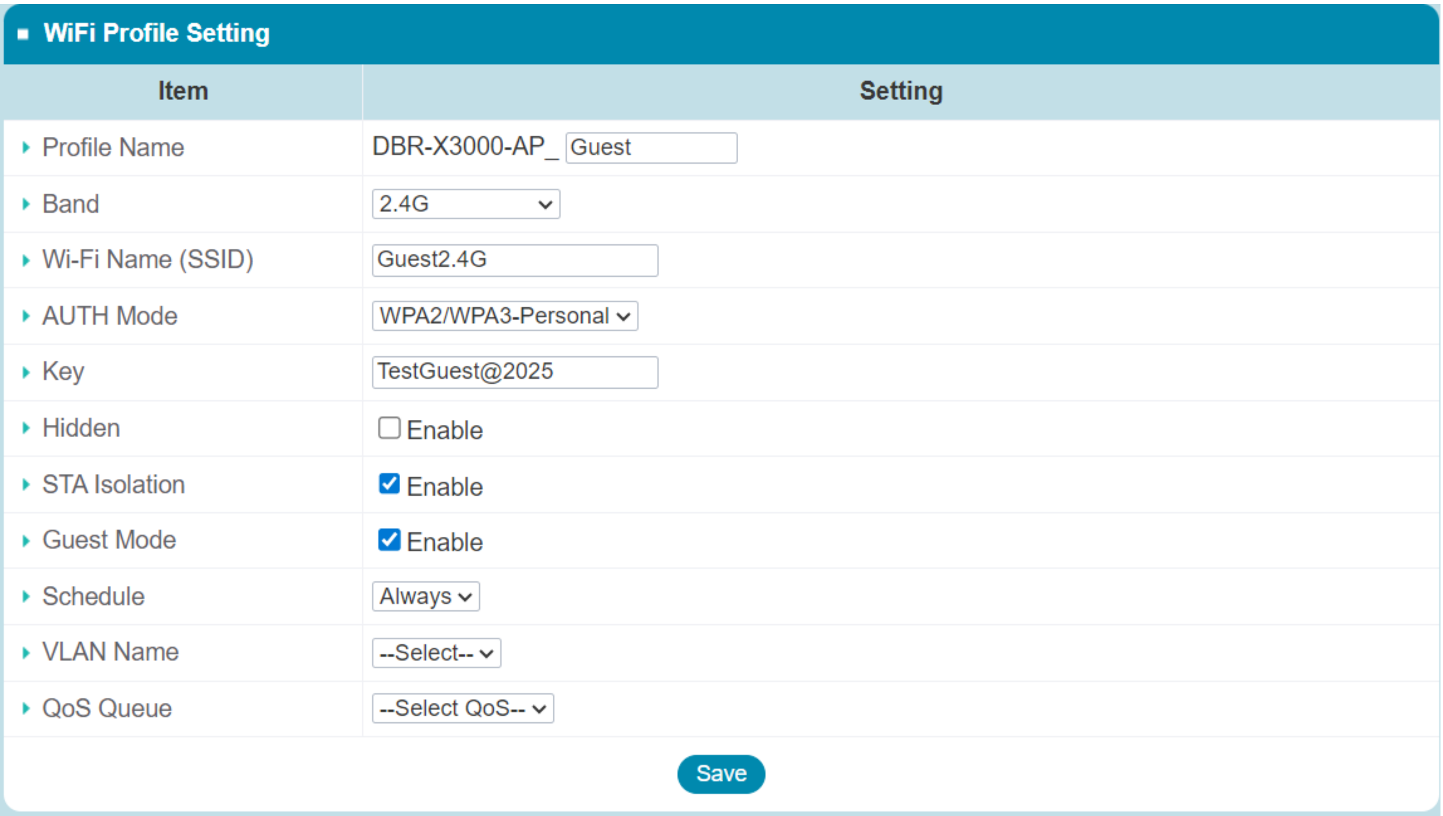
■ WiFi Profile Setting

Item	Setting
Profile Name	DBR-X3000-AP_
Band	Smart Connect
Wi-Fi Name (SSID)	
AUTH Mode	None
Hidden	□ Enable
STA Isolation	□ Enable
Guest Mode	□ Enable
Schedule	Always
VLAN Name	--Select--
QoS Queue	--Select QoS--

The fields available on this page are as follows:

Field	Description
Create Profile	Select the type of AP to create a new profile for.
Profile Name	Defines the unique name for this Wi-Fi profile.
Band	Selects which wireless frequency band to use. Smart Connect automatically selects the best band.
Wi-Fi Name (SSID)	Sets the name (SSID) broadcasted for wireless access.
AUTH Mode	Determines the authentication/encryption method used to secure the network.
Hidden	If enabled, the SSID will not be visible in scan results. Devices must enter it manually to connect.
STA Isolation	Prevents wireless clients from communicating with each other within the same SSID.
Guest Mode	Creates a separate network for guests, isolated from the main LAN.
Schedule	Sets the time period during which the SSID is active.
VLAN Name	Binds the Wi-Fi profile to a specific VLAN for network segmentation.
QoS Queue	Assigns priority for traffic from this SSID using QoS (Quality of Service).

Managed AP's Profile



WiFi Profile Setting

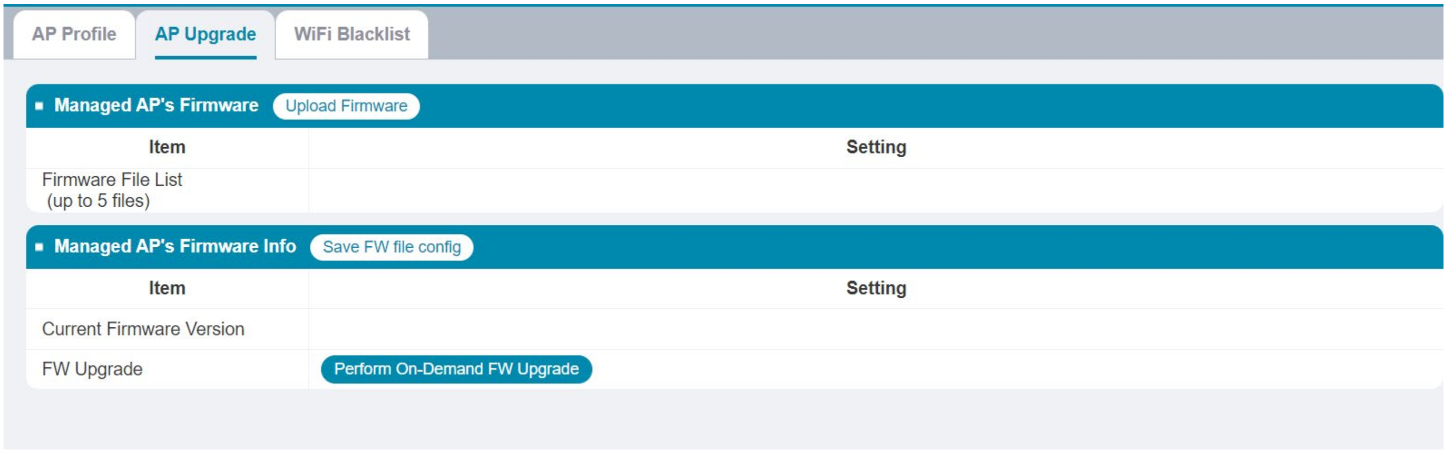
Item	Setting
Profile Name	DBR-X3000-AP_ Guest
Band	2.4G
Wi-Fi Name (SSID)	Guest2.4G
AUTH Mode	WPA2/WPA3-Personal
Key	TestGuest@2025
Hidden	□ Enable
STA Isolation	☑ Enable
Guest Mode	☑ Enable
Schedule	Always
VLAN Name	--Select--
QoS Queue	--Select QoS--

The fields available on this page are as follows:

Field	Description
Profile Name	Defines the unique name for this Wi-Fi profile.
Band	Selects the wireless frequency band for this SSID.
Wi-Fi Name (SSID)	Sets the name (SSID) broadcasted for wireless access.
AUTH Mode	Determines the authentication/encryption method used to secure the network.
Hidden	Hides the SSID from being publicly broadcasted.
STA Isolation	Prevents clients connected to the same SSID from communicating with each other.
Guest Mode	Creates a separate network for guests, isolated from the main LAN.
Schedule	Sets the time period during which the SSID is active.
VLAN Name	Assigns this SSID to a specific VLAN for network segmentation.
QoS Queue	Assigns priority for traffic from this SSID using QoS (Quality of Service).

6.5.2 AP Upgrade

This section allows you to manage firmware upgrades for managed Access Points (APs).



Item	Setting
Firmware File List (up to 5 files)	

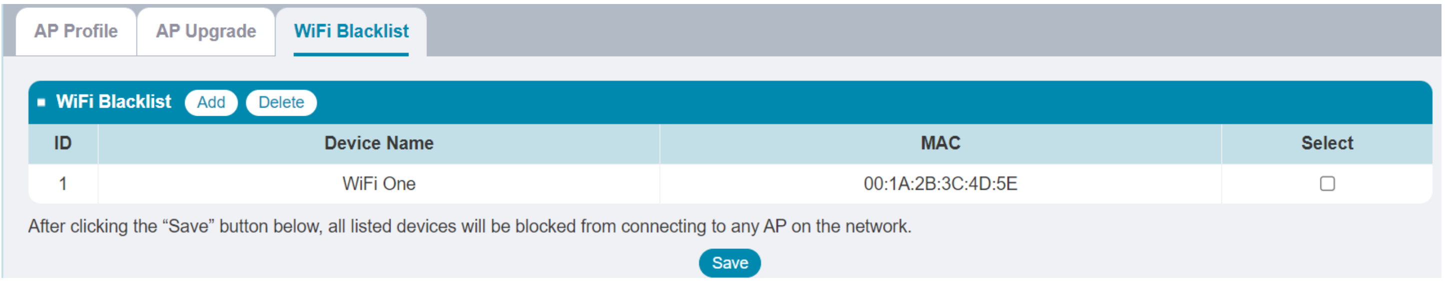
Item	Setting
Current Firmware Version	
FW Upgrade	Perform On-Demand FW Upgrade

The fields available on this page are as follows:

Field	Description
Upload Firmware	Upload new firmware files to the system.
Firmware File List	Displays the list of uploaded firmware files (maximum 5 files allowed).
Save FW file config	Saves the current firmware configuration file for record or future use.
Current Firmware Version	Shows the currently installed firmware version on the managed AP.
FW Upgrade	Manually triggers the firmware upgrade process immediately.

6.5.3 WiFi Blacklist

This section allows you to block Wi-Fi clients by adding their MAC addresses to the blacklist.



ID	Device Name	MAC	Select
1	WiFi One	00:1A:2B:3C:4D:5E	□

After clicking the “Save” button below, all listed devices will be blocked from connecting to any AP on the network.