8) Radius port

User can configure the port number of the radius server.

9) Encryption

User can configure the encryption method when communicating with the radius sever either as AES or TKIP/AES.

10) Radius key

User must enter the radius key value which is given by the radius server.

11) Password

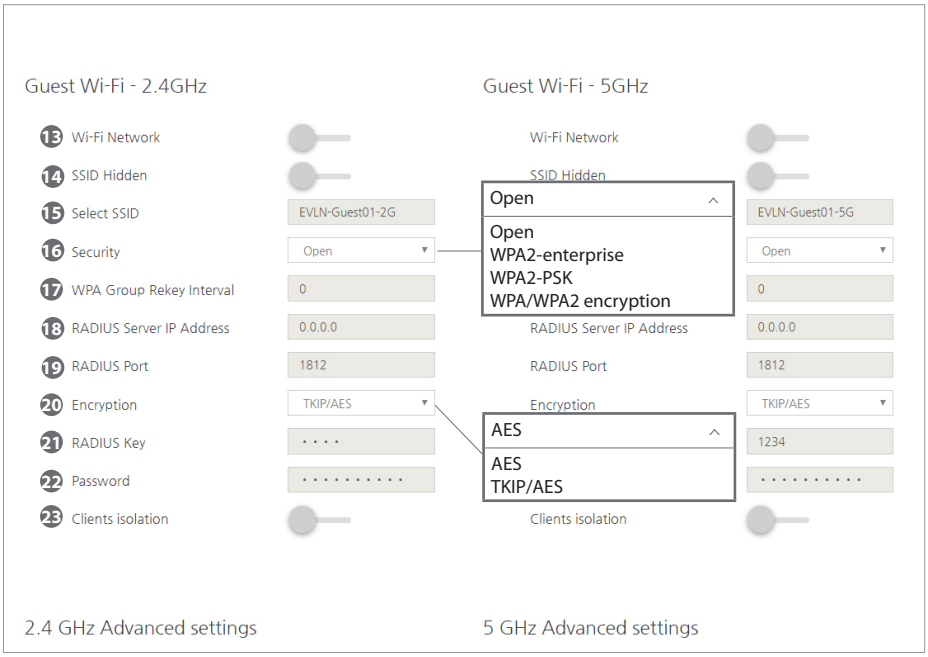
User can configure the password for the selected SSID connection.

12) Encryption

User can enable or disable the client isolation function. With this function, the clients under this WiFi interface can not communicate each other.

9.1.2 Wi-Fi – Guest Wi-Fi 2.4GHz & 5GHz Setting

* 2.4GHz and 5GHz configuration menus are same.



13) WiFi network
User can enable or disable the Wi-Fi network.

14) SSID hidden
User can hide the SSID.

15) Service type
User can create the SSID.

16) Security
User can select one of the following security mode: Open, WPA2-enterprise, WPA2-PSK, WPA/WPA2 encryption.

17) WPA group rekey interval
User can configure the WPA group key renewal time. "0" means the key is not being regenerated.
The unit is second.

18) Radius server IP address
User can configure the IP address of the radius server.

19) Radius port
User can configure the port number of the radius server.

20) Encryption
User can configure the encryption method when communicating with the radius sever either as AES or TKIP/AES.

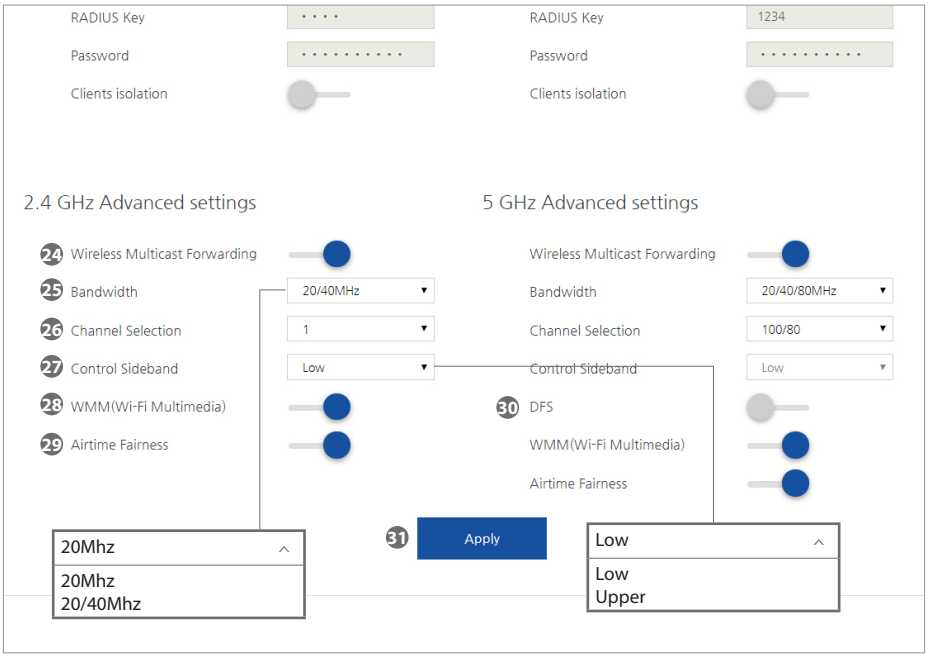
21) Radius key
User must enter the radius key value which is given by the radius server.

22) Password
User can configure the password for the selected SSID connection.

23) Clients isolation
User can enable or disable the client isolation function. With this function, the clients under this WiFi interface can not communicate each other.

9.1.3 Wi-Fi – 2.4GHz & 5GHz Advanced Settings

* 2.4GHz and 5GHz configuration menus are almost same. However a few of menus @ 5GHz is different. In this case, we have additional description in the below table.



24) Wireless multicast forwarding

Wireless multicast forward (WMF) transforms the incoming multicast packets to unicast packets.
User can enable or disable this WMF function.

25) Bandwidth

User can configure the bandwidth at each frequency band.
2.4GHz Options: 20Mhz, 20/40Mhz @ 2.4GHz
5GHz Options: 20Mhz, 20/40Mhz, 20/40/80MHz

26) Channel selection

User can select a specific channel or automatic mode.

27) Control sideband

User can select low channel or upper channel for control messaging.

28) WMM (Wi-Fi Multimedia)

User can enable or disable of the WMM QoS function.

29) Airtime fairness

User can enable or disable of airtime fairness function.
Airtime fairness: Make Intelligent Airtime Scheduling for Wi-Fi QoS.
Improve Wi-Fi QoS by controlling clients airtime usage.

30) DFS (Dynamic Frequency Selection)

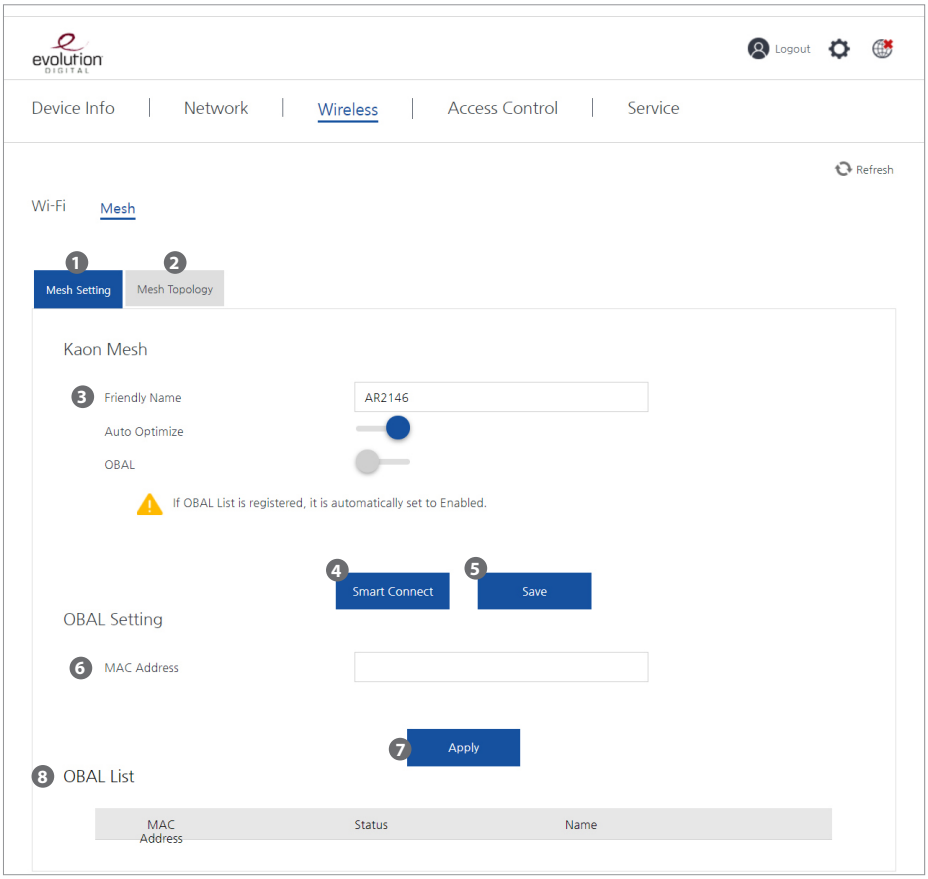
User can enable or disable DFS function.

31) Apply

Click the "Apply" button in order to save settings.

9.2.1 Mesh - Mesh Setting

User can configure regarding Mesh function in this page.



1) Mesh Setting
User can set the Mesh function of the AR2146.

2) Mesh Topology
Mesh topology shows the network map of the AR2146 to the user.

3) Friendly name
User can make a friendly SSID name of the WiFi Mesh so that others can easily find it.

4) Smart Connect
User click "Smart Connect" button to initiate Mesh grouping.

5) Save
Click "Apply" button for applying friendly name.

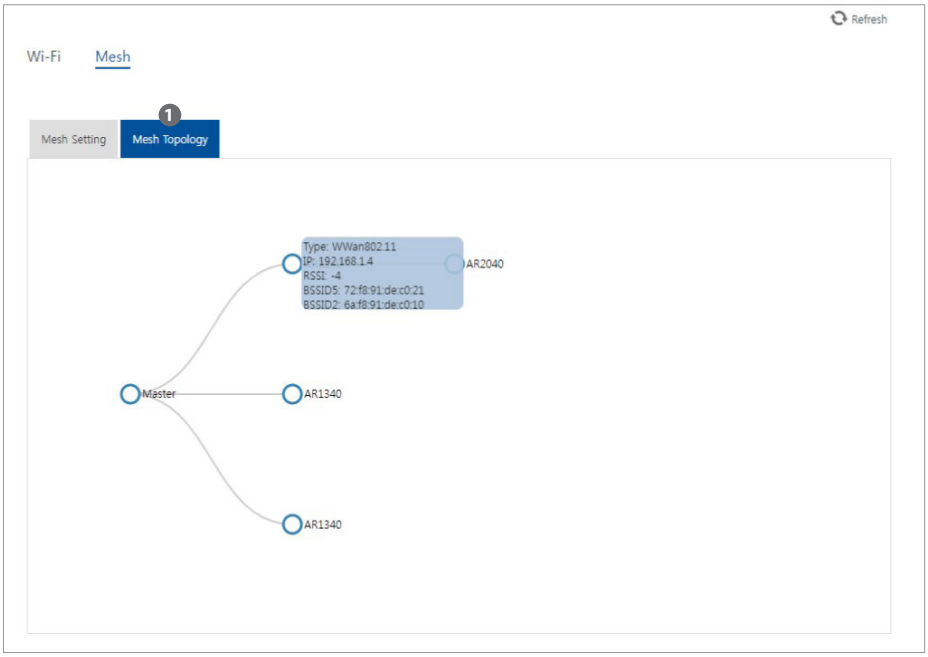
6) MAC address
You can manually enter the MAC addresses of the target repeaters if you cannot make QR code scan. You need to put ":" between the MAC addresses.
e.g. AA:BB:CC:DD:EE:FF

7) Apply
You can save the configureation.

8) OBAL List
OBAL means onboarding extender. This list shows Mesh Node List shows the mesh.

9.2.2 Mesh - Mesh Topology

This page shows the Mesh network topology the AR2146 forms with the Mesh repeaters



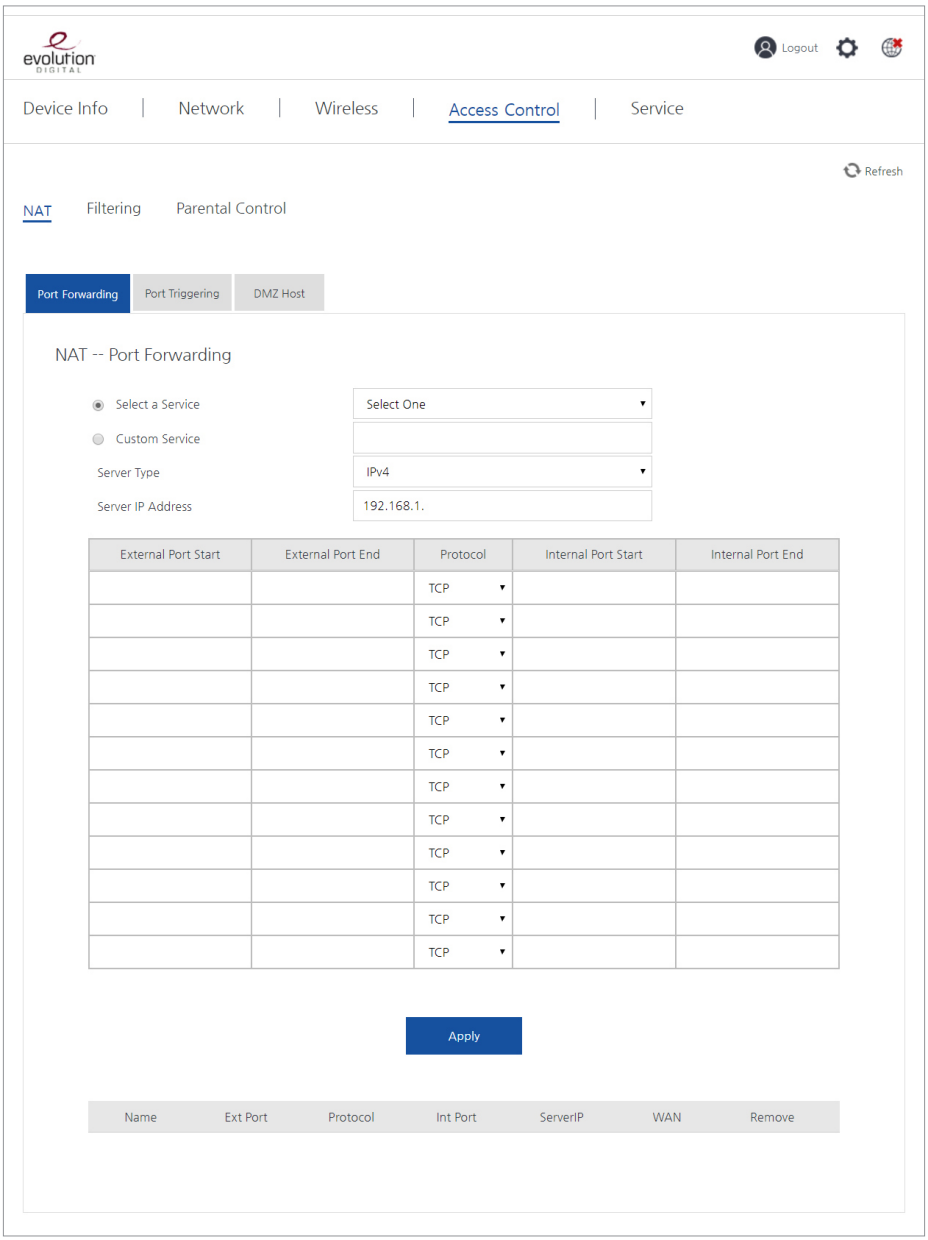
1) Mesh topology

Mesh topology shows the current mesh network between the AR2146 and extenders. It also shows the all clients connected to each node.

10. Access Control Menu

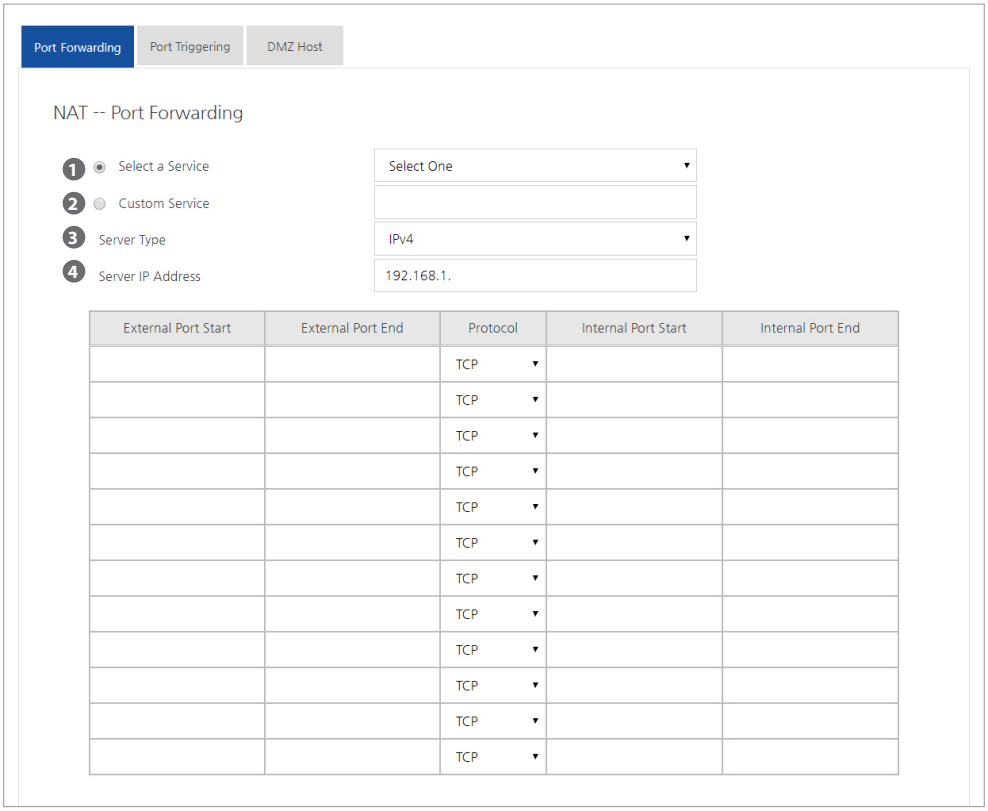
10.1 NAT

A user can configure port forwarding services in this page. The user can choose pre-defined port-forwarding services or make the user's own services. This might need to connect specific devices via the AR2146.
The table shows the external port start numbers, external port end numbers, and their relevant internal port start numbers and internal port end numbers.



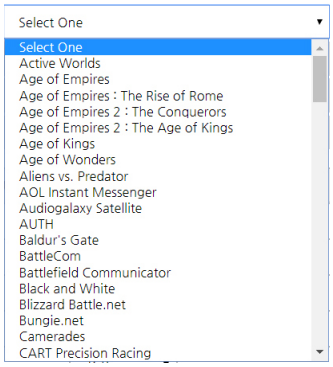
10.1.1 NAT – Port Forwarding

A user can configure port forwarding services in this page. The user can choose pre-defined port-forwarding services or make the user's own services. This might need to connect specific devices via the AR2146.
The table shows the external port start numbers, external port end numbers, and their relevant internal port start numbers and internal port end numbers.



1) Select a Service

You can choose pre-defined port-forwarding services from this section
Predefined services are following;



2) Custom service

You can configure the user's own port-forwarding services by entering service name, service type, server IP address, and related port numbers

3) Service type

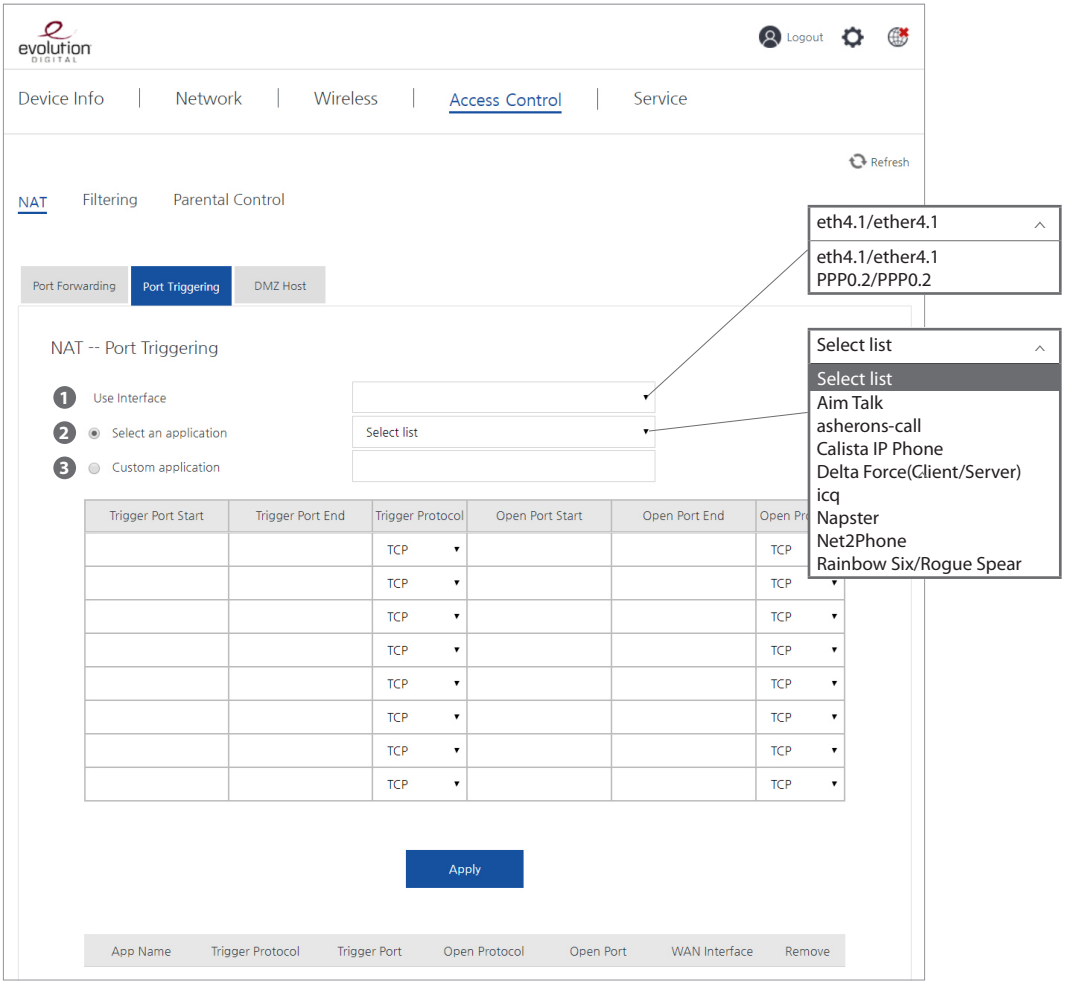
You can select either IPv4 or IPv6.

4) Serve IP Address

You can configure the IP address you want to use for Port Forwarding service.

10.1.2 NAT – Port Triggering

Port triggering is a dynamic form of the port forwarding model. Generally, port triggering is used when the user needs to use port forwarding to reach multiple local computers. However, port triggering is also used when applications need to open incoming ports that are different from the outgoing port.



1) Use interface

User can select either eth4.1/ether4.1 or PPP0.2/PPP0.2 interface.

2) Select an application

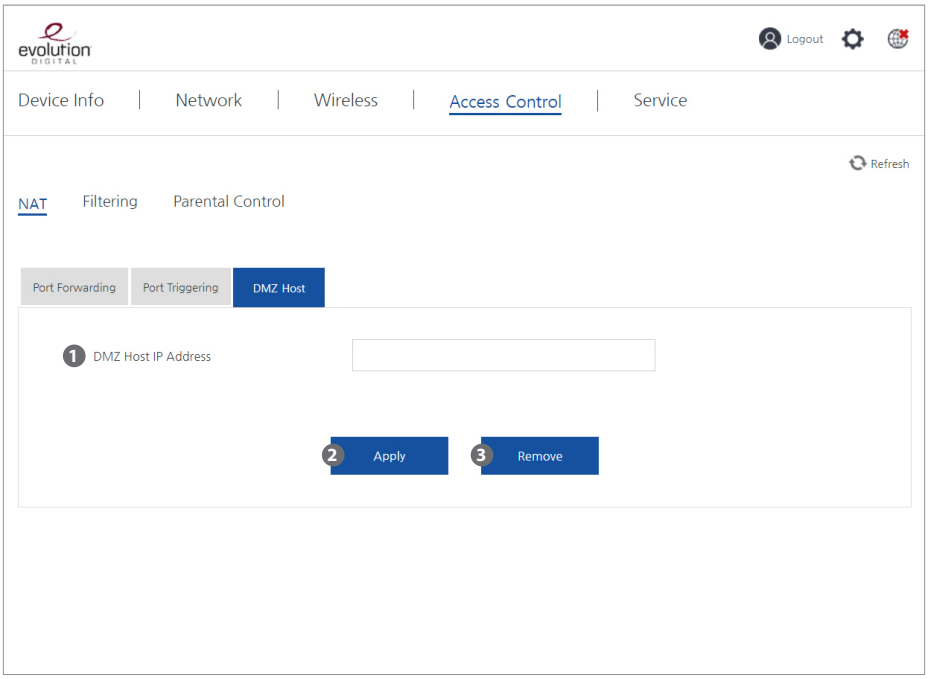
User can select pre-defined application to enable Port Triggering.

3) Custom application

User can configure the user's own port-triggering services by writing the application name and relevant triggering ports and the open ports in the table.

10.1.3 NAT – DMZ Host

DMZ stands for Demilitarized Zone. User only enables the DMZ in a specific case.



1) DMZ Host IP Address

Enter the IP address of the client that user wants to expose.

2) Apply

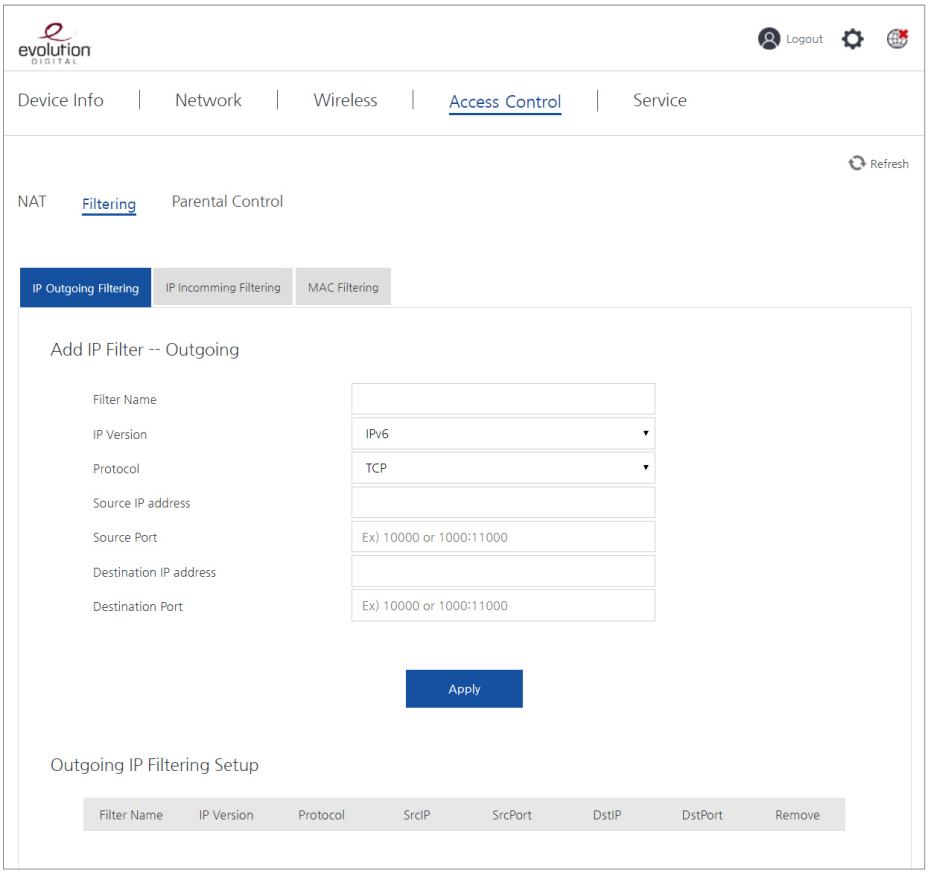
Click "Apply" button, then the IP address user entered will be exposed.

3) Remove

Click "Remove" button, then the exposure of client's IP address will be removed.

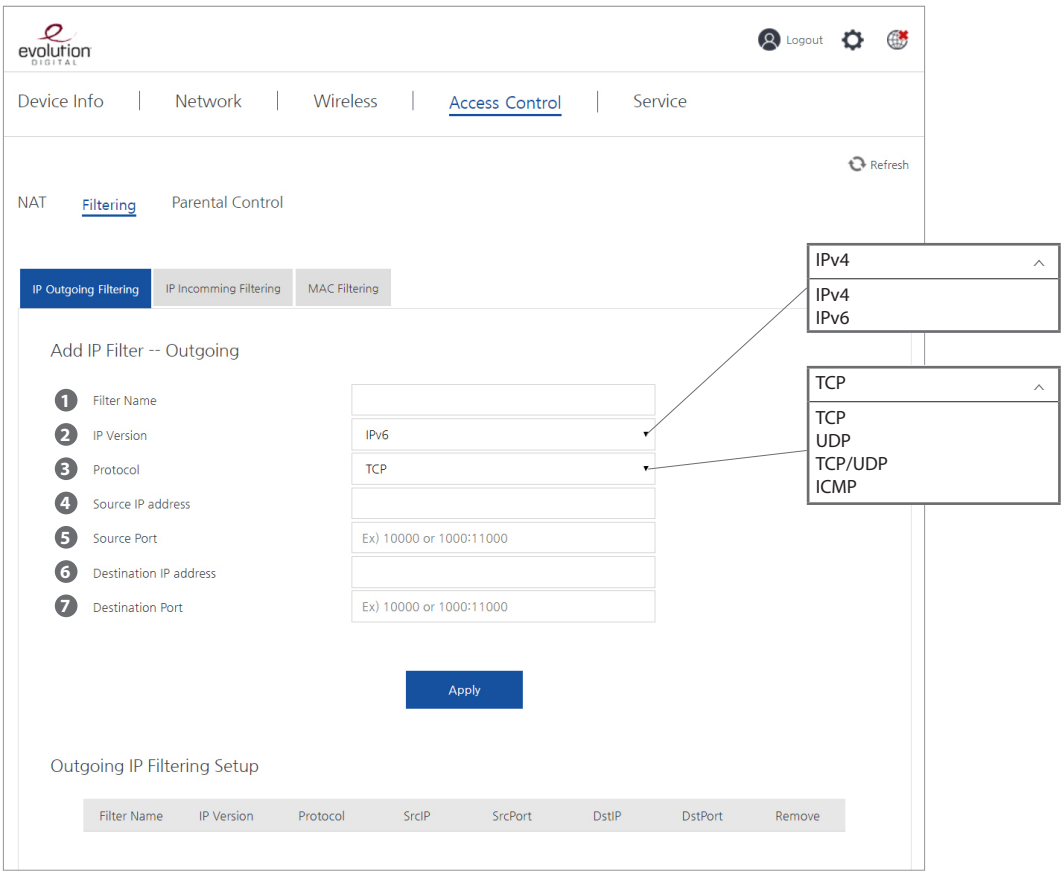
10.2. Filtering

In this page, you can configure a IP address and service type for filtering out.



10.2.1 Filtering – IP Outgoing Filtering

In IP outgoing filtering page, user can configure outbound filter as one of the firewall functions. In order to complete IP outgoing filter, the user must fill in all the following columns.



1) Filter name
User can make the name of the new filter entry.

2) IP version
User can select either IPv4 or IPv6.

3) Protocol
User can select either TCP, UDP, TCP/UDP, or ICMP to filter.

4) Source IP address
User can enter the source IP address to filter.

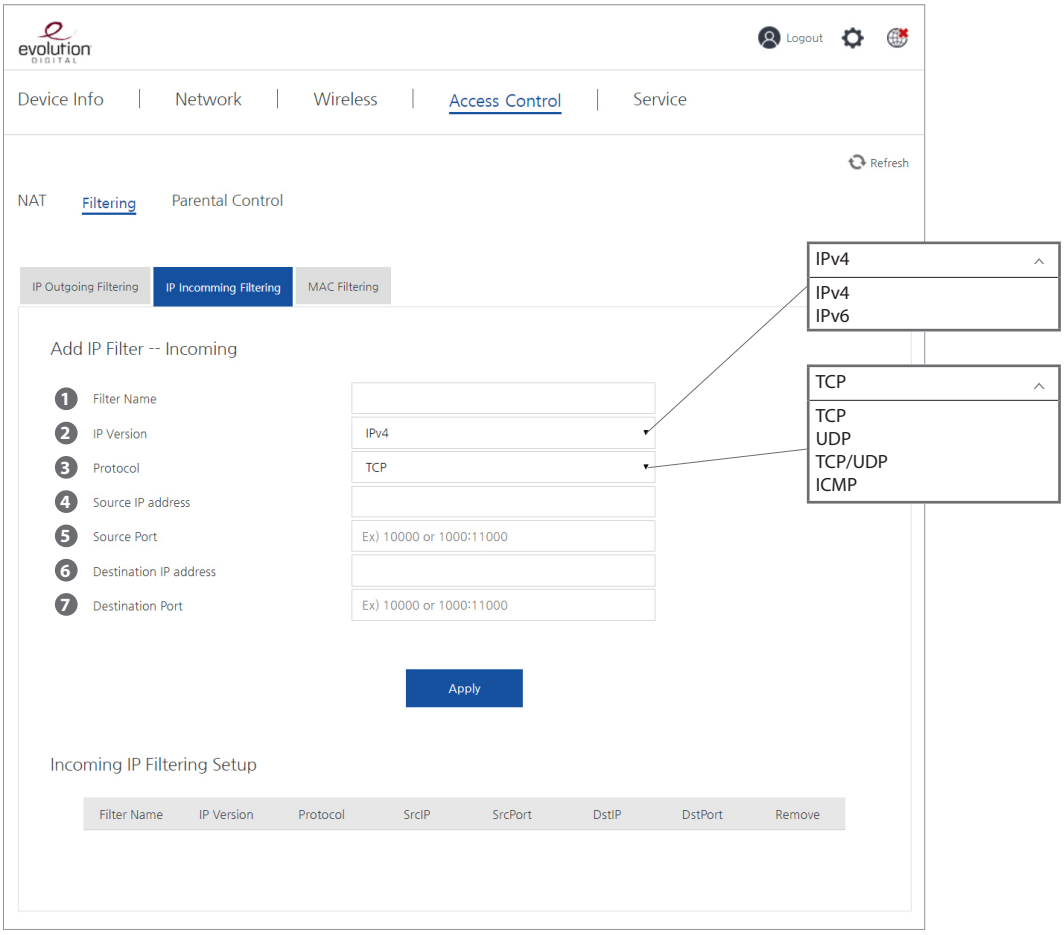
5) Source port
User can enter the source port to filter.

6) Destination IP address
User can enter the destination IP address to filter.

7) Destination port
User can enter the destination port to filter.

10.2.2 Filtering – IP Incomming Filtering

In IP outgoing filtering page, user can configure outbound filter as one of the firewall functions. In order to complete IP outgoing filter, the user must fill in all the following columns.



1) Filter name
User can make the name of the new filter entry.

2) IP version
User can select either IPv4 or IPv6.

3) Protocol
User can select either TCP, UDP, TCP/UDP, or ICMP to filter.

4) Source IP address
User can enter the source IP address to filter.

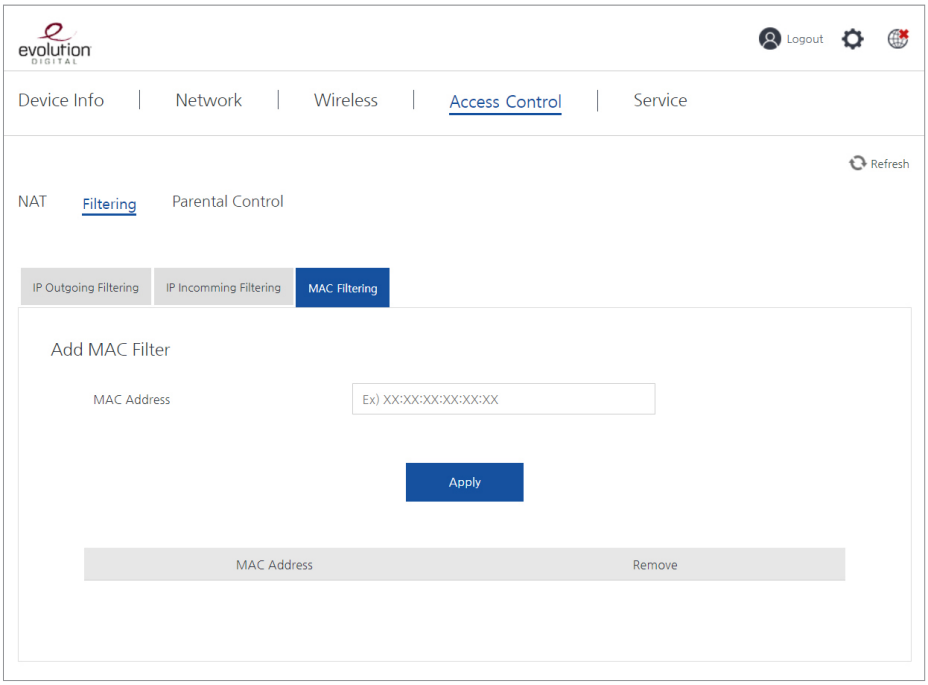
5) Source port
User can enter the source port to filter.

6) Destination IP address
User can enter the destination IP address to filter.

7) Destination port
User can enter the destination port to filter.

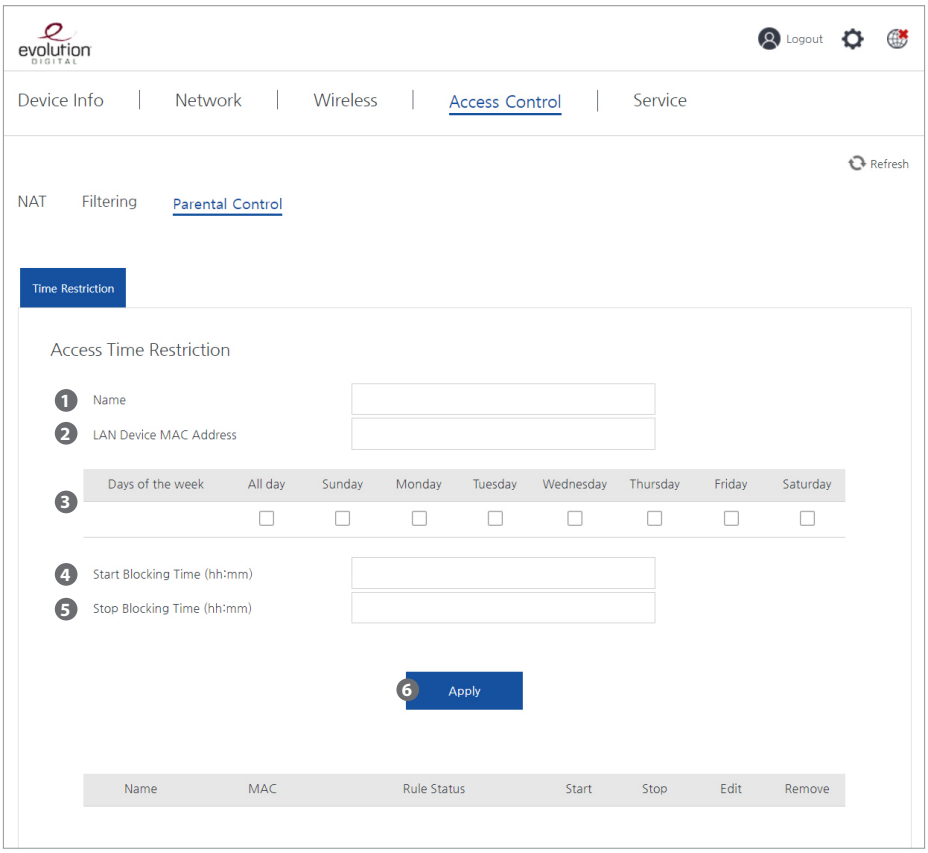
10.2.3 Filtering – MAC Filtering

In MAC filtering page, user can configure the specific device's MAC address to filter out.



10.3. Parental Control

In this page, user can manage the connected client's internet access time.



1) Name
User can make user friendly name for a internet access time control.

2) LAN device MAC address
User can enter the (W)LAN device MAC address to apply the internet access time control.

3) Days of the week
User can select which day to apply the internet access time control.

4) Start blocking time
The time when the internet access is blocked.

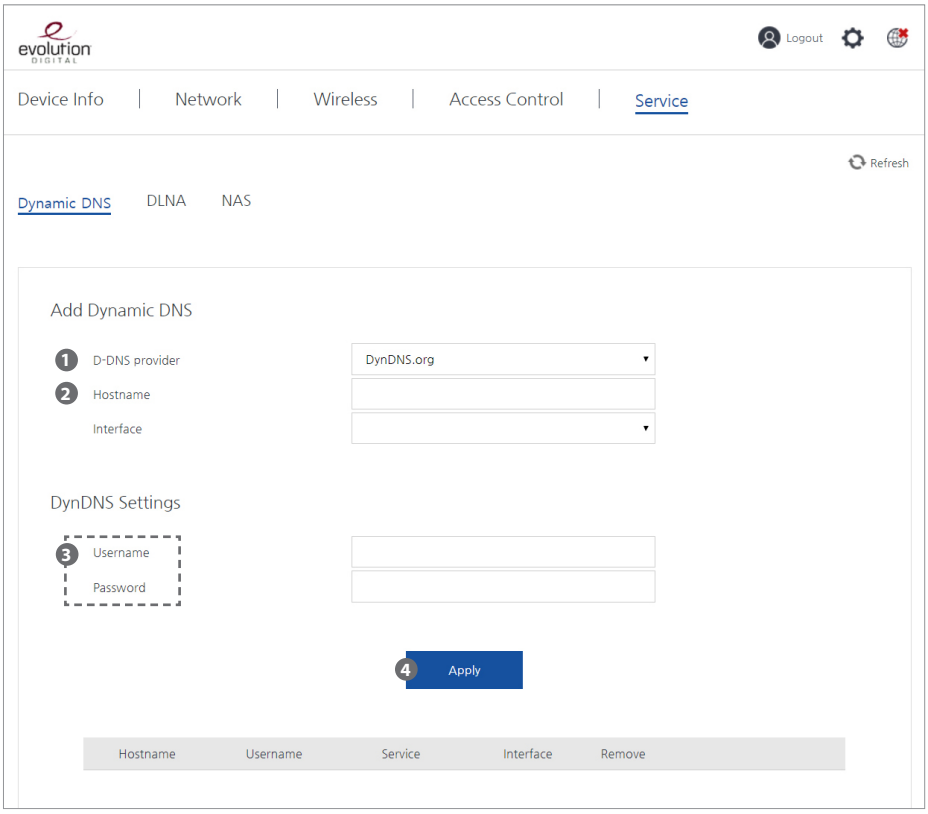
5) Stop blocking time
The time when the internet access is allowed.

6) Apply
Click the "Apply" button in order to save settings.

11. Service Menu

11.1. Dynamic DNS

In this page, a user can configure Dynamic DNS. The user also need to configure port forward a PC after D-DNS setting.



1) D-DNS provider
User can select predefined D-DNS provider from the list.

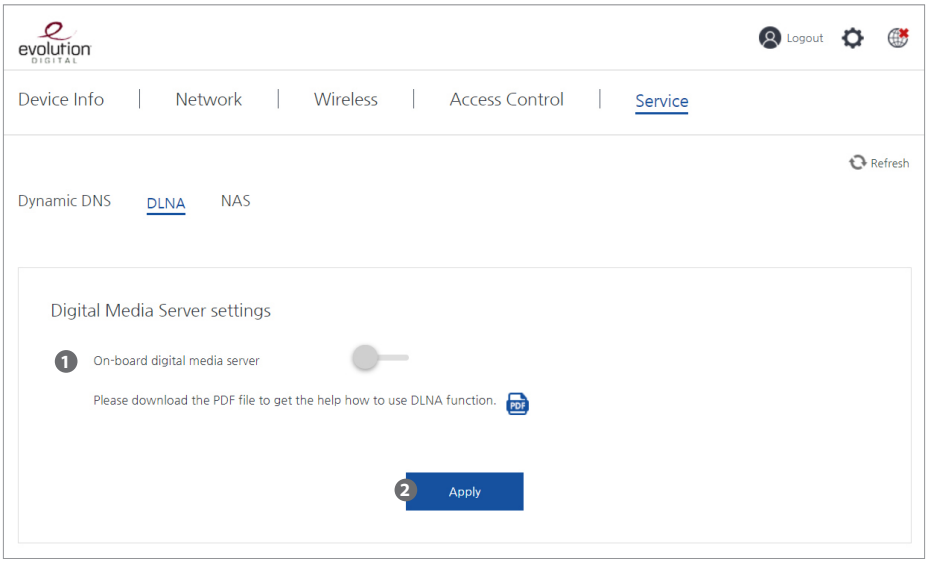
2) Hostname
User can configure a hostname the user want to use for this D-DNS service e.g. xxxx.DynDNS.org.

3) Username and password
User can configure the username and the password to access D-DNS service.

4) Apply
Click the "Apply" button in order to save settings.

11.2. DLNA

A user can enable or disable DLNA service.
DLNA configuration guideline document can be downloaded.

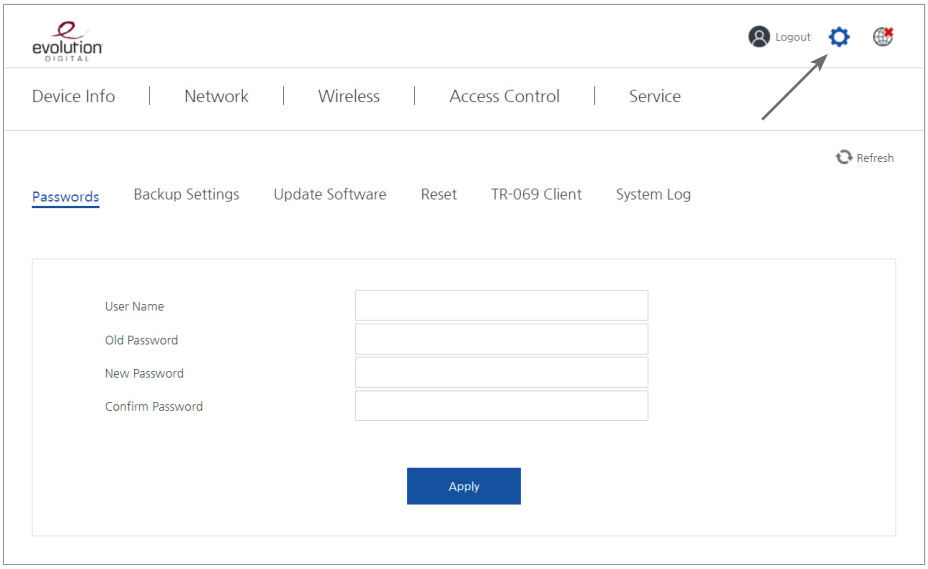


1) On-board digital media server
You can enable or disable the digital media server function.

2) Apply
Click the "Apply" button in order to save setting.

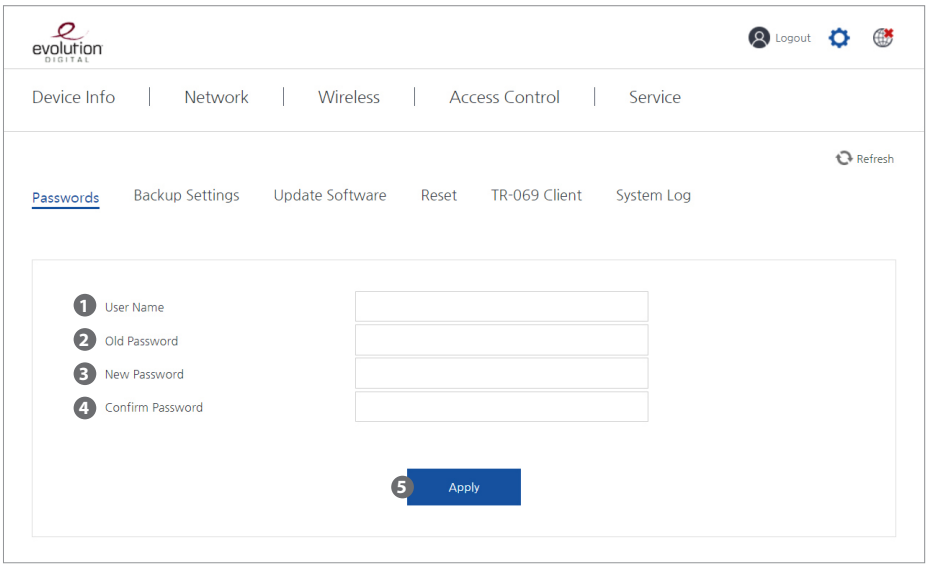
12. Management Setting Menu

This page is for an administrator. Click the icon, , then the user can manage system setting.



12.1. Passwords

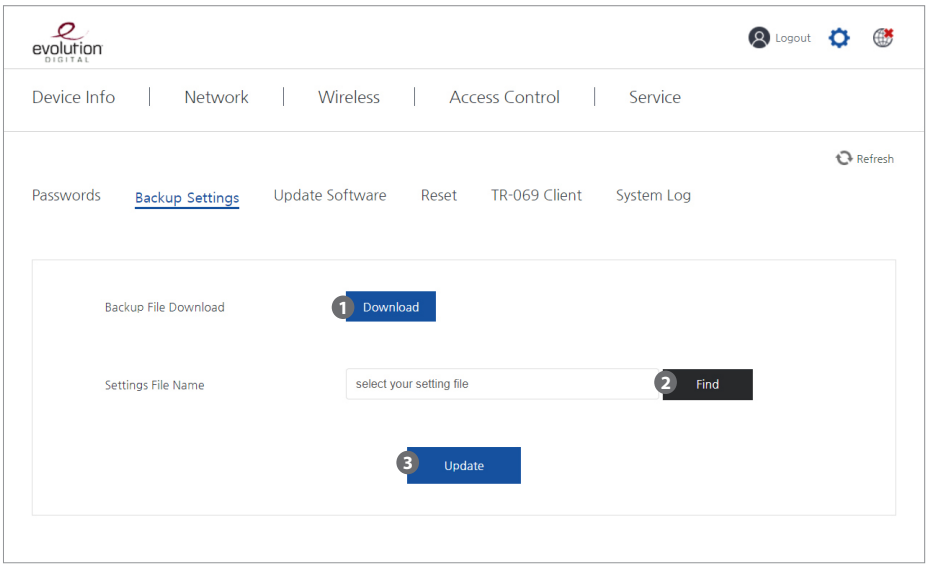
User can change the system password.



1) Username
Enter the username.
2) Old Password
Enter the current password.
3) New Password
Enter the new password.
4) Confirm Password
Re-enter the new password.
5) Apply
Click the "Apply" button to change the password.

12.2. Backup Settings

Users can make a back-up for the current configurations and download into a file.



1) Backup file download

A user can click the Download button to make a back-up file for the current configurations to download.

2) Settings file name and update

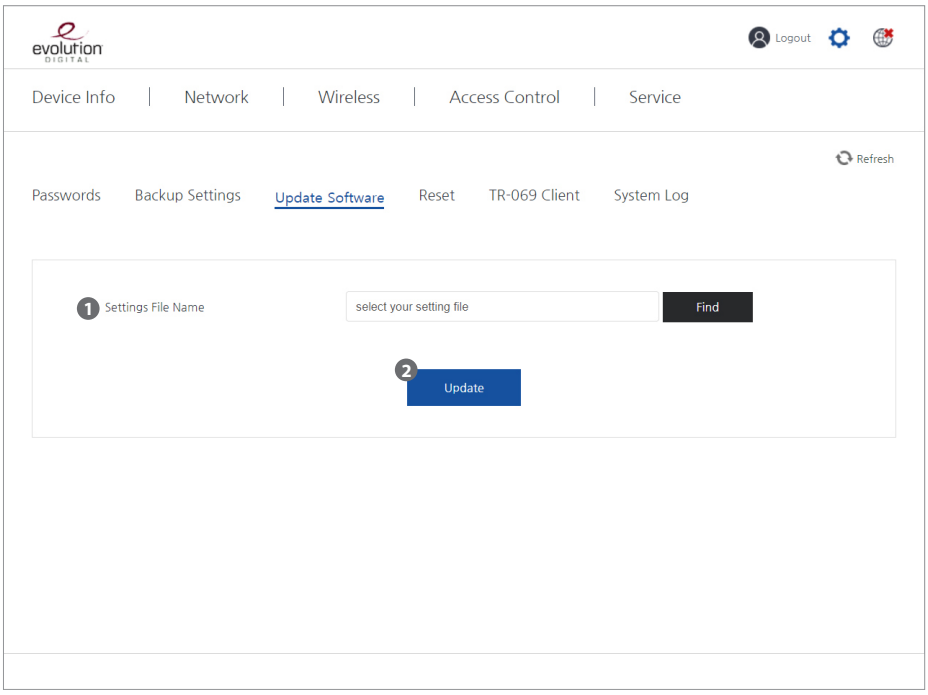
Click the "Find" button and a user can select one of configuration back-up file to apply.

3) Update

Click the "Update" button to save settings.

12.3. Update Firmware

In this page, user can upload CPE firmware file and update.



1) Find a New Firmware

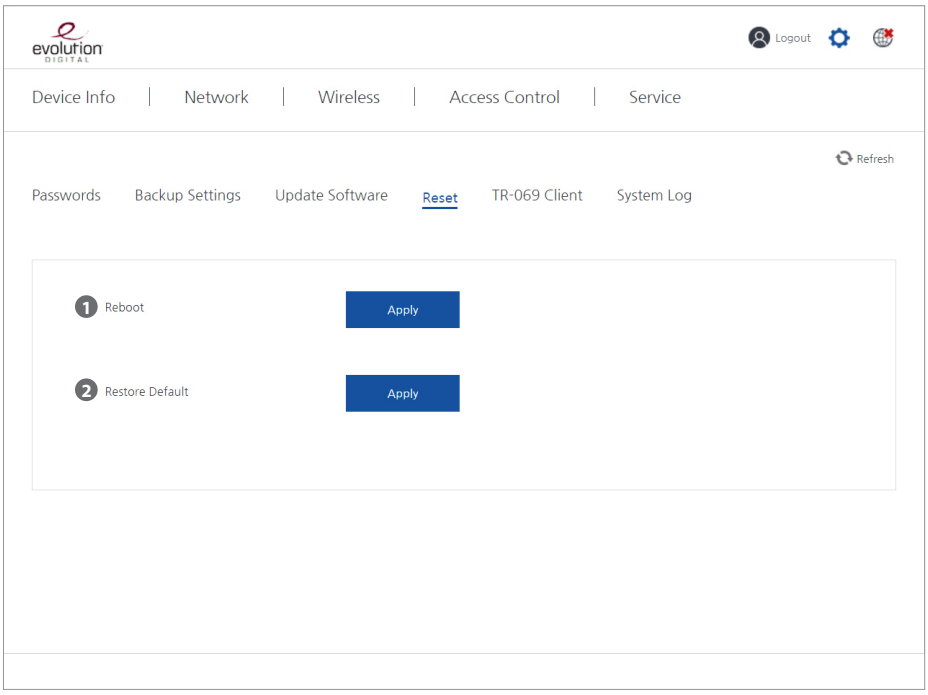
User can find a firmware file for the update.

2) Update

After click the "Update" button, the firmware file is uploaded and updated.

12.4. Reset

User can reboot or factory reset for the AR2146.



1) Reboot

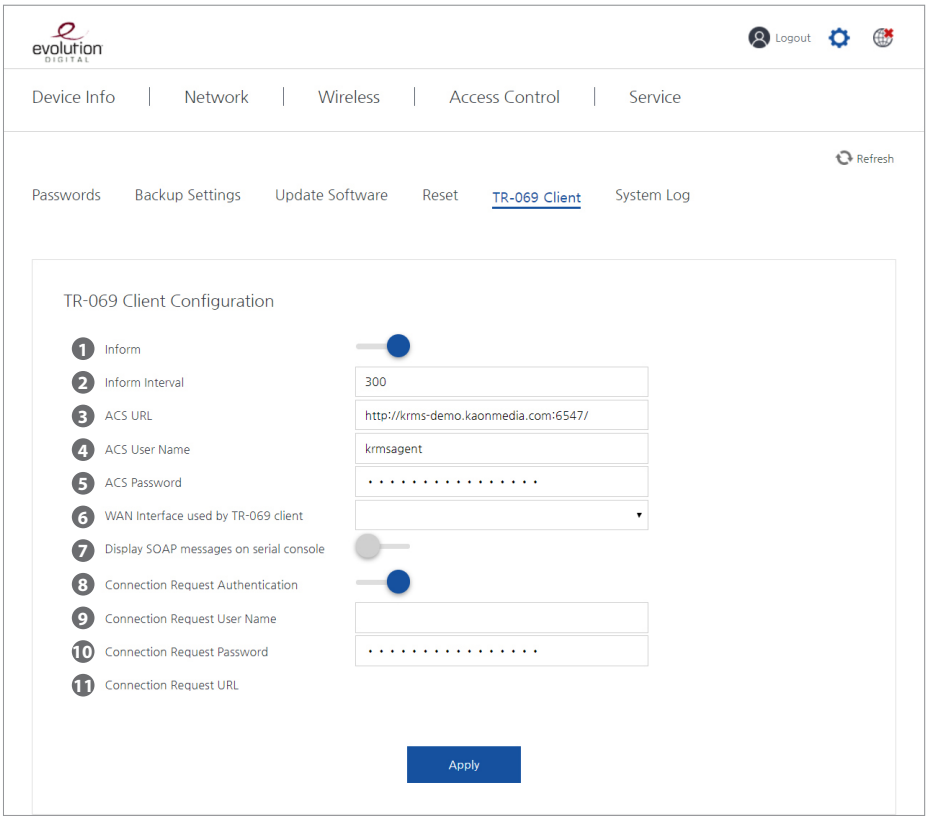
Click "Apply" button to make the AR2146 reboot.

2) Restore Default

Click "Apply" button to make the factory reset for the AR2146.

12.5. TR-069 Client

User can configure Auto Configuration Server(ACS) settings for the TR-069 embedded the CPE (AR2146).



1) Inform

User can enable or disable the TR-069 on the AR2146.

2) Inform Interval

User can set the interval time which the AR2146 communicate with ACS and check the updated data.

3) ACS URL

ACS (Automatic Configuration Server) URL.

4) ACS user name

User can make a friendly user name for a specific ACS server the user is configuring.

5) ACS password

User must enter the password given by the ACS to access it

6) WAN interface used by TR-69 client

User can select which WAN interface to connect to the ACS.
Options: any WAN, eth4.1/eth4.1, ppp0.2/ppp0.2, LAN, loopback.

7) Display SOAP messages on serial console

User can allow or prohibit SOAP message display on serial console.

8) Connection Request Authentication

User can enable or disable "connection request authentication" function.
If "disable" is selected, the following menu disappeared. (connection request user name, connection request pass word, connection request URL)

9) Connection Request user name

User can configure the friendly user name for connection request.

10) Display SOAP messages on serial console

User must enter the password given by the ACS to access it.

11) Connection Request URL

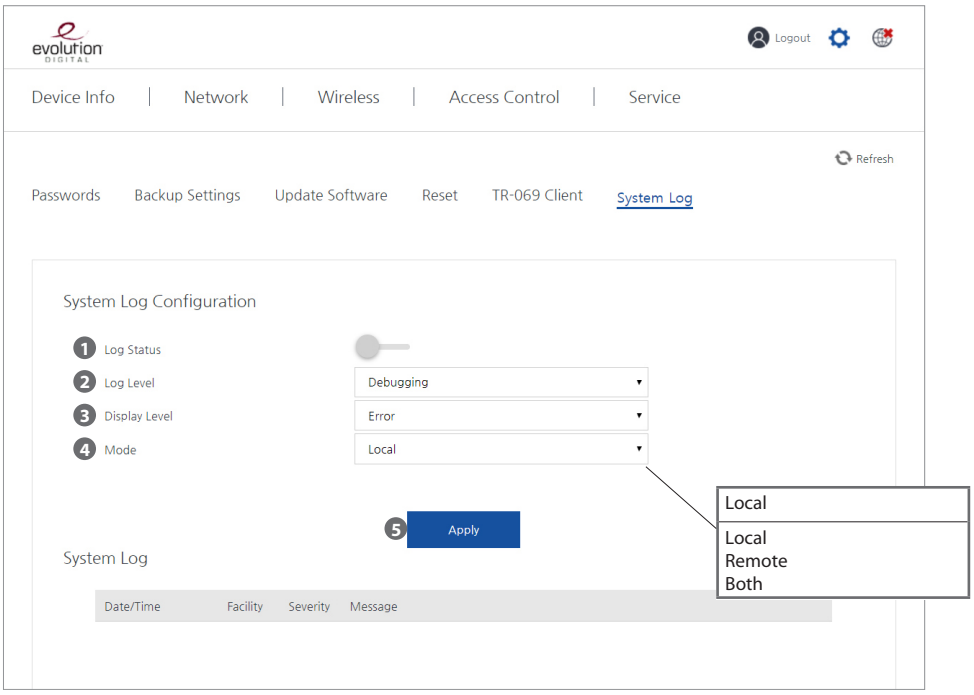
It is usually established automatically. However, the port should be configured in some cases.

12) Apply

Click the "Apply" button for save settings.

12.6. System Log

You can check and configure the system log generated by the AR2146.



1) Log status

You can enable or disable logging function.

2) Log level

User can select one of the following log levels, Emergency, Alert, Critical, Error, Notice, Informational, Warning, and Debugging.

3) Display level

User can select one of the following display levels.

4) Mode

User can select one of the following place to create logs.

Option: Local, Remote, Both.

* When Remote is selected, server IP address column and server UDP port column is displayed.
  A user can configure the server IP address and UDP port.

5) Apply

Click the "Apply" button for save settings.

KAON