

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

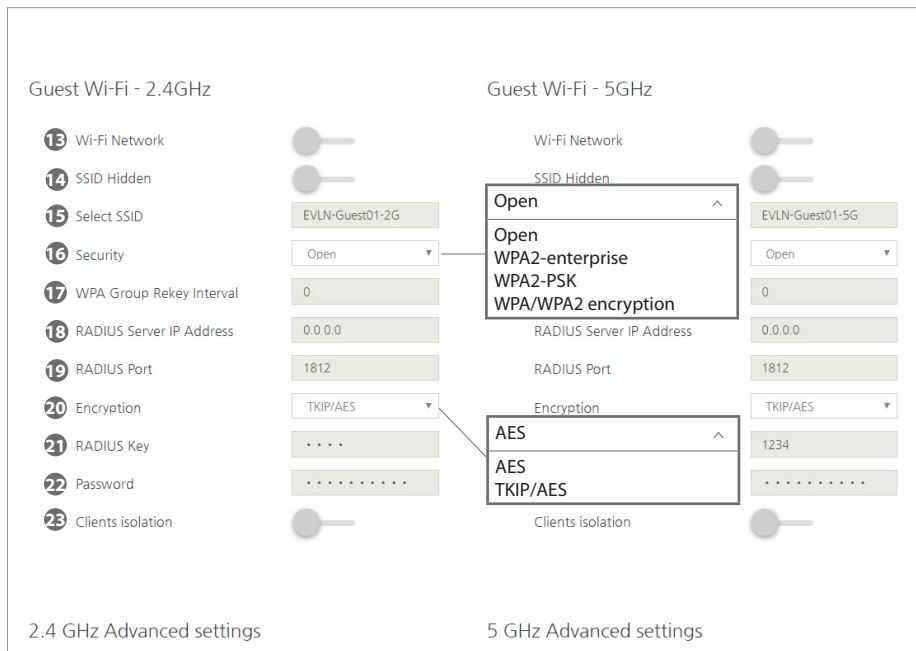
User can configure the password for the selected SSID connection.

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

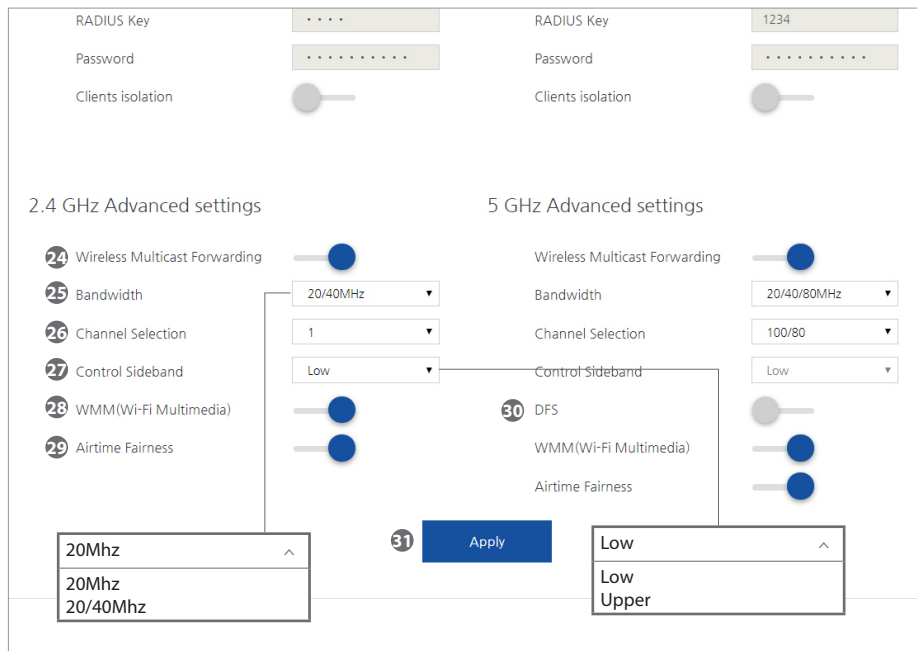
User can configure the password for the selected SSID connection.

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.

The screenshot shows the 'Mesh Setting' page for device AR2146. It features a navigation bar with 'Device Info', 'Network', 'Wireless', 'Access Control', and 'Service'. The 'Mesh' section has two tabs: 'Mesh Setting' (1) and 'Mesh Topology' (2). Under 'Kaon Mesh', there is a 'Friendly Name' field (3) containing 'AR2146', an 'Auto Optimize' toggle (checked), and an 'OBAL' toggle (unchecked). A warning icon states: 'If OBAL List is registered, it is automatically set to Enabled.' Below this are 'Smart Connect' (4) and 'Save' (5) buttons. The 'OBAL Setting' section has a 'MAC Address' field (6) and an 'Apply' button (7). At the bottom, the 'OBAL List' table has columns for 'MAC Address', 'Status', and 'Name'.

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

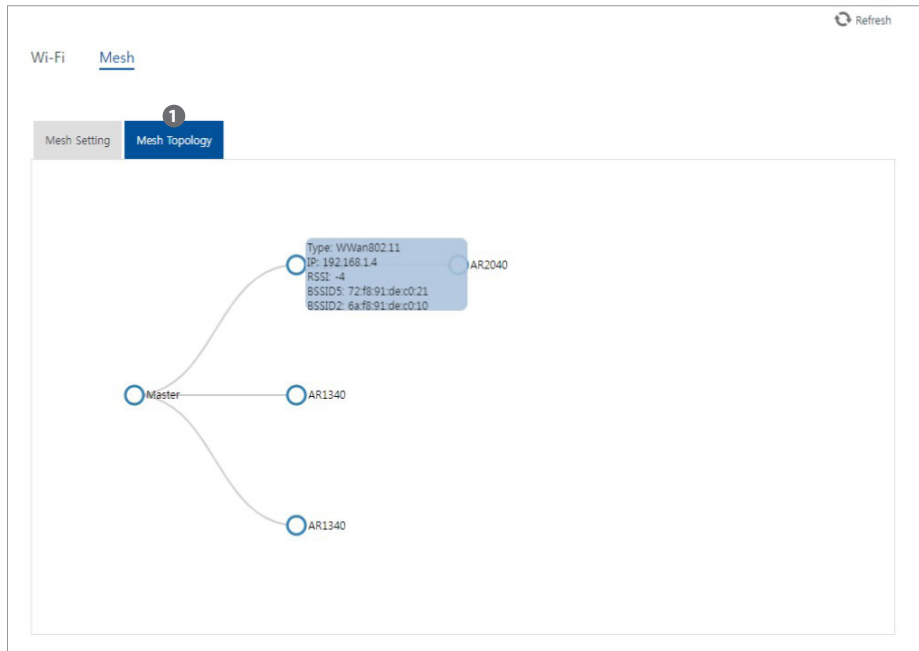
You can save the configuration.

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.

The screenshot shows the 'NAT -- Port Forwarding' configuration page. It includes a breadcrumb trail: Device Info | Network | Wireless | Access Control | Service. Below this, there are tabs for 'NAT', 'Filtering', and 'Parental Control'. Under the 'NAT' tab, there are sub-tabs for 'Port Forwarding', 'Port Triggering', and 'DMZ Host'. The 'Port Forwarding' sub-tab is active. The configuration area is titled 'NAT -- Port Forwarding' and contains the following fields:

- Select a Service (dropdown menu showing 'Select One')
- Custom Service
- Server Type: IPv4 (dropdown menu)
- Server IP Address: 192.168.1.

Below these fields is a table with the following structure:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		
		TCP ▼		

At the bottom of the configuration area is an 'Apply' button. Below the table is a summary table with the following columns: Name, Ext Port, Protocol, Int Port, ServerIP, WAN, and Remove.

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.

NAT -- Port Forwarding

1 Select a Service

2 Custom Service

3 Server Type: IPv4

4 Server IP Address: 192.168.1.

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		
		TCP		

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.

The screenshot displays the 'NAT -- Port Triggering' configuration page. It includes a breadcrumb trail: Device Info | Network | Wireless | Access Control | Service. The 'NAT' tab is active, with sub-tabs for Filtering and Parental Control. Under 'NAT', there are three options: Port Forwarding, Port Triggering (selected), and DMZ Host. The configuration steps are: 1) Use Interface, 2) Select an application, and 3) Custom application. A table for custom applications is shown with columns: Trigger Port Start, Trigger Port End, Trigger Protocol, Open Port Start, Open Port End, and Open Protocol. Two dropdown menus are shown: one for selecting an interface (eth4.1/ether4.1 or PPP0.2/PPP0.2) and another for selecting a pre-defined application (Aim Talk, ashérons-call, Calista IP Phone, Delta Force(Client/Server), icq, Napster, Net2Phone, Rainbow Six/Rogue Spear). An 'Apply' button is at the bottom.

1) Use interface

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

2) Select an application

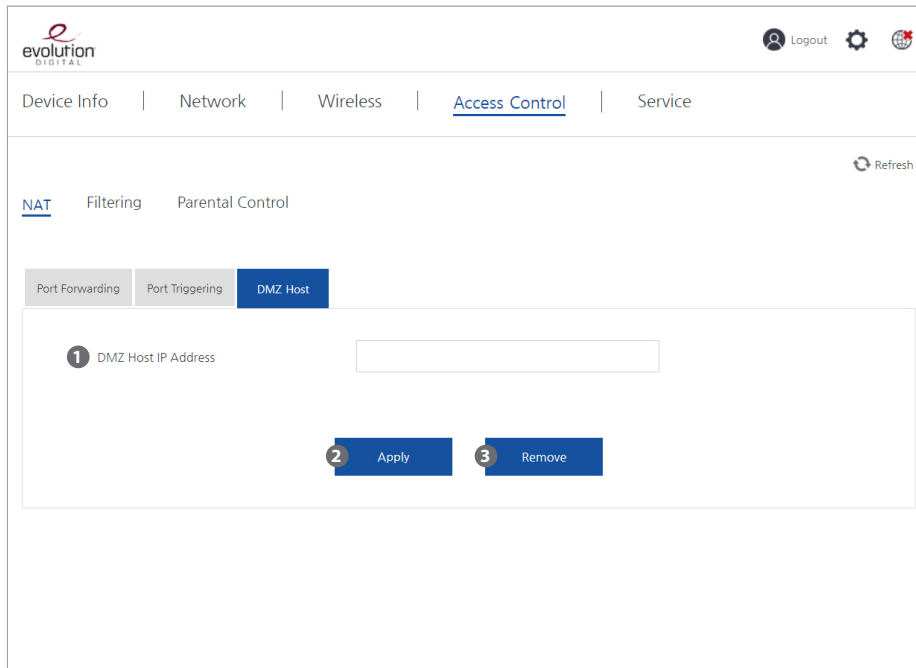
User can select pre-defined application to enable Port Triggering.

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.



The screenshot displays the Evolution Digital web interface. At the top left is the 'evolution DIGITAL' logo. The top right contains a 'Logout' button and two icons (a gear and a globe). Below the logo is a navigation menu with 'Device Info', 'Network', 'Wireless', 'Access Control', and 'Service'. The 'Access Control' menu item is highlighted. Below the navigation menu is a 'Refresh' button. The main content area has three tabs: 'NAT', 'Filtering', and 'Parental Control'. The 'NAT' tab is active. Underneath, there are three sub-tabs: 'Port Forwarding', 'Port Triggering', and 'DMZ Host'. The 'DMZ Host' sub-tab is selected. The main content area contains a form with a label '1 DMZ Host IP Address' and an empty text input field. Below the input field are two buttons: '2 Apply' and '3 Remove'.

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.

The screenshot shows the Evolution Digital web interface. At the top left is the logo "evolution DIGITAL". On the top right, there are icons for "Logout", a gear for settings, and a globe for language. Below the logo is a navigation menu with "Device Info", "Network", "Wireless", "Access Control" (highlighted), and "Service". Under "Access Control", there are sub-menus for "NAT", "Filtering" (highlighted), and "Parental Control". A "Refresh" button is in the top right corner of the main content area. Below the sub-menus, there are three tabs: "IP Outgoing Filtering" (highlighted), "IP Incomming Filtering", and "MAC Filtering". The main content area is titled "Add IP Filter -- Outgoing" and contains the following fields:

- Filter Name:
- IP Version:
- Protocol:
- Source IP address:
- Source Port:
- Destination IP address:
- Destination Port:

Below the fields is a blue "Apply" button. At the bottom, there is a section titled "Outgoing IP Filtering Setup" with a table header:

Filter Name	IP Version	Protocol	SrcIP	SrcPort	DstIP	DstPort	Remove
-------------	------------	----------	-------	---------	-------	---------	--------

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.

The screenshot shows the 'evolution DIGITAL' web interface. The navigation menu includes 'Device Info', 'Network', 'Wireless', 'Access Control', and 'Service'. The 'Access Control' section is active, with sub-tabs for 'NAT', 'Filtering', and 'Parental Control'. The 'Filtering' sub-tab is selected, and the 'IP Outgoing Filtering' sub-tab is active. The main content area is titled 'Add IP Filter -- Outgoing' and contains a numbered list of fields: 1) Filter Name, 2) IP Version, 3) Protocol, 4) Source IP address, 5) Source Port, 6) Destination IP address, and 7) Destination Port. The 'IP Version' dropdown is set to 'IPv6', and the 'Protocol' dropdown is set to 'TCP'. The 'Source Port' and 'Destination Port' fields have example text: 'Ex) 10000 or 1000:11000'. An 'Apply' button is located below the form. At the bottom, there is a table titled 'Outgoing IP Filtering Setup' with columns: Filter Name, IP Version, Protocol, SrcIP, SrcPort, DstIP, DstPort, and Remove. Two callout boxes on the right show the dropdown options: the first for 'IP Version' lists 'IPv4' and 'IPv6'; the second for 'Protocol' lists 'TCP', 'UDP', 'TCP/UDP', and 'ICMP'.

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 Incoming 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.

The screenshot shows the Evolution Digital web interface for configuring IP Incoming Filtering. The page is titled "Add IP Filter -- Incoming" and includes a numbered list of fields to be filled:

- 1) Filter Name
- 2) IP Version
- 3) Protocol
- 4) Source IP address
- 5) Source Port
- 6) Destination IP address
- 7) Destination Port

The "IP Version" dropdown is set to "IPv4". The "Protocol" dropdown is set to "TCP". The "Source Port" and "Destination Port" fields have example text: "Ex) 10000 or 1000:11000". An "Apply" button is located below the form.

Two callout boxes highlight the dropdown menus:

- The "IP Version" dropdown shows options: IPv4, IPv4, IPv6.
- The "Protocol" dropdown shows options: TCP, TCP, UDP, TCP/UDP, ICMP.

At the bottom, there is an "Incoming IP Filtering Setup" table with columns: Filter Name, IP Version, Protocol, SrcIP, SrcPort, DstIP, DstPort, and Remove.

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.

The screenshot shows the Evolution Digital web interface for MAC filtering. At the top left is the 'evolution DIGITAL' logo. The top right contains 'Logout', a settings gear, and a globe icon. A navigation bar includes 'Device Info', 'Network', 'Wireless', 'Access Control' (highlighted), and 'Service'. Below this, there are tabs for 'NAT', 'Filtering' (selected), and 'Parental Control', with a 'Refresh' button on the right. Under 'Filtering', there are sub-tabs for 'IP Outgoing Filtering', 'IP Incoming Filtering', and 'MAC Filtering' (selected). The main content area is titled 'Add MAC Filter' and features a 'MAC Address' label, a text input field with the example 'Ex) XX:XX:XX:XX:XX:XX', and a blue 'Apply' button. At the bottom, a table header shows 'MAC Address' and 'Remove' columns.

10.3. Parental Control

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

The screenshot shows the 'Parental Control' settings page in the Evolution Digital web interface. The page is titled 'Access Time Restriction' and contains several input fields and checkboxes. The fields are numbered 1 through 6: 1) Name, 2) LAN Device MAC Address, 3) Days of the week (with checkboxes for All day, Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday), 4) Start Blocking Time (hh:mm), 5) Stop Blocking Time (hh:mm), and 6) Apply button. Below the form is a table with columns: Name, MAC, Rule Status, Start, Stop, Edit, and Remove.

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.

The screenshot shows the 'Service' menu in the Evolution Digital web interface. The 'Dynamic DNS' sub-menu is active. The page contains the following elements:

- Navigation:** Device Info | Network | Wireless | Access Control | Service
- Sub-menu:** Dynamic DNS | DLNA | NAS
- Refresh:** Refresh button
- Add Dynamic DNS:**
 - 1) D-DNS provider: Dropdown menu with 'DynDNS.org' selected.
 - 2) Hostname: Text input field.
 - Interface: Dropdown menu.
- DynDNS Settings:**
 - 3) Username: Text input field.
 - Password: Text input field.
- Apply:** Blue button with 'Apply' text.
- Table:** A table with columns: Hostname, Username, Service, Interface, Remove.

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.

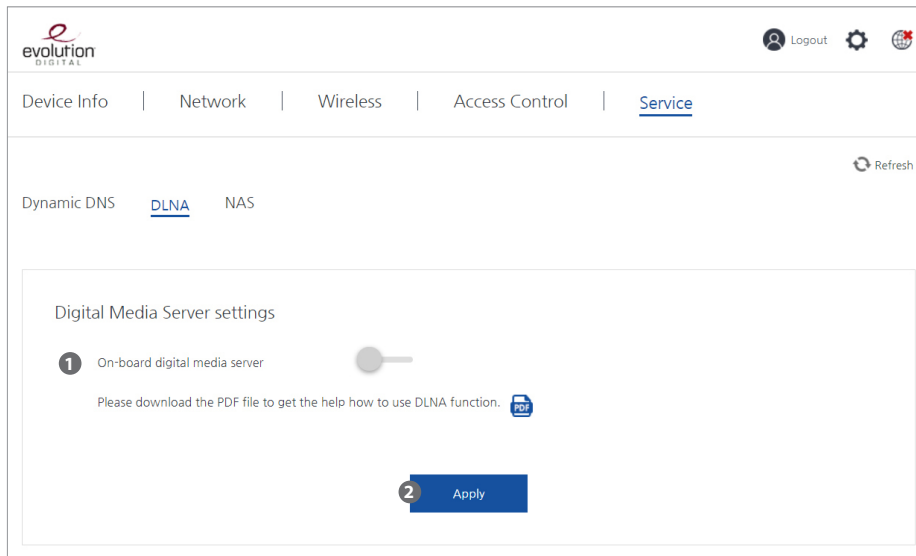
4) Apply

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

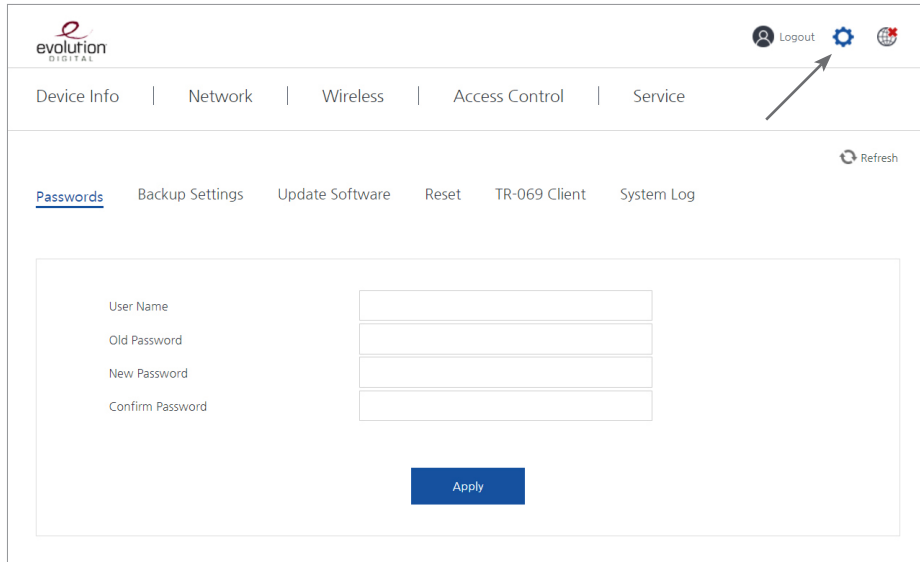
You can enable or disable the digital media server function.

2) Apply

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

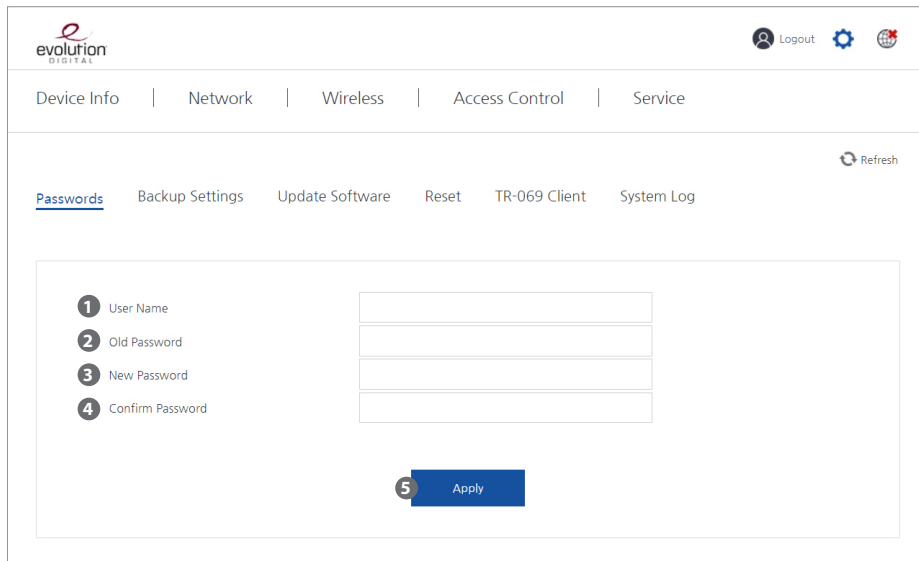
12. Management Setting Menu

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.



The screenshot shows the Evolution Digital web interface. At the top left is the logo "evolution DIGITAL". At the top right are icons for "Logout", a gear, and a globe. Below the logo is a navigation menu with "Device Info", "Network", "Wireless", "Access Control", and "Service". Below the navigation menu is a "Refresh" button. The main content area has a "Passwords" tab selected, with other tabs: "Backup Settings", "Update Software", "Reset", "TR-069 Client", and "System Log". The "Passwords" form contains four input fields: "1) User Name", "2) Old Password", "3) New Password", and "4) Confirm Password". Below the fields is a blue "5) Apply" button.

1) Username

Enter the username.

2) Old Password

Enter the current password.

3) New Password

Enter the new password.

4) Confirm Password

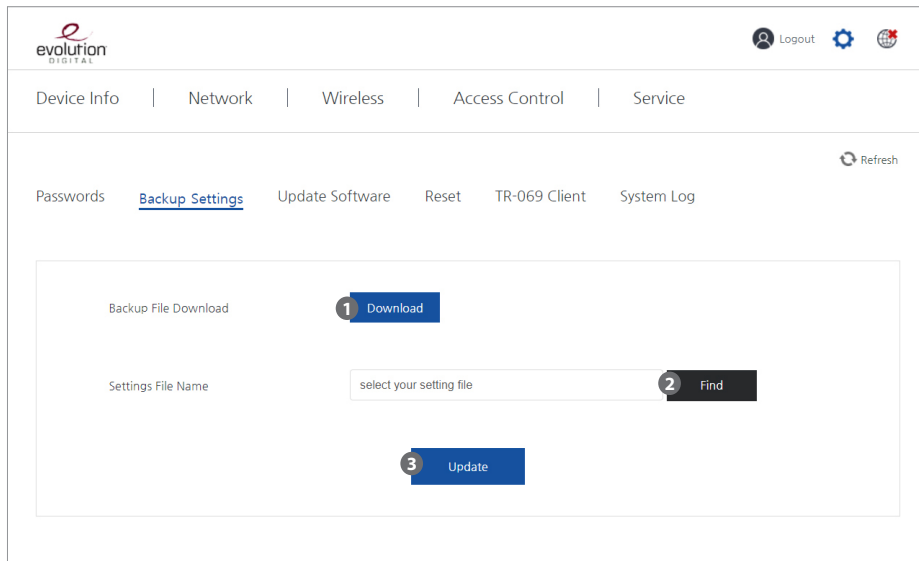
Re-enter the new password.

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.



The screenshot shows the Evolution Digital web interface. At the top left is the 'evolution DIGITAL' logo. On the top right are 'Logout', a gear icon, and a globe icon. Below the logo is a navigation bar with 'Device Info', 'Network', 'Wireless', 'Access Control', and 'Service'. Underneath is another navigation bar with 'Passwords', 'Backup Settings' (highlighted), 'Update Software', 'Reset', 'TR-069 Client', and 'System Log'. A 'Refresh' icon is on the far right. The main content area contains a 'Backup File Download' section with a '1 Download' button. Below it is a 'Settings File Name' section with a text input field containing 'select your setting file' and a '2 Find' button. At the bottom of this section is a '3 Update' button.

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.

The screenshot shows the Evolution Digital web interface. At the top left is the logo 'evolution DIGITAL'. At the top right are icons for 'Logout', a gear, and a globe. Below the logo is a navigation menu with 'Device Info', 'Network', 'Wireless', 'Access Control', and 'Service'. Below the menu is a secondary navigation bar with 'Passwords', 'Backup Settings', 'Update Software', 'Reset', 'TR-069 Client', and 'System Log'. A 'Refresh' button is located to the right of this bar. The main content area contains a form with a text input field labeled 'select your setting file' and a 'Find' button. Below the input field is an 'Update' button. The form is annotated with numbered steps: '1 Settings File Name' pointing to the input field and '2 Update' pointing to the 'Update' button.

1) Find a New Firmware

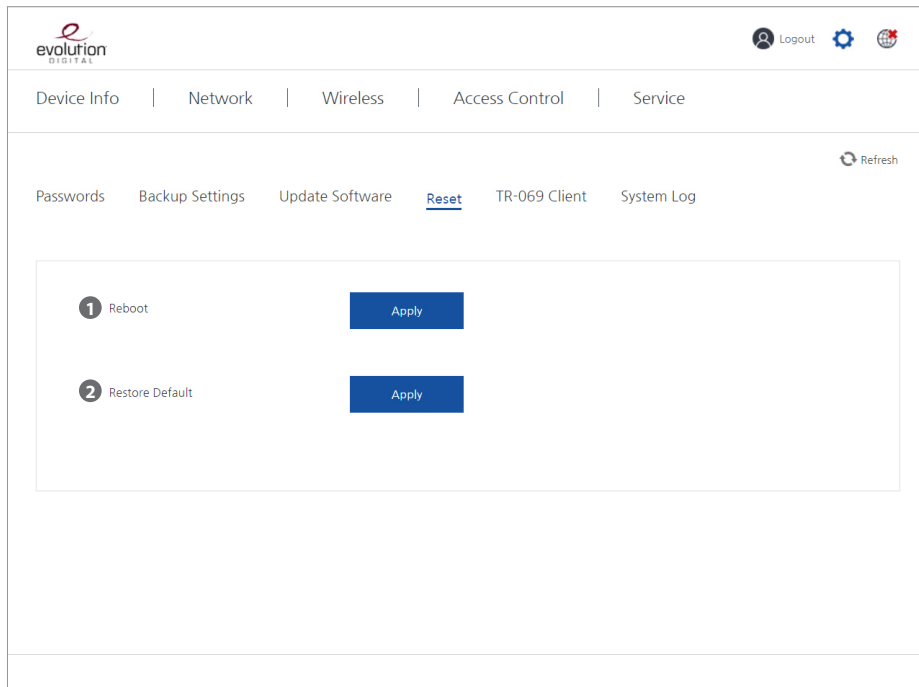
User can find a firmware file for the update.

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).

The screenshot shows the 'TR-069 Client Configuration' page in a web browser. The page has a navigation bar with 'Device Info', 'Network', 'Wireless', 'Access Control', and 'Service'. Below the navigation bar, there are links for 'Passwords', 'Backup Settings', 'Update Software', 'Reset', 'TR-069 Client' (which is highlighted), and 'System Log'. A 'Refresh' button is also present. The main configuration area is titled 'TR-069 Client Configuration' and contains the following settings:

- 1 Inform: A toggle switch that is currently turned on (blue).
- 2 Inform Interval: A text input field containing '300'.
- 3 ACS URL: A text input field containing 'http://krms-demo.kaonmedia.com:6547/'.
- 4 ACS User Name: A text input field containing 'krmsagent'.
- 5 ACS Password: A password input field with masked characters.
- 6 WAN Interface used by TR-069 client: A dropdown menu.
- 7 Display SOAP messages on serial console: A toggle switch that is currently turned off (grey).
- 8 Connection Request Authentication: A toggle switch that is currently turned on (blue).
- 9 Connection Request User Name: A text input field.
- 10 Connection Request Password: A password input field with masked characters.
- 11 Connection Request URL: A text input field.

An 'Apply' button is located at the bottom of the configuration area.

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 password, 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

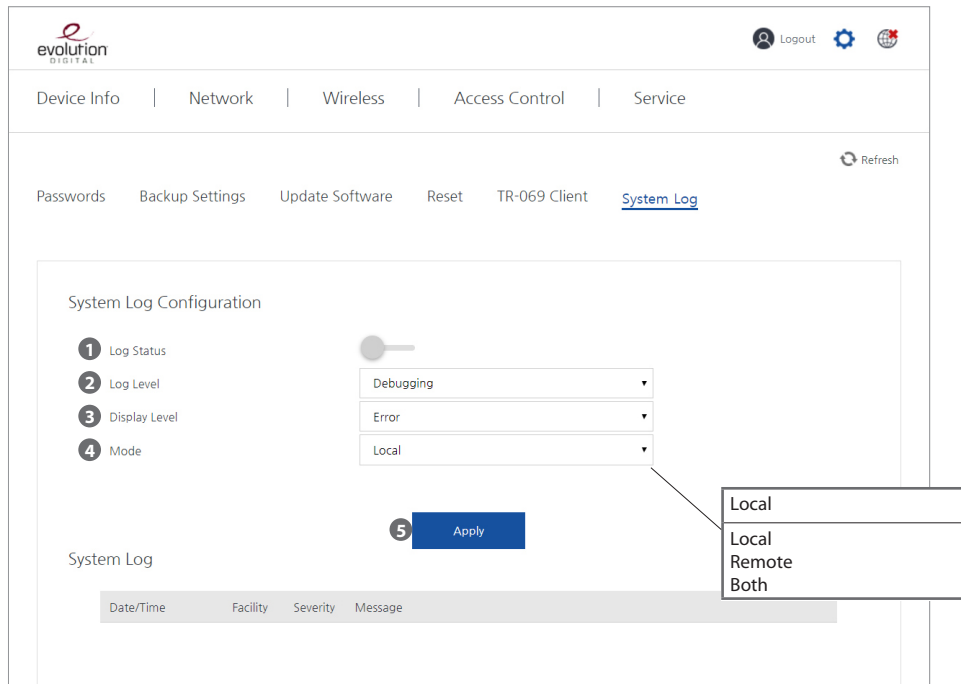
It is usually established automatically. However, the port should be configured in some cases.

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