Technical Guide

Authentication Flow on Controller

Released: 2018-05-03
Doc Rev. No: R1

Table of Contents

1 Introduction

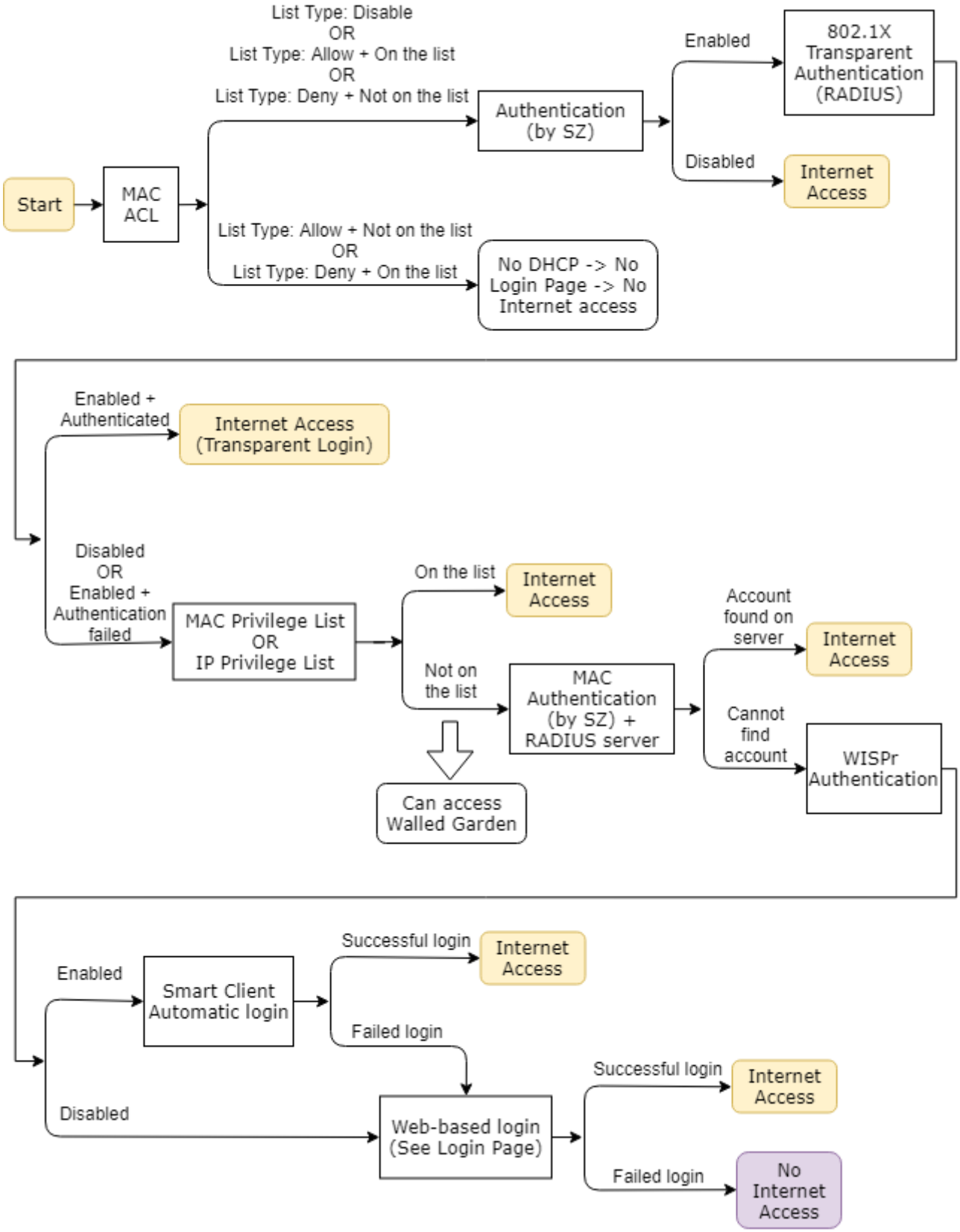
With support for authentication, authorization, and accounting (AAA), the controller allows network administrators to effectively manage network access, control network usage and monitor user activities.

In this technical guide, the authentication flow on the controller is illustrated using a flowchart. With this flowchart, readers would be able to understand the order in which authentication methods are presented on the controller, so they could better plan the authentication methods they'd like to leverage as well as better understand how they could troubleshoot if necessary.

Furthermore, as will be seen from the flowchart, a variety of authentication methods are available on the controller for network access control, including web-based, 802.1X, WISPr and MAC authentication. How each authentication method works and where to configure its settings are also explained.

2 Authentication Flow on Controller

Flowchart below illustrates the authentication flow on the controller.



As can be seen from the flowchart, the authentication flow on the controller goes in the general order of **MAC Access Control List > Privilege List > Walled Garden > Non-web Authentication > Web-based Authentication**.

For all clients, MAC Access Control List (ACL) is the first "gate". When MAC ACL is enabled, if a client device is not on the Allow List or if it is on the Deny List, it would not be able to obtain a DHCP IP address, and thus would not see the Login Page and be denied network access through the controller.

Clients can be granted network access directly based on their MAC address and/or IP address through the MAC/IP Privilege List. Note that clients authenticated through this method would not appear in "Online Users" but in "Non-Login Devices".

3 Authentication Methods

3.1 MAC Access Control List (ACL)

MAC Access Control is used to grant or deny permission to access the User Login Page. As mentioned earlier, if a client device is denied access to the network based on this list, it would not even obtain a DHCP IP address and thus would not be able to access the Login Page.

When the List Type is "Allow", the list can be considered as a whitelist because only the MAC addresses on this list can access network. When the list type is "Deny", the list can be considered as a blacklist.

"Allow" type is usually used for closed systems.

3.2 IP Privilege List

IPv4 addresses of client devices can be added to the IP Privilege List so that these devices can be granted network access without login. Each device/IP address can be assigned to a Group so that Group Policy can be enforced on the device. For each entry on the list, the client device's MAC address can be optionally added to bind to its IPv4 address.

IP Privilege List can be used with client devices having static IP addresses. Alternatively, it can be used with a DHCP server for assigning DHCP IP addresses to client devices.

3.3 MAC Privilege List

MAC addresses of devices can be added to the MAC Privilege List so that these devices can be granted

network access without login. Note that Default Policy (excluding QoS) of the particular Service Zone will be enforced on clients authenticated this way. To configure Default Policy, go to *System > Service Zone > Service Zone Configuration*, and disable Authentication under Authentication Settings to reveal Default Policy. Note that this Default Policy still applies even when Authentication is set to "Enable".

With IP Privilege List, IP address based Group Policy enforcement can be achieved. However, with MAC Privilege List, QoS in Group Policy cannot be applied. Thus, to achieve MAC address based Group Policy enforcement with QoS, one can combine the use of IP Privilege List with DHCP Reserved IP List. An example of this will be provided later in Section 4.3.1.

3.4 Walled Garden List

Client devices can access destinations on the Walled Garden List without login, where the destinations are defined by their domain name, IP address or subnet.

Traffic to Walled Garden List can be blocked by User Firewall Rules under Policy.

3.5 802.1X Authentication

802.1X authentication is to be used in conjunction with back-end authentication server configured on the controller. When enabled, if the connected device has its credentials stored on the back-end server, the controller will automatically authenticate and grant network access to provide transparent login.

For 802.1X authentication, the controller must be the RADIUS server configured on the AP (or switch).

3.6 MAC Authentication

MAC Authentication is to be used in conjunction with a RADIUS server configured on the controller. When enabled, if the connected device has its MAC address stored on the RADIUS Server, the controller will automatically authenticate and grant network access to provide transparent login.

3.7 WISPr Authentication

Similar to WebSheet (Captive Network Assistant) on iOS devices, some devices have built-in Smart Client. The Smart Client will detect if the WLAN is a Captive Network by sending requests to a URL as defined by the manufacturer. When WISPr authentication is configured and the Smart Client on a client device is connected to the WLAN, the controller will automatically authenticate and grant network access to provide transparent login for the device.

Some Android devices do not have built-in Smart Client. For Windows systems, built-in Network

Connectivity Status Indicator (msftncsi) is available for Windows 7 and above.

3.8 Web-based Authentication

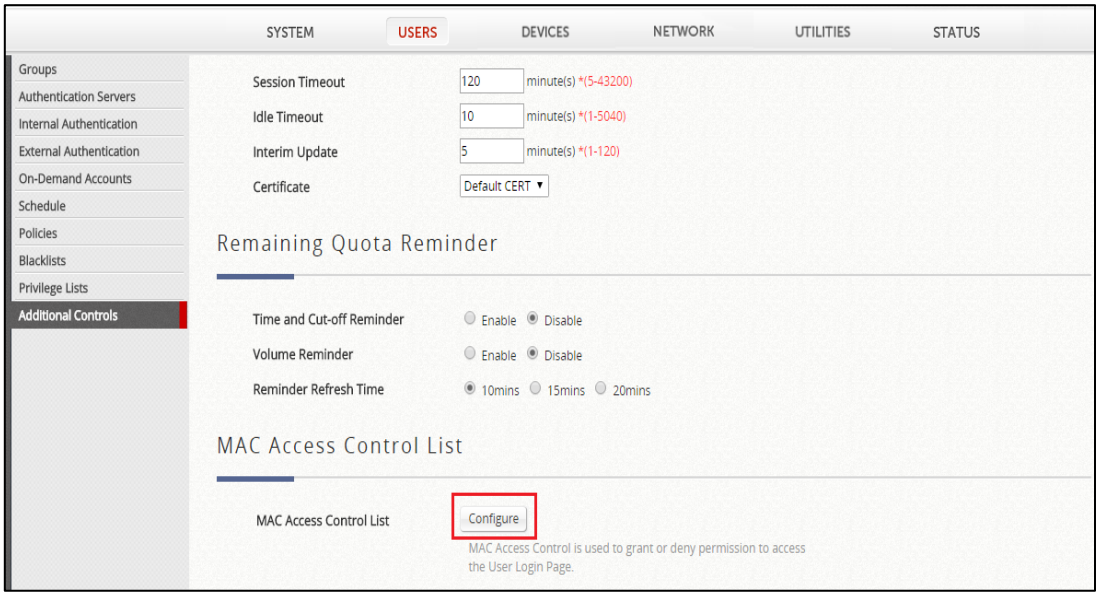
If client devices cannot be granted network access by all of above methods, a browser or browser-like may pop up, or the user has to open browser to visit a web site then redirect to login page (Captive Portal).

Web-based authentication also called Universal Access Method (UAM).

4 Configurations

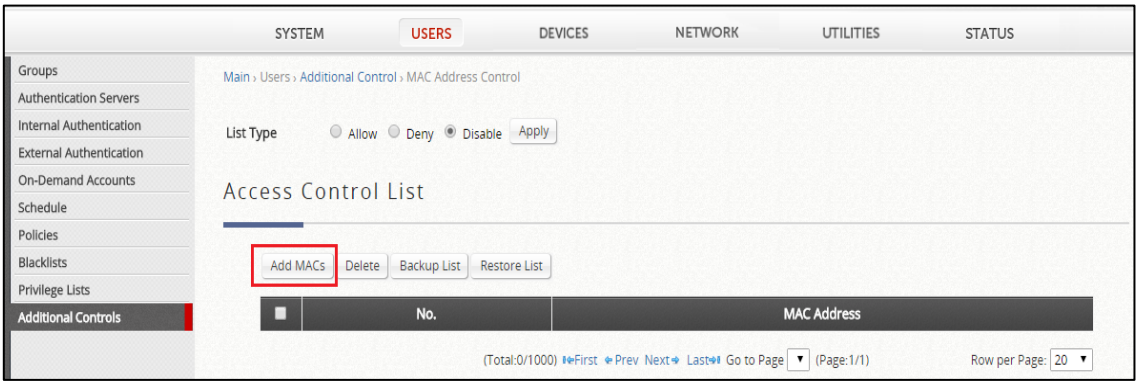
4.1 MAC Access Control List

a. Go to *User > Additional Controls*, scroll down to "MAC Access Control List" and click "Configure" to enter the configuration page.



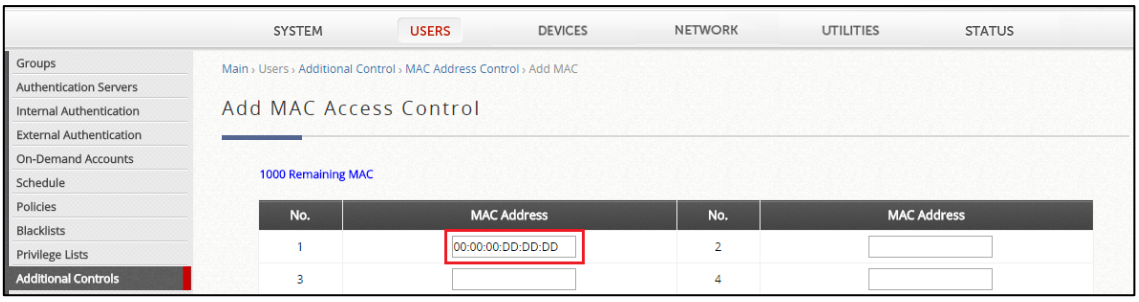
Configure the MAC Access Control List

a. Click "Add MACs" to start adding entries to the list.



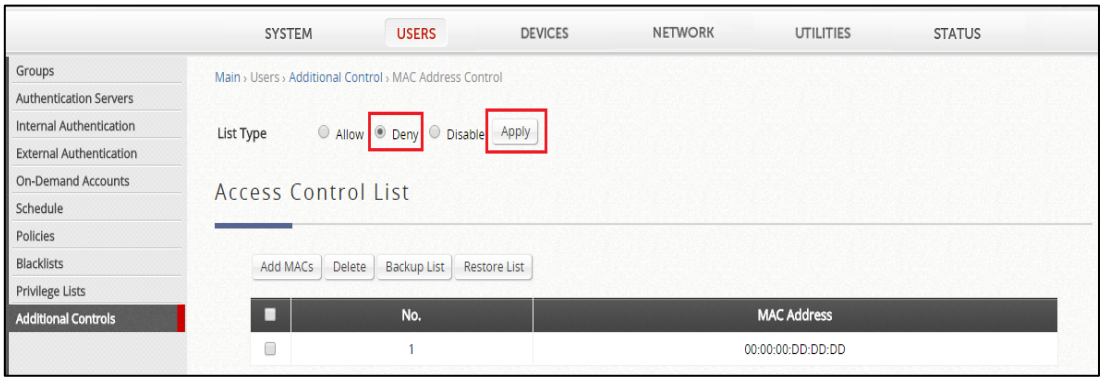
Click “Add MACs” button

c. Enter the MAC address(es) of the client device(s) and click “Apply”.



Enter the client device’s MAC address

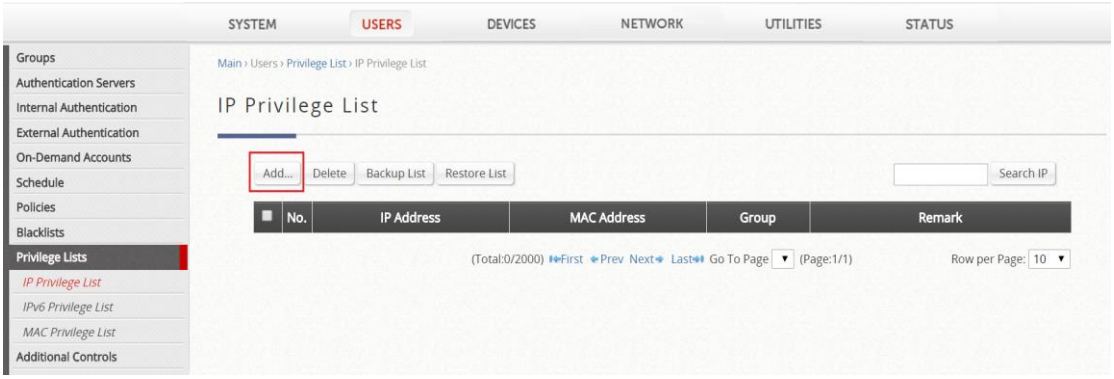
d. Select List Type “Deny” and click Apply. As mentioned earlier, client devices with their MAC addresses on the Deny List would not be able to 1) get a DHCP IP address from the controller, 2) access the Login Page; and 3) have network access through the controller.



Configure List Type to “Deny”

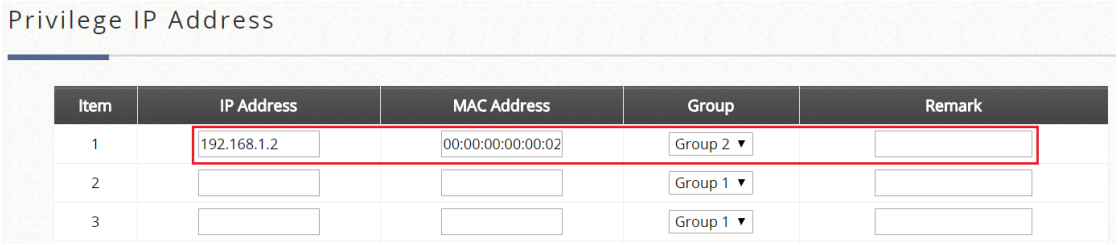
4.2 IP Privilege List

a. Go to *Users > Privilege Lists > IP Privilege Lists*, click “Add”.



Click Add button

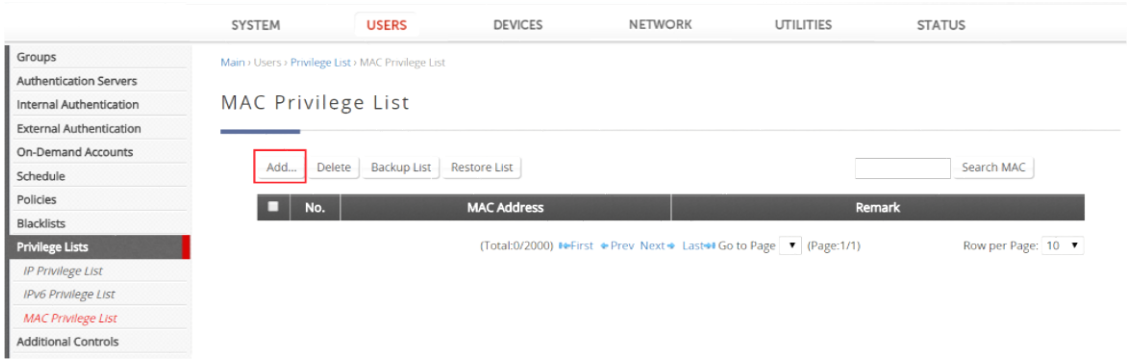
b. Enter the client device's IP address and click "Apply". The device can access the network without redirection to login page, and be authorized based on its Group Policy. However, only Firewall, Session Limit, QoS and Specific Routes will apply.



Enter address to IP Privilege List

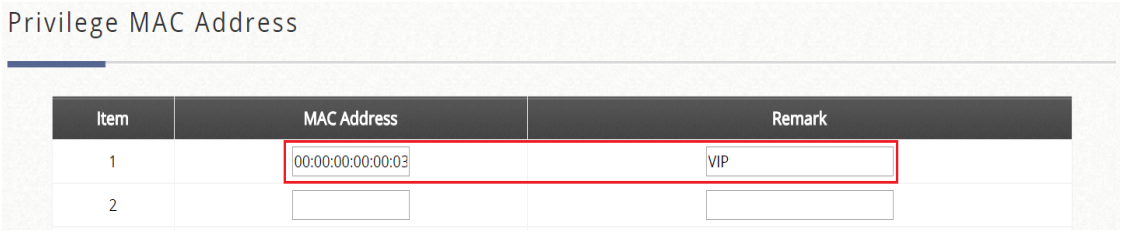
4.3 MAC Privilege List

a. Go to *Users > Privilege Lists > MAC Privilege Lists*, click "Add".



Click "Add" button from MAC Privilege List

b. Add the client device's MAC address to the list and click "Apply". The device with this MAC address can access network without redirect to login page.



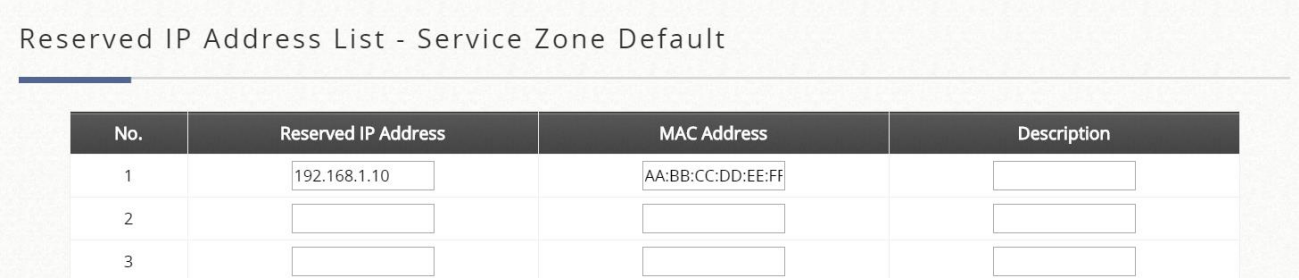
Enter address to MAC Privilege List

4.3.1 Example: MAC Address Based Full Group Policy Enforcement (with QoS)

A client device will be given MAC address based privileged network access in multiple Service Zones with full Group Policy enforcement (with QoS). The client device will have Privilege IP Addresses of

192.168.1.10 in the Default Service Zone, 172.21.0.10 in SZ1 and 172.22.0.10 in SZ2, respectively.

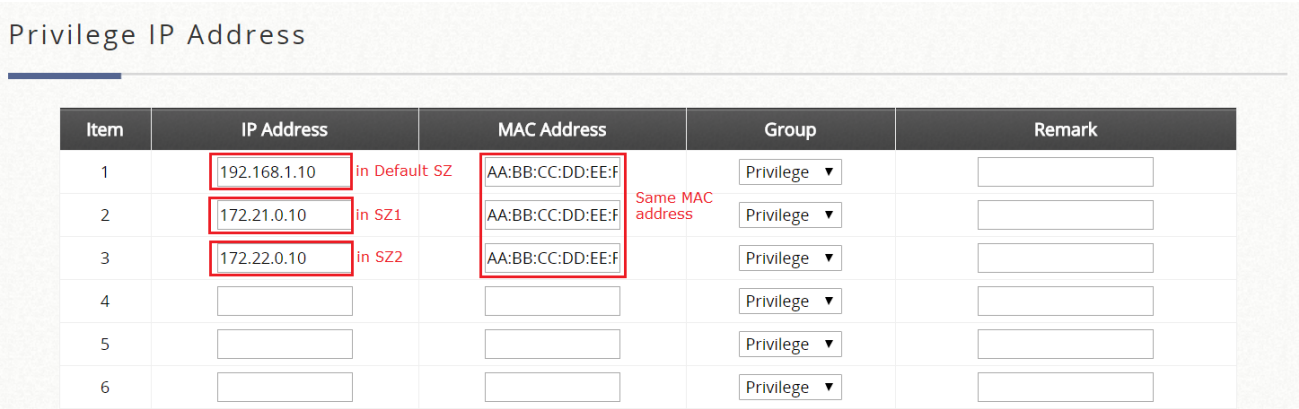
a. Go to *System > Service Zone > Service Zone Configuration > DHCP Configuration > Reserved IP Address List* in the Default Service Zone, add an entry with a Reserved IP Address of 192.168.1.10 with a MAC Address of AA:BB:CC:DD:EE:FF.



b. Go to the Reserved IP Address List in SZ1, add an entry with a Reserved IP Address of 172.21.0.10 with the same MAC Address.

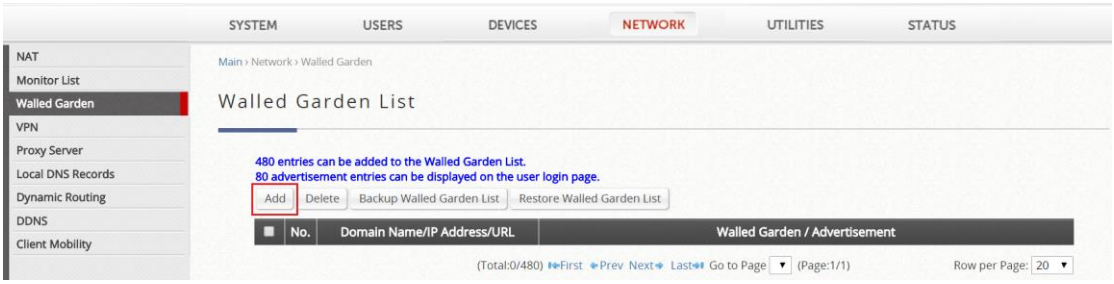
c. Go to the Reserved IP Address List in SZ2, add an entry with a Reserved IP Address of 172.22.0.10 with the same MAC Address.

d. Go to *Users > Privilege List > IP Privilege List*, add multiple entries with the same client device's MAC address binding to different Privilege IP Addresses for different Service Zones.



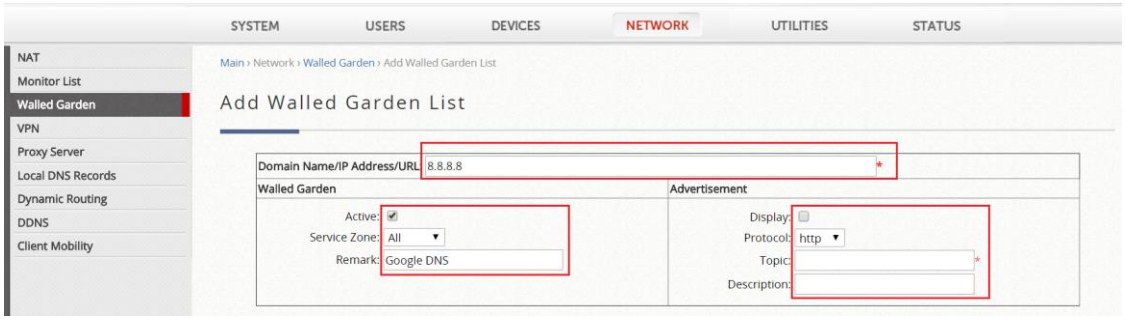
4.4 Walled Garden List

a. Go to *Network > Walled Garden*, click "Add".



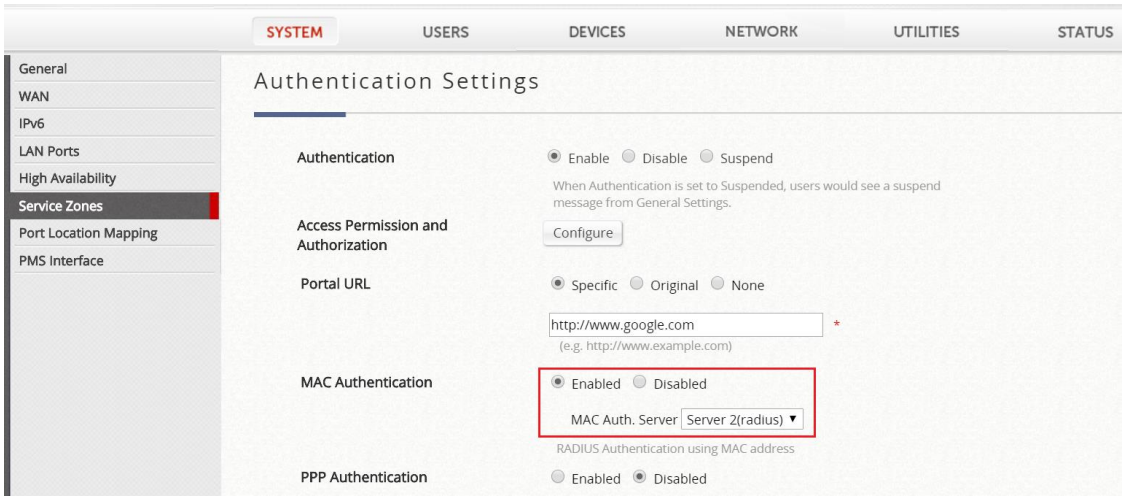
Click “Add” button from Walled Garden List

b. Add the domain name, IP address or subnet of the desired destination to the list and click “Apply”. Client devices can go to these destinations without redirection to the Login Page.



Add destinations to Walled Garden List

c. Go to *System > Service Zone > Service Zone Configuration*, scroll down to “MAC Authentication” of Service Zone and Enable this option. By default, the back-end RADIUS server is “Server 2” (Configured in the Auth. Option for RADIUS).



MAC Authentication

4.5 802.1X Authentication

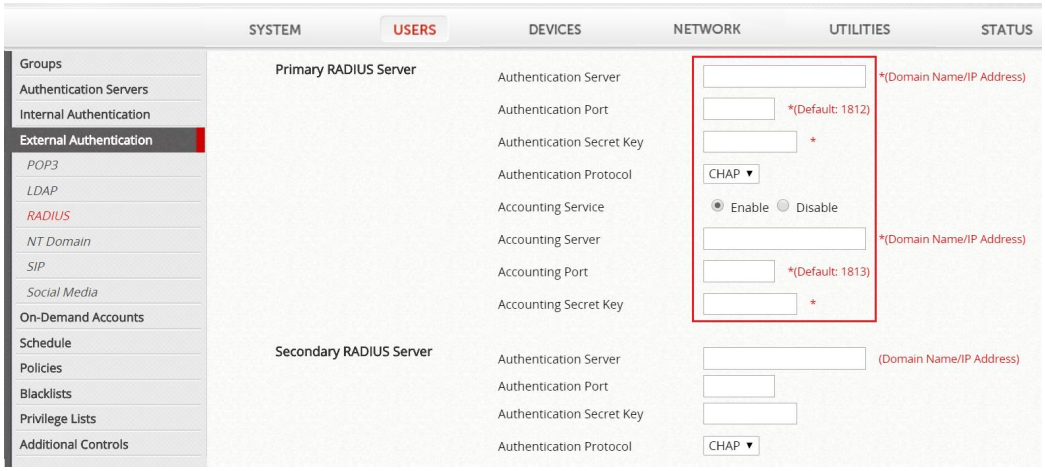
a. Go to *Users > Authentication Servers*, click Server Name “Server 2” in this case.

Authentication Servers

b. Configure Authentication Option. The postfix is “example.com” in this case.

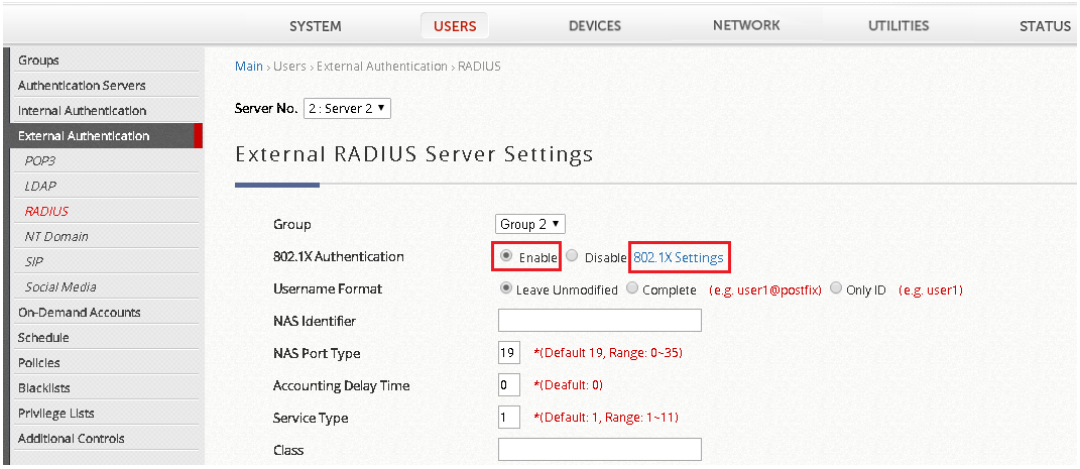
Configure Authentication Option

c. Go to *Users > Internal Authentication > RADIUS*, configure RADIUS Server settings.



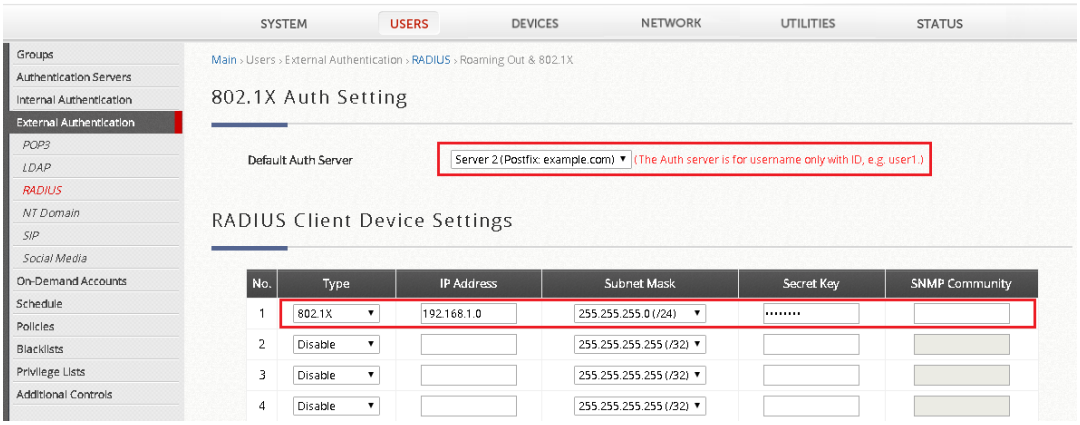
Configure RADIUS Server settings

d. Enable “802.1X Authentication” and click “Apply”. Then, go to “802.1X Settings”.



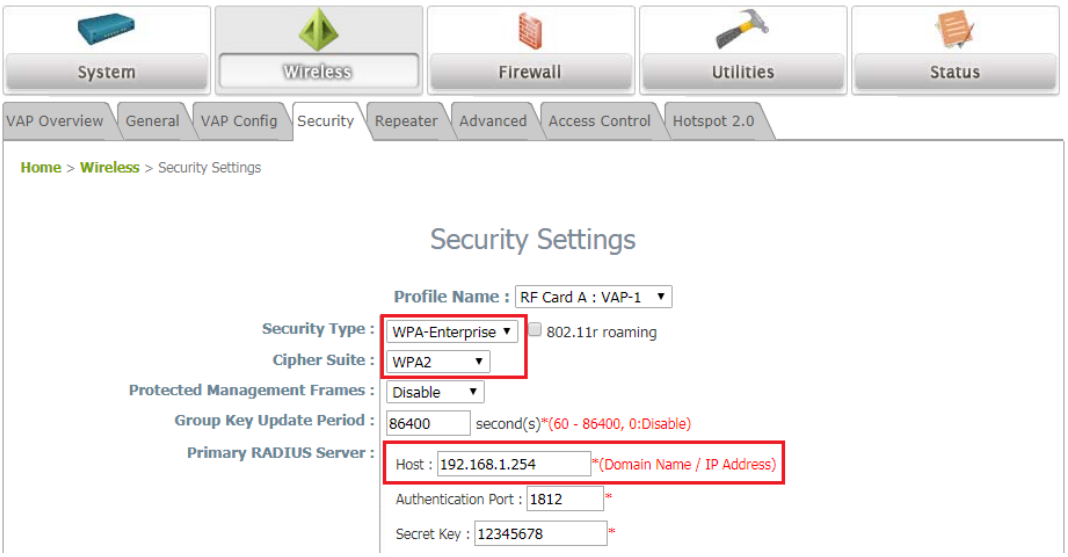
Enable 802.1X Authentication

e. Add the subnet or IP address of the 802.1X authenticator (AP or switch) to the RADIUS Client Device List, and select default RADIUS server for the client credential only with ID (without the email-like postfix “@example.com”).



Configure RADIUS client device list

f. Configure control as RADIUS server in AP, and security should be WPA2-Enterprise.



Configure RADIUS server in AP

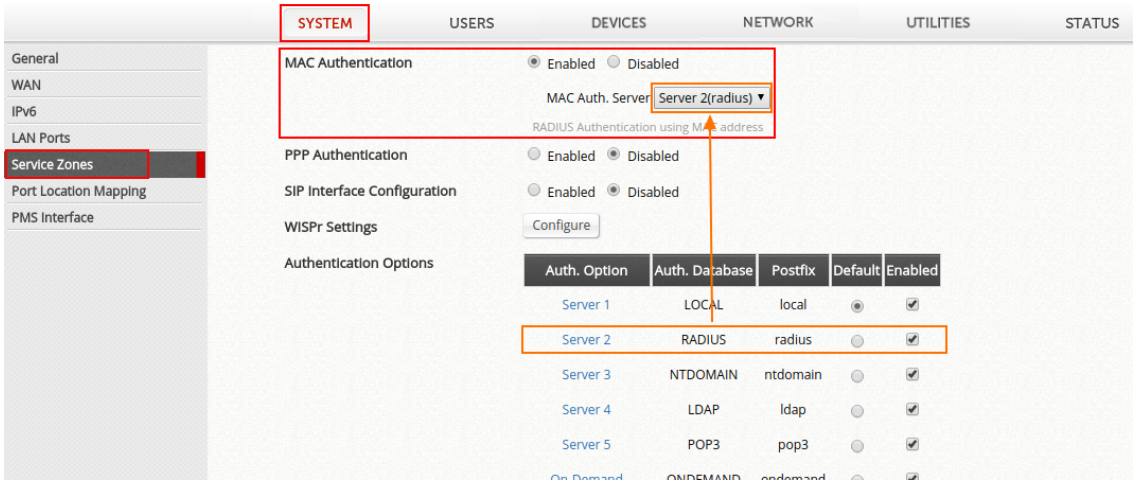
g. When client device connected to the WLAN, the controller will automatically authenticate and grant network access to provide transparent login.

4.6 MAC Authentication

a. Go to *System > Service Zones*. In this example, "Default" Service Zone is selected.

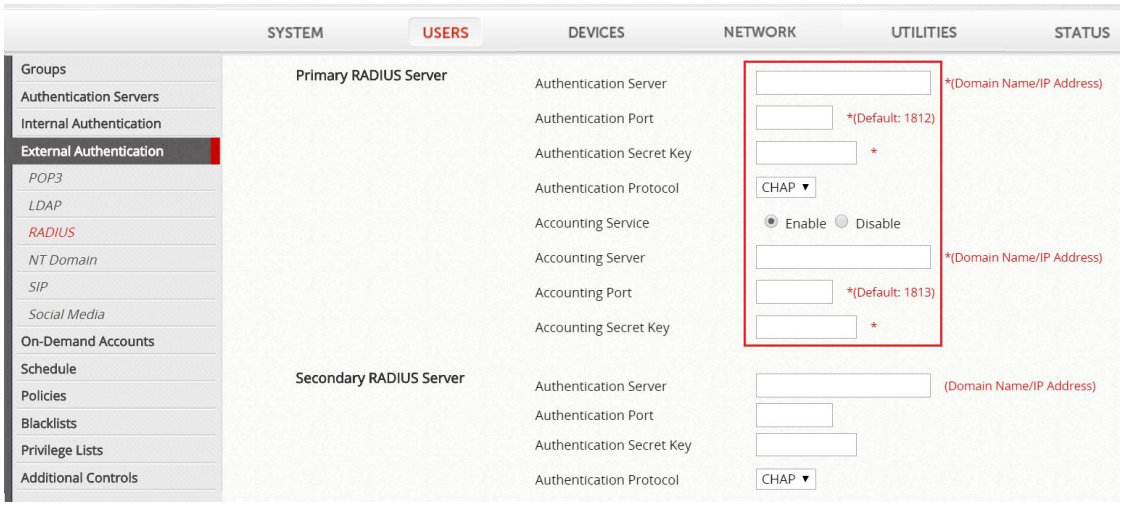
To configure Default Service Zone

b. Scroll down to "MAC Authentication" of Service Zone and Enable this this option. By default, the back-end RADIUS server is "Server 2" (Configured in the Auth. Option for RADIUS).



MAC Authentication

c. Go to *Users > External Authentication > RADIUS*, enter settings of RADIUS server.

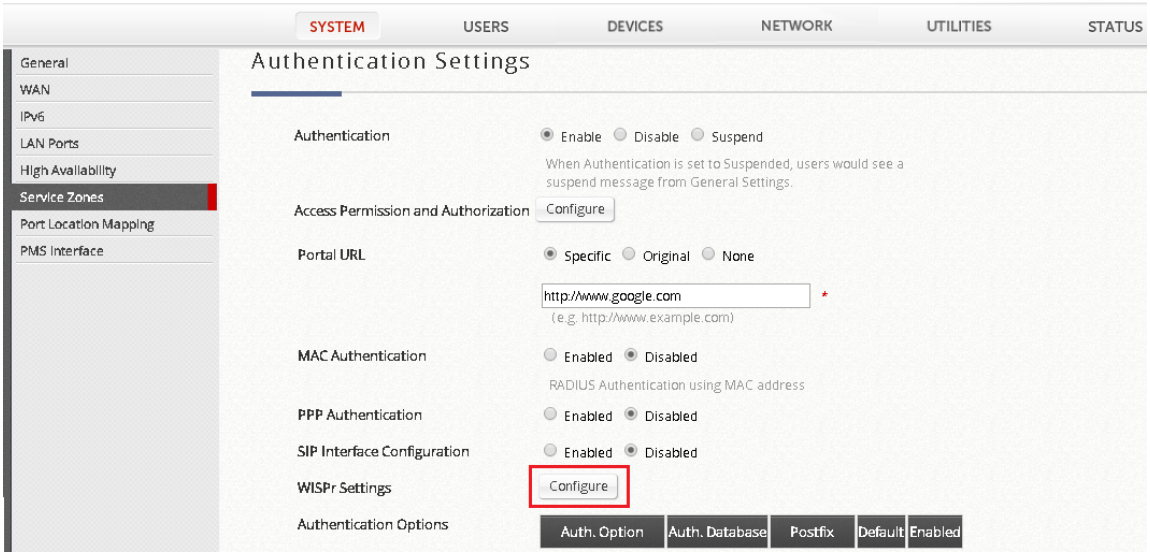


Configure RADIUS server

d. When the connected device has its MAC address stored on the RADIUS Server, the controller will automatically authenticate and grant network access to provide transparent login.

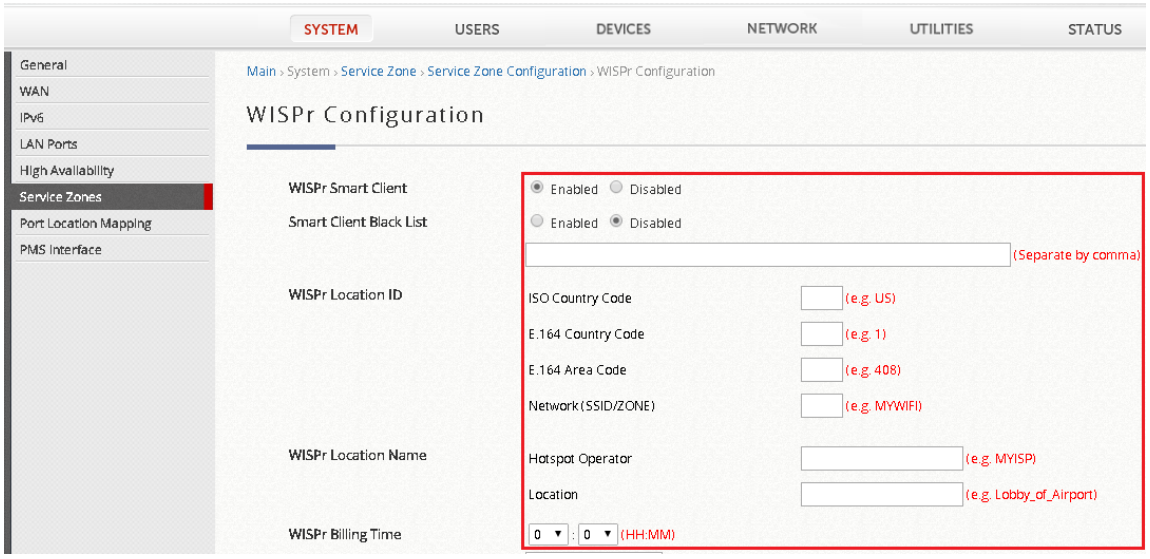
4.7 WISPr Authentication

a. Go to *System > Service Zones > Service Zone Configuration*, configure WISPr Settings.



Configure "WISPr Settings"

b. Enable WISPr Smart Client and enter related parameters.



Enter WISPr Parameters

c. When Smart Client on a client device is connected to the WLAN, the controller will automatically authenticate the device and grant network access to provide transparent login.

5 Remarks

Please contact Technical Support Team for additional inquiries.