Technical Guide

MAC Address Based Access Control

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

Table of Contents

1 Introduction

MAC address-based access control grants or denies users' access to the network based on the MAC addresses of users' devices. On the controller, there are three types of MAC address-based access control available – MAC Authentication (by Service Zone), MAC Privilege List, and MAC Access Control List. In this guide, mechanisms of these different MAC address-based access control options are explained and a comparison between them is given. Possible scenarios for these MAC address-based access control options are also illustrated. Moreover, step-by-step configuration guides are provided to facilitate the configuration process.

1.1 Access Control Mechanisms

Access Control Type	Mechanism
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.
MAC Privilege List	MAC Privilege List is one of the three types of Privilege List supported by the controller, where the other two are IP Privilege List (based on IPv4 address) and IPv6 Privilege List (based on IPv6 address). Devices added to the MAC Privilege List are readily granted network access and require NO authentication. Note that devices on the IP Privilege List can be assigned to a Group, but devices on the MAC Privilege List can NOT be assigned to a Group.
MAC Access Control List	When enabled, MAC Access Control List (or ACL) either allows or denies access to the Login Page based on List Type – Allow, Deny or Disable. When the List Type is "Allow", the list can be considered as a whitelist because only the MAC addresses on this list can access the Login Page. When the List Type is "Deny", the list can be considered as a blacklist. Note that devices on the MAC Access Control List when the List Type is "Allow" or "Disable" also can be assigned to a Group.

1.2 Comparison

Access Control Type	Login Page Display	Authentication	Group Assignment and Policy Enforcement	User Monitoring*
MAC Authentication	No	Yes	Yes	Monitor Users > Online Users
MAC Privilege List	No	No	No	Monitor Users > Non-Login Devices
MAC Access Control List	Yes if List Type is "Disable" or "Allow"; No if List Type is "Deny"	Yes if List Type is "Disable" or "Allow"; No if List Type is "Deny"	Yes if List Type is "Disable" or "Allow"; No if List Type is "Deny"	If List Type is "Disable" or "Allow": Monitor Users > Online Users

* After the user has been granted network access

1.3 Use Case Scenarios

Access Control Type	Scenarios
MAC Authentication	1. Can be used to provide transparent login as an alternative to 802.1X authentication. 2. Can be used as an alternative to web-based authentication for devices that do not support browsers (e.g. IP cameras, printers etc.) 3. Can be used to grant network access for a specific group of devices (e.g. administrative PCs) for convenience.
MAC Privilege List	1. Can be used as an alternative to web-based authentication for devices that do not support browsers (e.g. IP cameras, printers etc.)

MAC Access Control List	1. Can be used to prevent unwanted access to the Login Page to provide better security and higher system performance.

2 Configurations

2.1 MAC Authentication

a. Go to *Main Menu > SYSTEM > Service Zones*; in this sample case, "Default" Service Zone is selected.

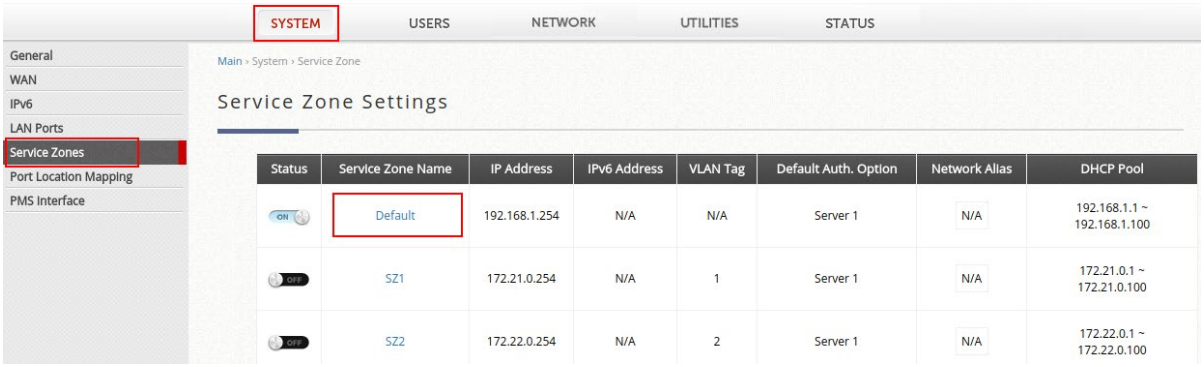

Figure 2.1a – To Configure Default Service Zone

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

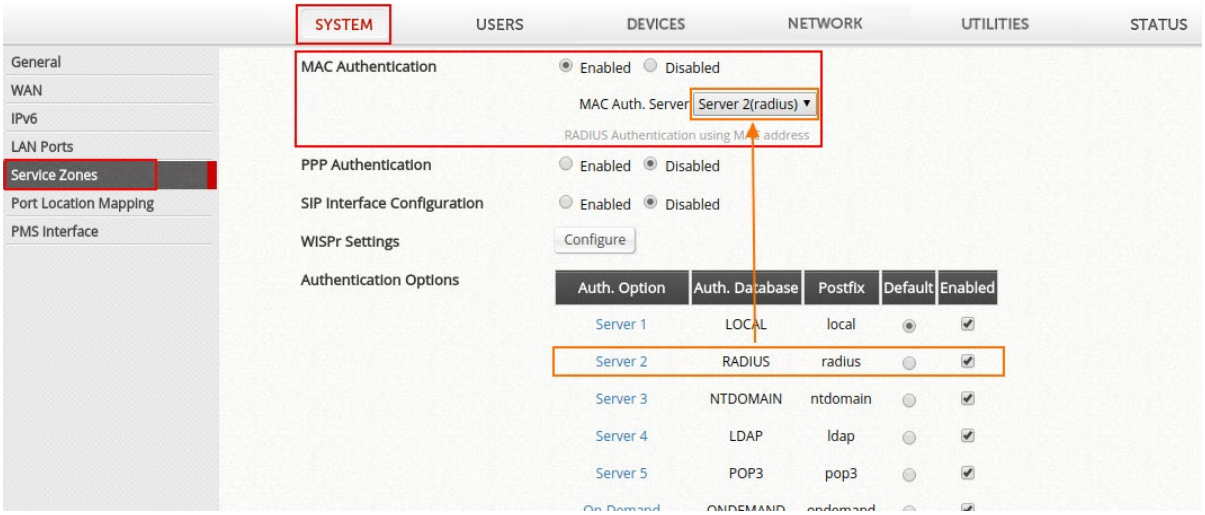

Figure 2.1b – MAC Authentication

For MAC Authentication to work, a pre-existing database of MAC addresses of the devices that are allowed on the network must be created and maintained in the associated RADIUS server. In other words, the MAC address (as both username and password) of each user

device must be created in the account database of the RADIUS server beforehand.

For instance, the following screenshot is a sample configuration file of FreeRADIUS, which includes an account "**acccc8e4ea147/acccc8e4ea147**" for the device with the MAC address of "AC:CC:8E:4E:A1:47". Note that username/password is in the format "aabbccddeeff" (no need to specify ":" or "-" contained in the MAC address).

```
[FreeRADIUS-Server:~]$ cat users
acccc8e4ea147 Cleartext-Password := "acccc8e4ea147"
              Session-Timeout = 3600,
              Idle-Timeout = 600,
              Acct-Interim-Interval = 60,
              Reply-Message = "MAC-Auth-Account"

testuser01    Cleartext-Password := "testpass01"
              Session-Timeout = 3600,
              Idle-Timeout = 600,
              Acct-Interim-Interval = 60,
              Reply-Message = "Test-Account"
```

Figure 2.1c – Sample Configuration File of FreeRADIUS Account Database

When a device is connected to the network, the controller will automatically obtain the MAC address from the system "ARP table", and perform authentication against the RADIUS server using the standard RADIUS protocol.

2.2 MAC Privilege List

Go to *Main Menu > USERS > Privilege Lists > MAC Privilege List*

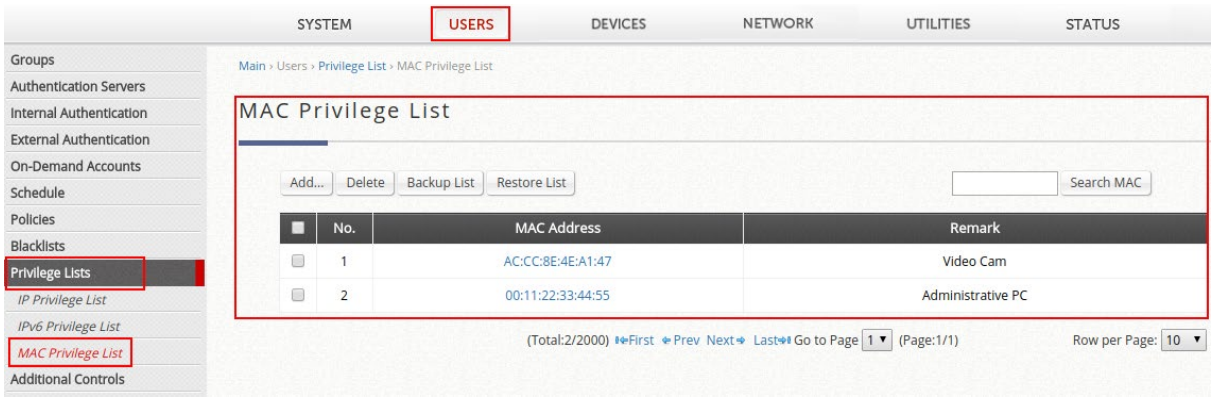

Figure 2.2a – MAC Privilege List

Users' devices on this MAC Privilege List are granted the network access automatically – i.e. users not required to enter username/password in a web browser in order to access the network.

2.3 MAC Access Control List

a. Go to *Main Menu > USERS > Additional Controls*, and scroll down to "MAC Access Control List" section.

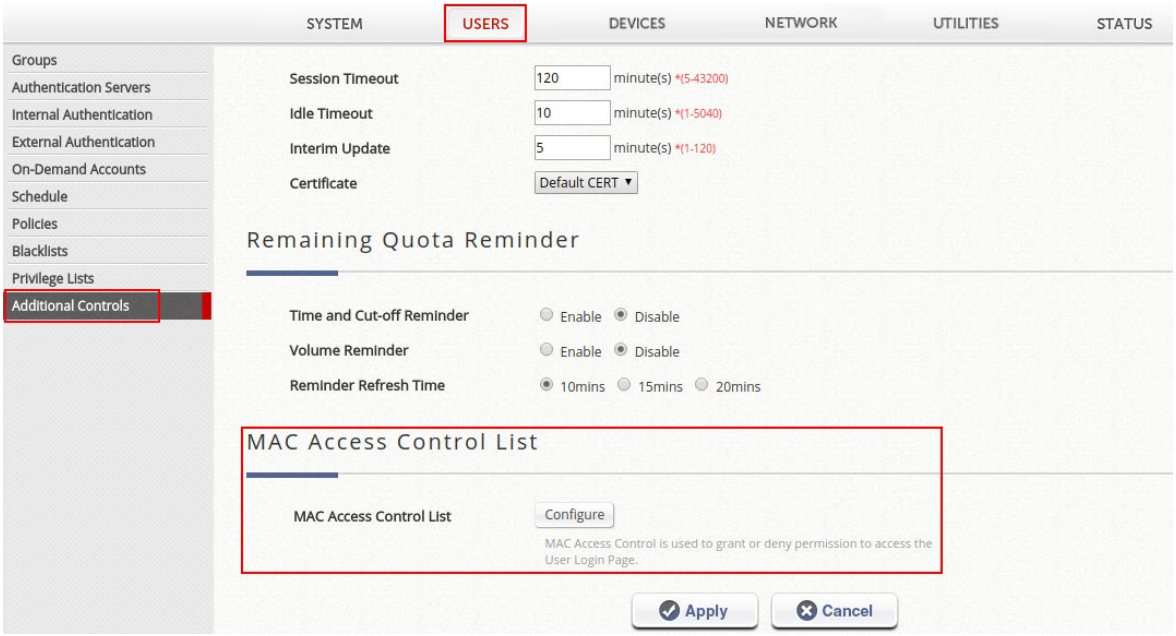

Figure 2.3a – MAC Access Control List Configuration

b. Click Configure to enter the configuration page.

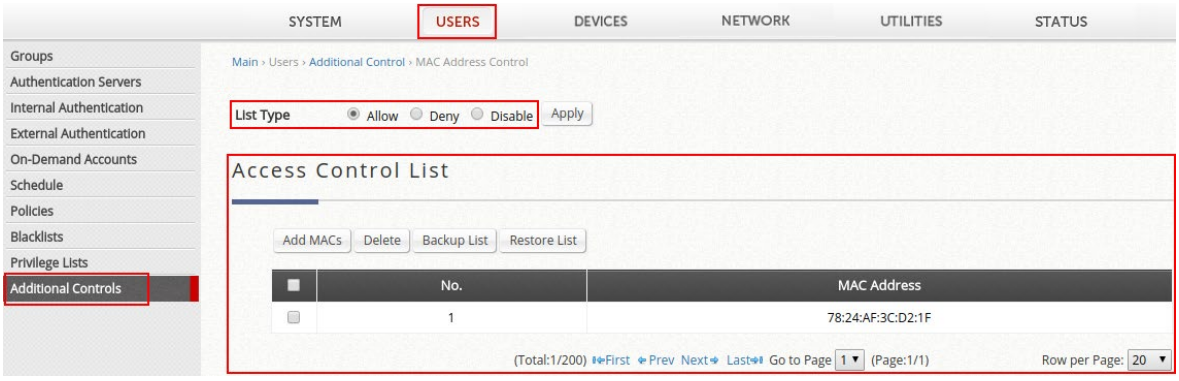

Figure 2.3b – MAC Access Control List

By "**List Type**", MAC ACL is used to grant or deny users' access to the Login Page (Captive Portal Page) upon entering any URL in a web browser --

Allow: This list acts as a "White List", i.e. only users' devices on this MAC ACL are allowed to see the Login Page.
Deny: This list acts as a "Black List", i.e. only users' devices on this MAC ACL are not allowed to see the Login Page (in this situation, users will see a blank page upon entering any URL in a

web browser).
Disable: This list, by default, is disabled, i.e. each user device is allowed to see the Login Page.

3 Remarks

Please contact Technical Support Team for additional inquiries.