tp-link MAC-Based Authentication Configuration User Guide

MAC-Based Authentication Configuration Guide

Contents

Overview

MAC-based authentication is an authentication method that controls users' right to access networks based on their MAC addresses. With MAC-Based Authentication enabled, the controller takes the wireless clients' MAC addresses as their usernames and passwords for authentication when the client
requests internet access for the first time. Clients can access the wireless networks configured with MAC-based authentication after passing authentication successfully.

MAC-based authentication method takes effect based on SSID. The MAC address is used as username and password in the authentication process. When the MAC address of the device is stored in the RADIUS server database and relevant configurations are completed on the controller, the device can access the internet without the need to enter the username and password. Meanwhile, devices whose MAC addresses are not in the database will be denied. During the process, the user does not need to manually enter the username or password, and the wireless devices don't need to install any client
software.

Example for Mac-based Authentication

Network Requirements

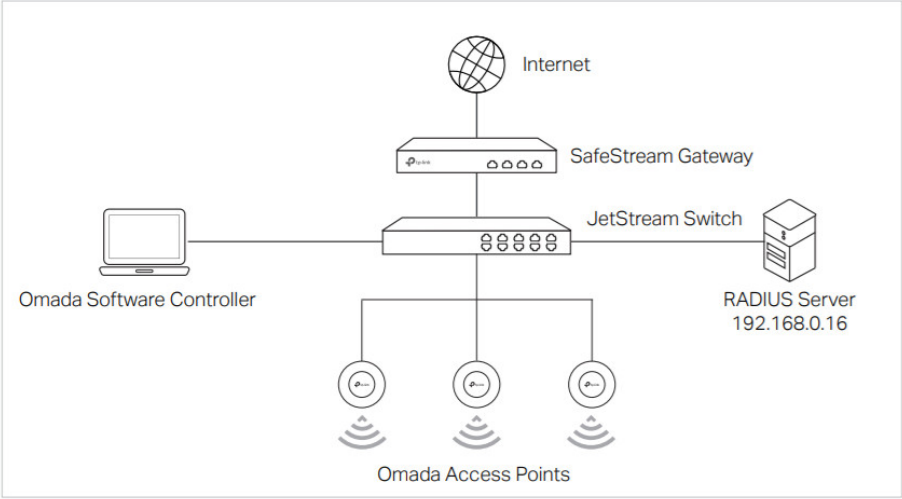
The network administrator wants to give a batch of wireless devices the right to access the internet.
These devices should be authenticated before getting access to the internet. For convenience, the authentication process is required to be operated automatically, and no extra client software is needed on the device. To meet the requirement, MAC-based authentication is recommended.

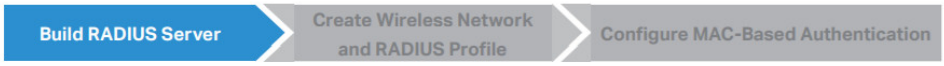
Configuration

MAC-based authentication authenticates the devices with their MAC address. Check the MAC addresses of the devices in advance. FreeRADIUS is used for demonstration in the configuration of MAC-based authentication with Omada SDN Controller. The process includes three steps as below.

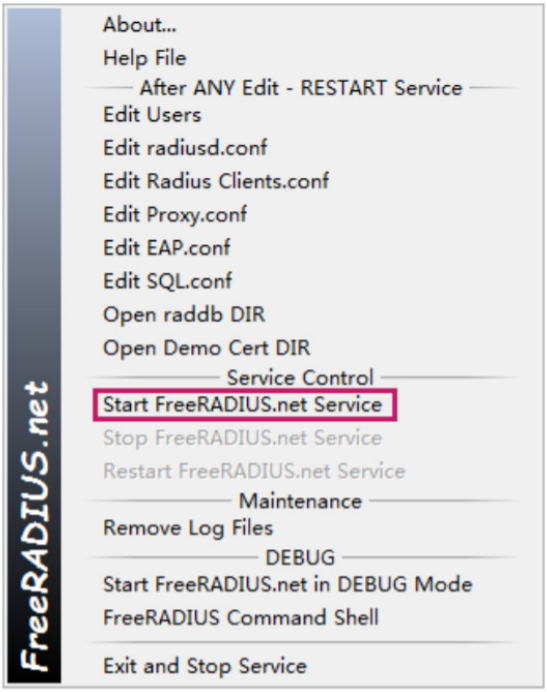
1. Build a RADIUS server.
2. Create a wireless network (SSID) and a RADIUS profile on the controller.
3. Configure MAC-based authentication on the controller.

Take Omada Software Controller as an example, the network topology is shown as below.

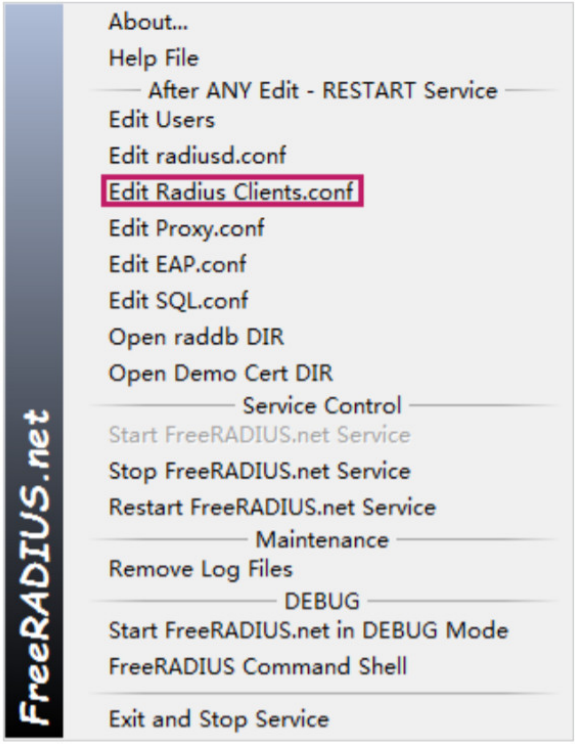




1. Download FreeRADIUS.net and follow the wizard to install it.
2. Right-click the icon to load the following page. Choose Start FreeRADIUS.net Service to start the RADIUS server.



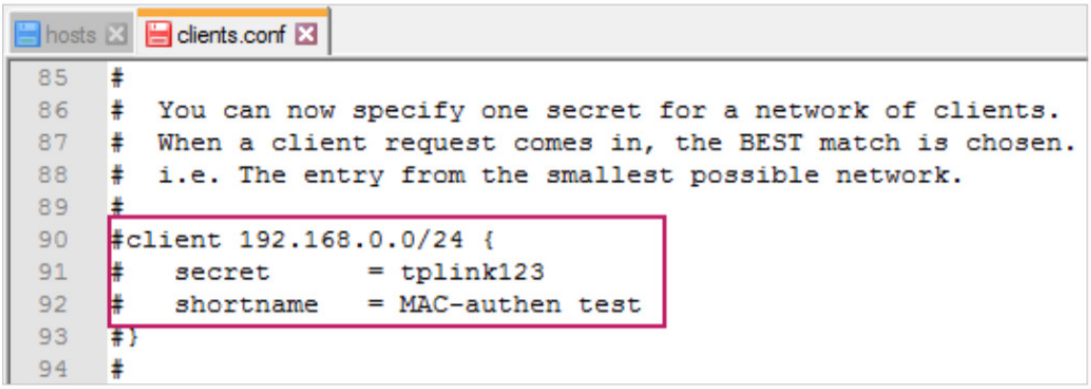
3. Right-click the icon and choose Edit Radius Clients. conf to add an entry for the RADIUS client.



One client section means a RADIUS client. You can choose one of the client sections and edit the following attributes, or add a new client section.

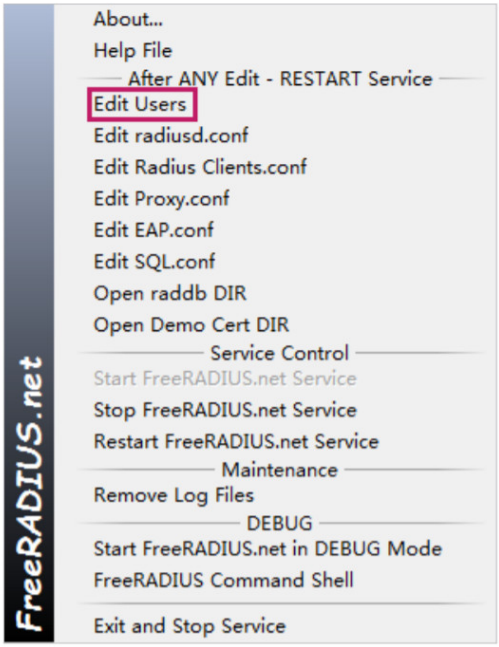
To avoid format error, it is recommended to use a code editor to edit the configuration file.

Notepad++ is used for demonstration in this guide. Edit or add the attributes and save the file.

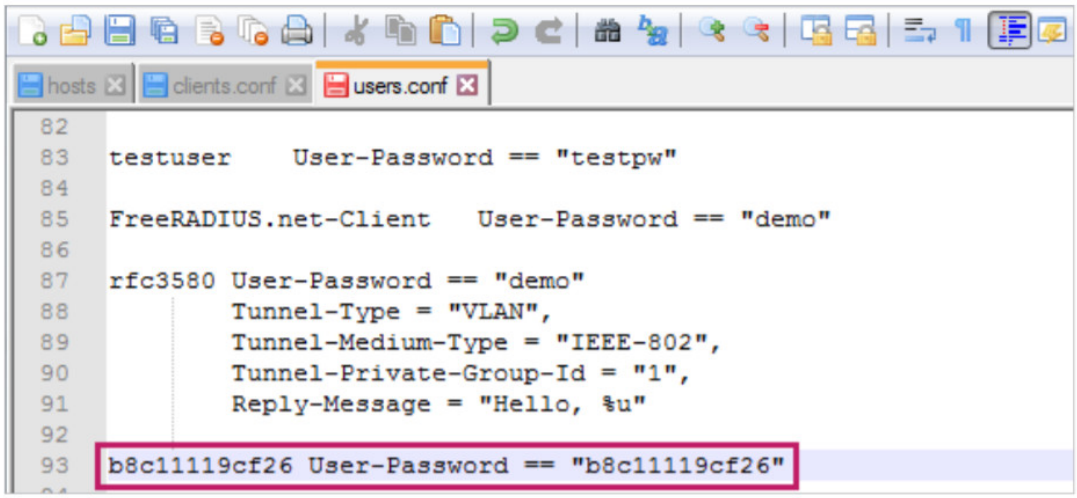


The First Line	Define the RADIUS client, which is usually a NAS (Network Access Server), in the format of “client [hostname | ip-address]”. Here you should enter the IP addresses of the EAPs. Note that FreeRADIUS supports entering IP addresses in the format of “IP/mask”, but other RADIUS servers may not support it. Check the supported format first when using other RADIUS servers.
Secret	Enter the shared key between the RADIUS server and the Controller. The RADIUS server and the Controller use the key string to encrypt passwords and exchange responses.
Shortname	(Optional) Enter a short name to identify the client section.

4. Right-click the icon and choose Edit Users to add MAC addresses of the devices into the database.



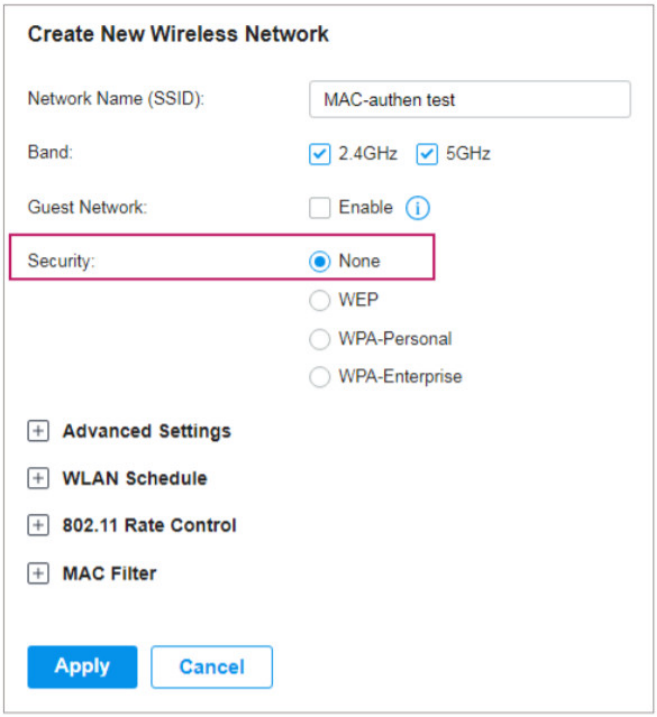
5. Add the MAC addresses of the devices into the database as username and password. Note that the format of the MAC address should be 12 hexadecimal digits in lowercase without any punctuation or space.



6. **Click** Restart FreeRaDIUS.net Service to restart FreeRaDIUS.net for the newly edited code to take effect.

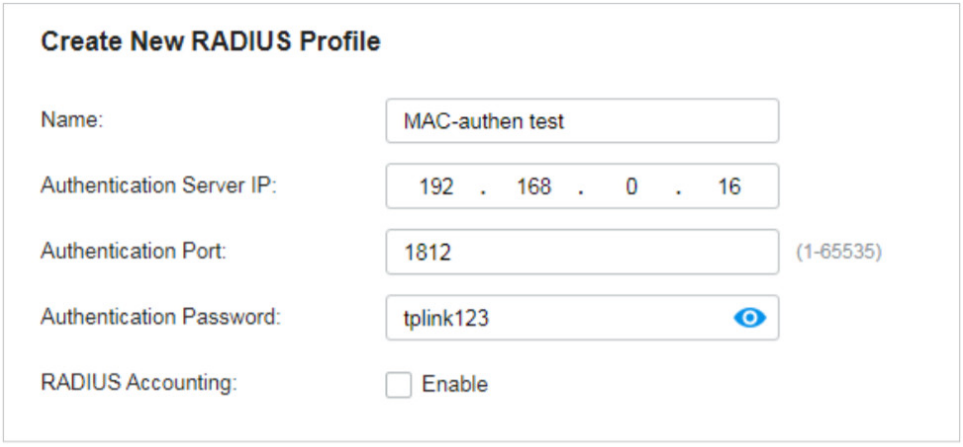
Build RADIUS Server > Create Wireless Network and RADIUS Profile > **Configure MAC-Based Authentication**

1. Go to Settings > Wireless Networks to create a wireless network.
2. Click + Create New Wireless Network to load the following page. Configure the basic parameters for the wireless network, and choose None as the security strategy.

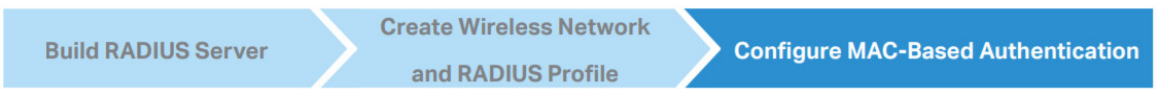


Network Name (SSID)	Enter the network name (SSID) to identify the wireless network. The MAC-based authentication takes effect based on SSIDs.
Band	Enable 2.4 GHz and/or 5 GHz radio band for the wireless network.
Guest Network	With Guest Network-enabled, all the clients connecting to the SSID are blocked from reaching any private IP subnet.
Security	Select the security strategy for the wireless network. When you want to use the SSID for MAC-based authentication, choose None as the security strategy, otherwise, a client needs to pass both MAC-based authentication and the security strategy you choose here before accessing the internet.

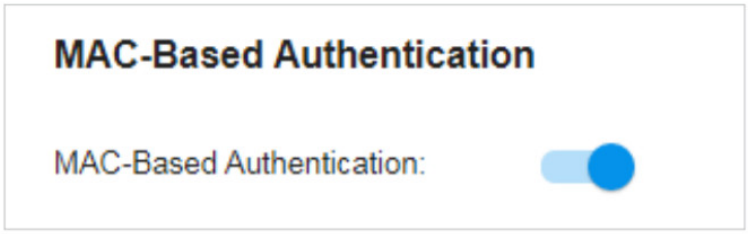
3. Go to Settings > Authentication > RADIUS Profiles to create a RADIUS profile.
4. Click + Create New RADIUS Profile to load the following page. Configure the following parameters.



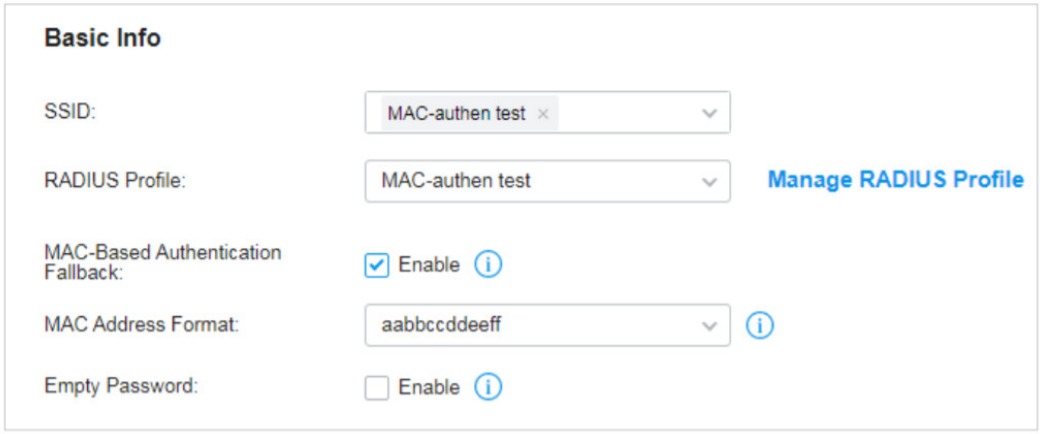
Name	Enter a name to identify the RADIUS profile.
Authentication Server IP	Enter the IP address of the authentication server. Here enter the IP address of the computer on which you install the freeRADIUS.net.
Authentication Port	Enter the UDP destination port on the authentication server for authentication requests. Port 1812 is the default port for RADIUS server authentication, so you can keep it in most cases.
Authentication Password	Enter the password that will be used to validate the communication between Omada devices and the RADIUS authentication server. Here enter the secret, namely the shared key you set in the free radius.



1. Go to Settings > Authentication > MAC-Based Authentication to enable the feature.



2. Configure the following parameters.



SSID	Select one or more SSIDs for MAC-based authentication to take effect.
RADIUS Profile	Select the RADIUS profile you have created from the drop-down list. The RADIUS profile records the information of the RADIUS server which acts as the authentication server during MAC-based authentication.
MAC-Based Authentication Fallback	If the wireless network is configured with both MAC-based authentication and portal authentication, when you enable this feature, a wireless client needs to pass only one authentication. The client tries MAC-based authentication first and is allowed to try Portal authentication if it failed the MAC-based authentication. When you disable this feature as default, a wireless client needs to pass both the MACbased authentication and portal authentication for internet access and will be denied if it fails either of the authentications.
MAC Address Format	Select clients' MAC address format which the controller uses for authentication. Then the controller will change the MAC addresses in the specified format, and they are used as usernames for the clients on the RADIUS server. Here in freeRADIUS.net, the MAC addresses are stored in the format of aabbccddeeff (12 hexadecimal digits in lowercase with no punctuation or space).
Empty Password	Click to allow a blank password for MAC-based authentication. With this option disabled, the password will be the same as the username.

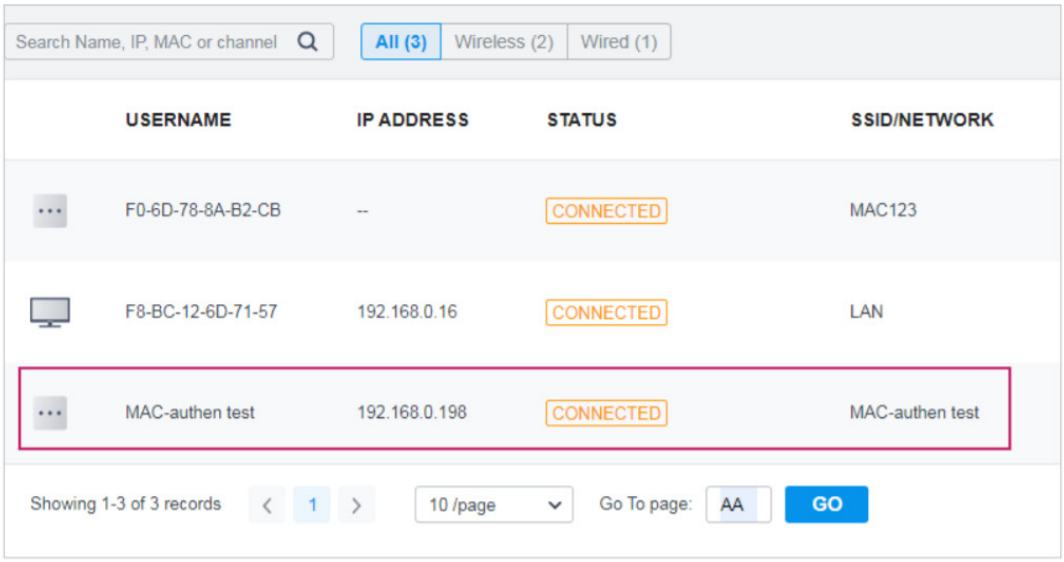
Verification of the Configuration

After all configurations are completed, you can follow the steps below to test whether the MAC-based authentication works.

1. Search for the wireless network on the device whose MAC address has been added into the database of the RADIUS server.

2. Select the SSID which you choose for MAC-based authentication to take effect.
3. If the device connects to the SSID and has access to the internet, it means the device has passed the authentication.

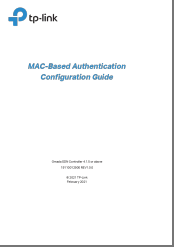
   Go to **Clients** and check, if the device is in the client list in the status of Connected, it means the device has passed the authentication.



Omada SDN Controller 4.1.5 or above
19110012900 REV1.0.0

February 2021

Documents / Resources

	tp-link MAC-Based Authentication Configuration [pdf] User Guide tp-link, MAC-Based, Authentication, Configuration