Configuration Guide

How to Configure WLAN Client MAC Authentication on the DWC-1000

Overview

This guide describes how to configure the D-Link DWC-1000 Unified Controller's wireless client MAC authentication.

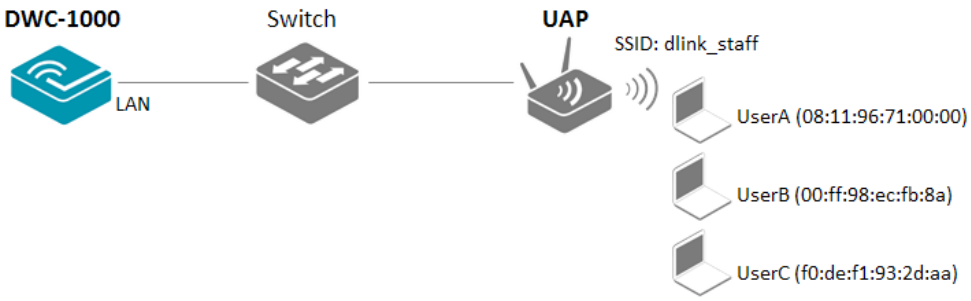
D-Link®

MAC authentication is useful in networks that operate in Open mode to grant and deny access to clients with specific MAC addresses. MAC Authentication can also be used in conjunction with 802.1X security methods, in which case MAC Authentication is done prior to 802.1X authentication. To enable MAC authentication, wireless clients must first be authenticated by the Unified Access Point (UAP) in order to connect to the network. There are two options for the authentication database: (a) local and (b) RADIUS.

Situation note

To control wireless access, network administrators can use WLAN MAC Authentication to grant or deny connection requests from wireless clients. The scenario in this guide features 3 wireless clients in the field who require wireless connection via the VAP (Virtual Access Point) dlink_staff. The wireless access rules are:

1. The client UserC is not in the Known Client list and will be denied wireless access.
2. The client UserA is in the Known Client list and will be granted wireless access.
3. The client UserB is in the Known Client list and may be granted or denied wireless access from time to time based on demand. For example, a company has overseas branch employees who will visit the company. These employees will be allowed wireless access when they use the office network temporarily on spare notebooks. When these notebooks are not in use by the overseas employees, the notebooks will not be allowed wireless access.



Configuration steps

1. The WLAN Clients MAC Authentication has two levels to define the actions to be taken for the list of Known Clients: (a) MAC Authentication Mode, and (b) MAC Authentication Action.
   MAC Authentication Mode defines whether the Known Clients list should be "white-list" or "black-list."
   MAC Authentication Action specifies which action should be taken. This is important because this is the first setting the system checks when authenticating clients and it takes precedence over the MAC Authentication Mode settings, unless "Global Action" is selected.

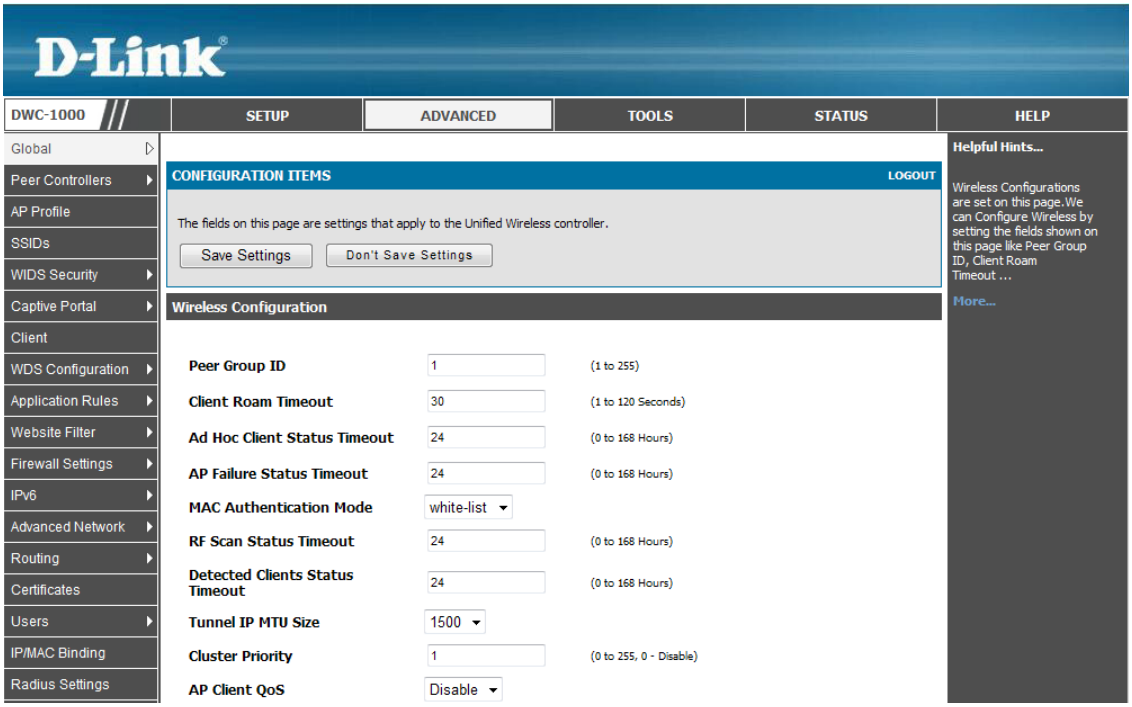
NOTE: The screenshots in this guide are from the DWC-1000's firmware version 4.1.0.10_10260W. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see on your browser.

To verify MAC Authentication Mode, first go to ADVANCED> Global> General/ MAC Authentication Mode, then select the global action to be taken with wireless clients. There are two global actions:

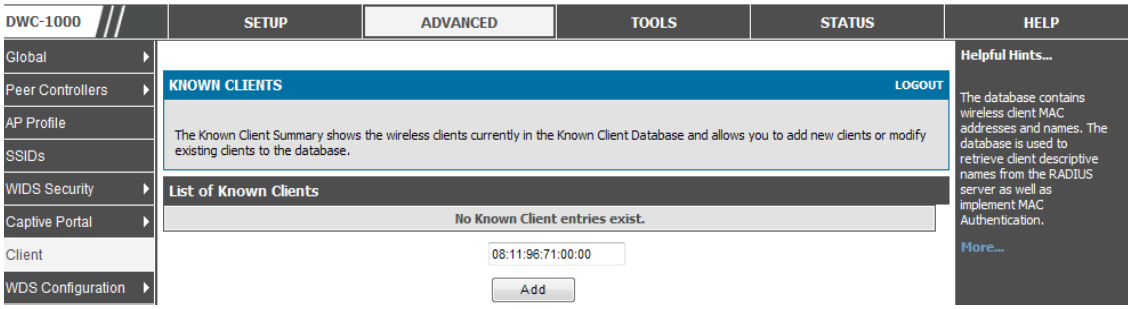
White-list: Select this option to grant access to any wireless clients with MAC addresses that are specified in the Known Clients database and are not explicitly denied access. If the MAC address is not in the database, then access will be denied to the client.

Black-list: Select this option to deny access to any wireless clients with MAC addresses that are specified in the Known Clients database, and are not explicitly granted access. If the MAC address is not in the database, then access will be granted to the client.

In this case, select "white-list" in MAC Authentication Mode. Click **Save Settings** to confirm.



2. To establish the client list in Known Clients, first go to ADVANCED> Client. Enter the MAC addresses of the wireless LAN adapter of each WLAN client. Click **Add**.



There are three types of actions that can be performed on a wireless client when MAC authentication is enabled on the network. These include:

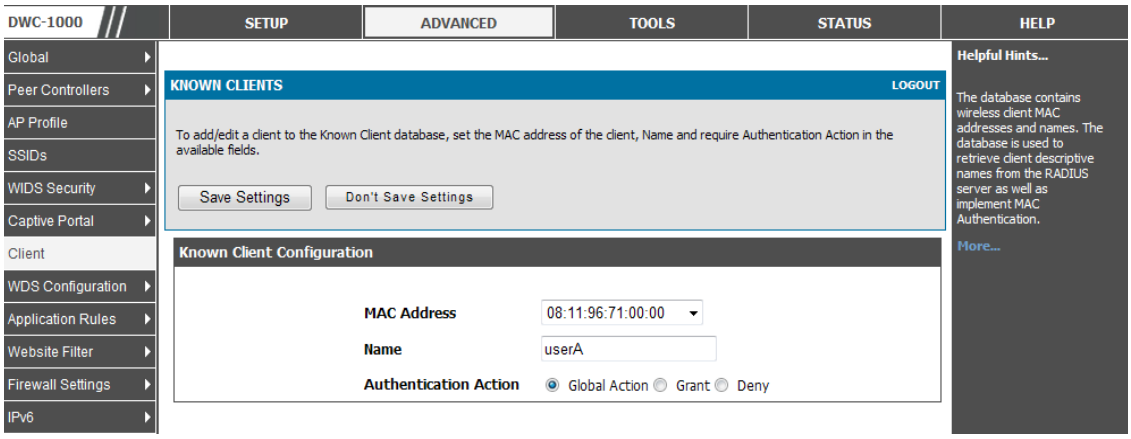
Grant— Allow the client with the specified MAC address to access the network.

Deny— Prohibit the client with the specified MAC address from accessing the network.

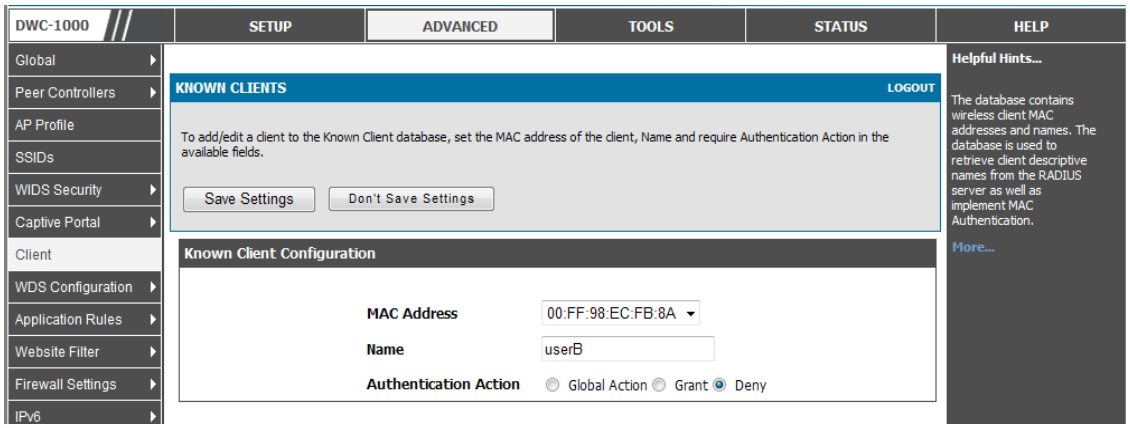
Global Action—Use the global white-list/black-list setting in ADVANCED> Global> General/ MAC Authentication Mode to determine how to handle the client. If Authentication Mode is set as "white-list," the client with the specificed MAC address will be automatically allowed to access the network; if Authentication Mode is set as "black-list," the client with the specificed MAC address will be prohibited from accessing the network.

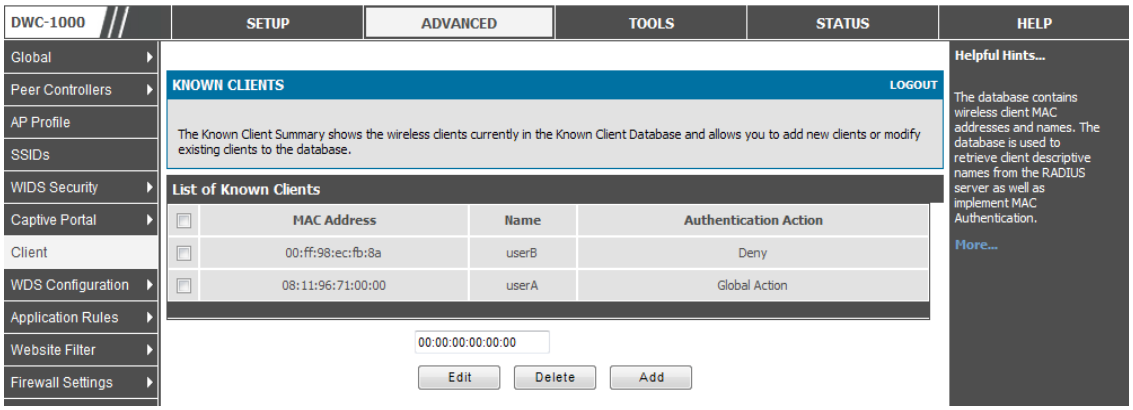
Grant and Deny in MAC Authentication are absolute actions which are not impacted by the settings in MAC Authentication Mode. For the clients not listed in the database, the action that will be taken will follow the settings in MAC Authentication Mode. If Authentication Mode is set as "white-list," the client who is not in the list is prohibited from accessing the network; if Authentication Mode is set to black-list, the client who is not in the list will be allowed to access the network.

In this case, as the MAC Authentication Mode is set as "white-list," the list in Known Clients serves as a "white-list" and all the accounts on this list will be allowed wireless connection. Add the UserA MAC address and select "Global Action" in Authentication Action.

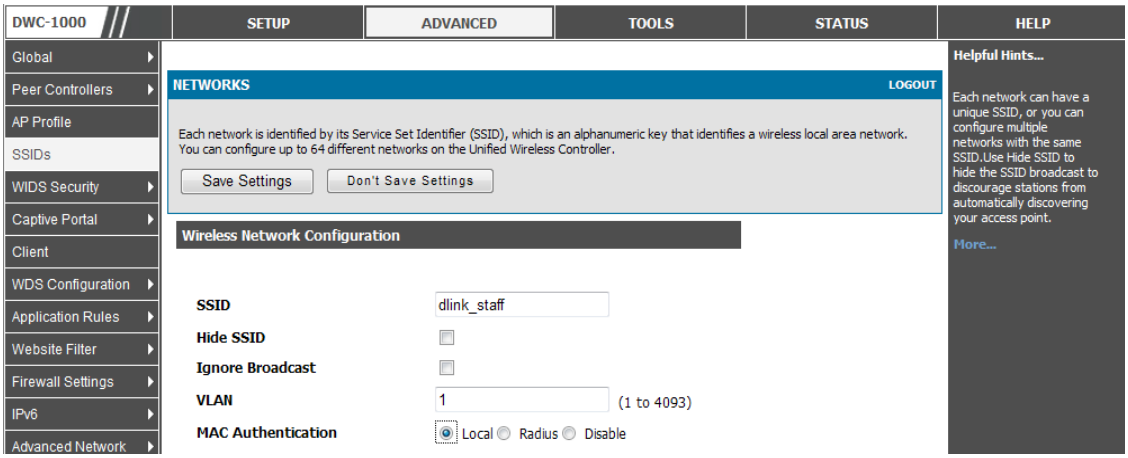


As UserB is a known client, the wireless connection request should be denied by default. Add the UserA MAC address and select "Deny" in Authentication Action.





3. Create an AP Profile and enable MAC Authentication. For the relavant AP profile settings, please refer to the "How to Configure AP Profile" guide. MAC Authentication can be triggered by each SSID. In the SSID session, enable MAC Authentication by choosing an authentication database from either Local or Radius. In this case, select "Local" for MAC Authentication.



4. To discover and manage an AP on the network, please refer to the "How to Configure L2 Discovery on the DWC-1000" guide.

5. The WLAN Client MAC Authentication result in this scenario will be:

Global Action: White-list

USER	ACTION
UserA (Global Action)	Grant
UserB (Deny)	Deny
UserC (not in the list)	Deny

If MAC Authentication Mode is set as Black-list, then the results based on user settings will be:
Global Action: Black-list

USER	ACTION
User (Global Action)	Deny
User (Deny)	Deny
User (Grant)	Grant
User (not in the list)	Grant

D-Link®

www.dlink.com