Configuration Guide

How to Configure a BYOD Environment with the DWS-4026

(MAC Authentication + Captive Portal)

Overview

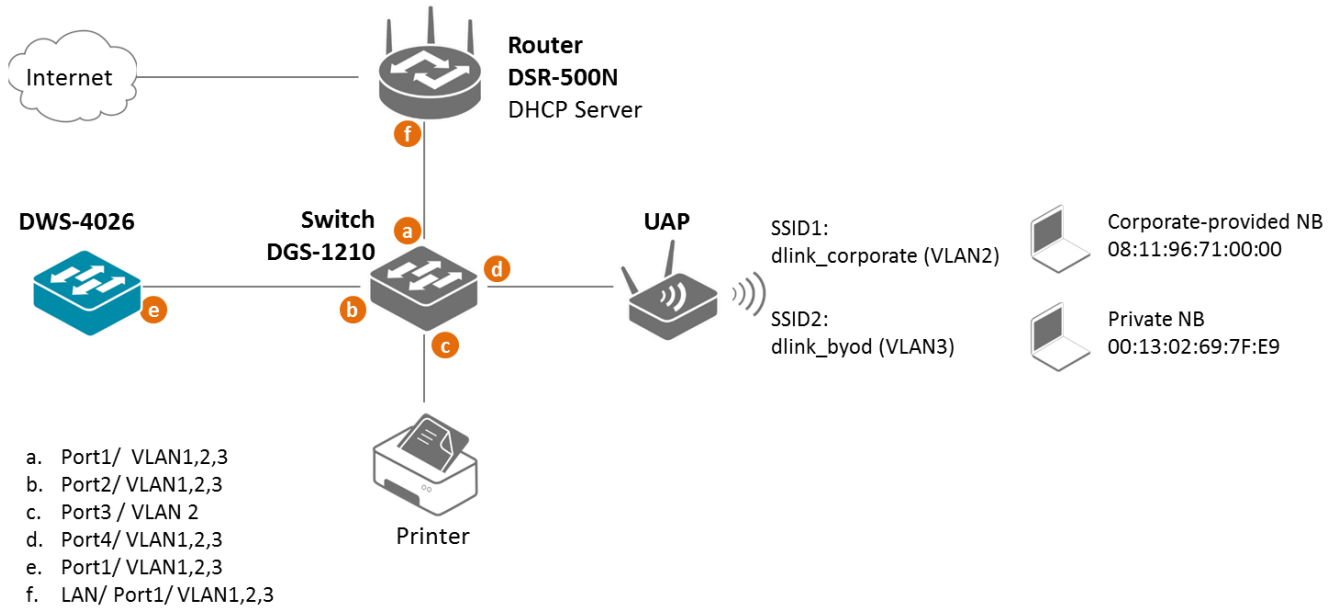
This guide describes how to configure and implement BYOD environment with the D-Link DWS-4026 Unified Switch for user and device authentication.

D-Link®

Situation Note

The trend of Bring Your Own Device (BYOD) in working place is a new challenge on network security and management. Many corporations that allow employees to use their own device at work expecting have better performance and productivity; however, on the downside, corporations also concern the network security and information leakage by using private device. How to distinguish corporate-provided device and private device (BYOD device), and give different authorities is the major task for IT teams.

The scenario in this guide shows you how to implement a BYOD environment with DWS-4026. Use device MAC authentication to enforce client associating specific SSIDs based on the device which is corporate-provided or private. All connection from SSIDs required performing authentication before granted authority.



The authentication methods on each SSID are different:

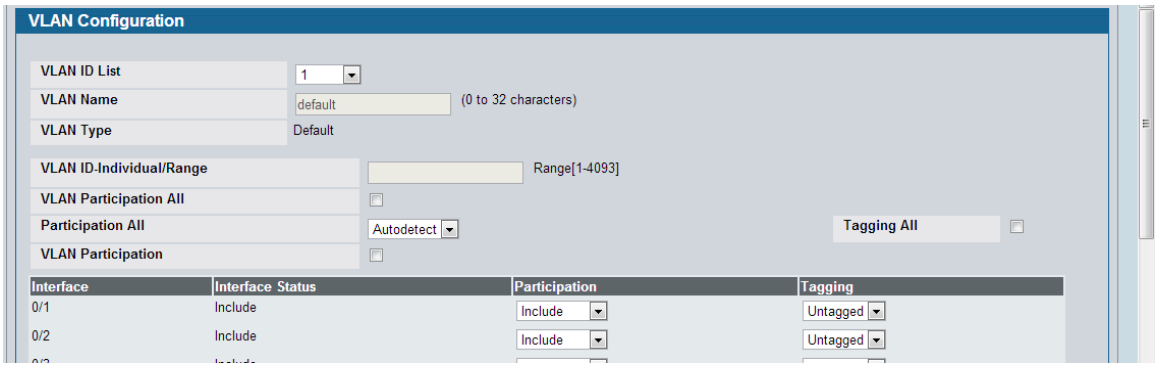
- dlink_corporate SSID: This SSID is for D-Link employee who works with cooperate-provided device. It requires device MAC authentication and Captive Portal to complete the authentication process. After complete authentication, the client is authorized in VLAN2 network.
- dlink_byod SSID: This SSID is for D-Link employee who works with his private device(BYOD device). It requires Captive Portal to complete the authentication process. After complete authentication, the client is authorized in VLAN3 network.

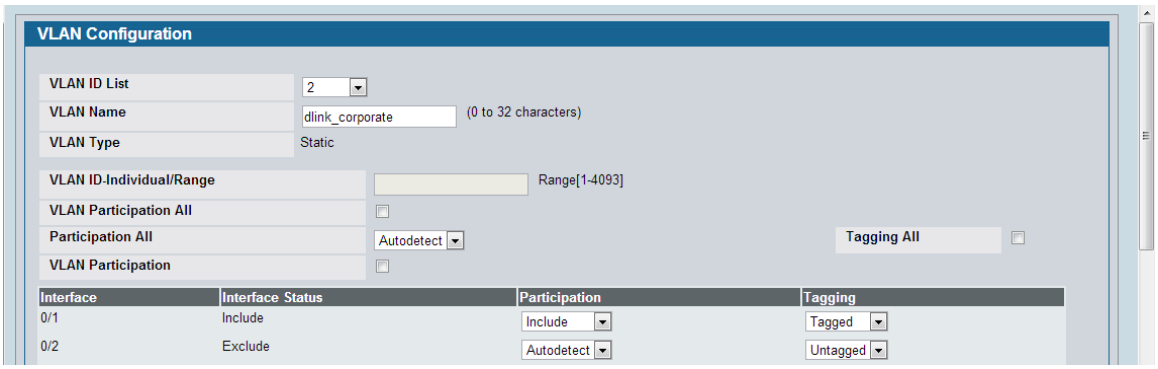
NOTE: The screenshots in this guide are from the DWS-4026's firmware version 4.3.0.3. If you are using an earlier version of the firmware, the screenshots may not be identical to what you see on your browser.

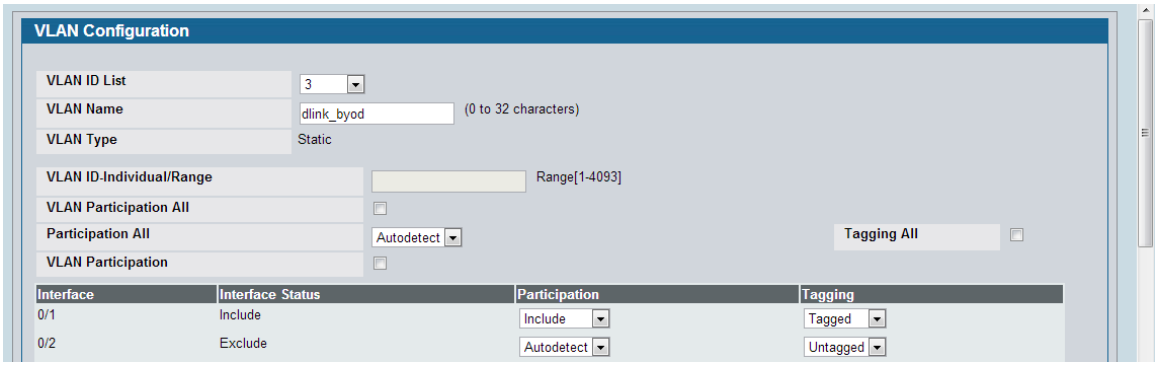
Configuration Steps (DWS-4026)

1. Set up VLANs based on the network architecture. Create three VLANs. VLAN1 is the default VLAN for AP management, VLAN2 is for the traffic associated from SSID dlink_corporate, and VLAN3 is for the traffic associated from SSID dlink_byod. Associate VLAN 1 to 3 memberships on Port1.

   Create three VLANs. Un-tag VLAN1, and tag VLAN2 and VLAN3 on port 1 (0/1). Navigate to LAN> DWS-4026> L2 Feature> VLAN> VLAN Configuration.

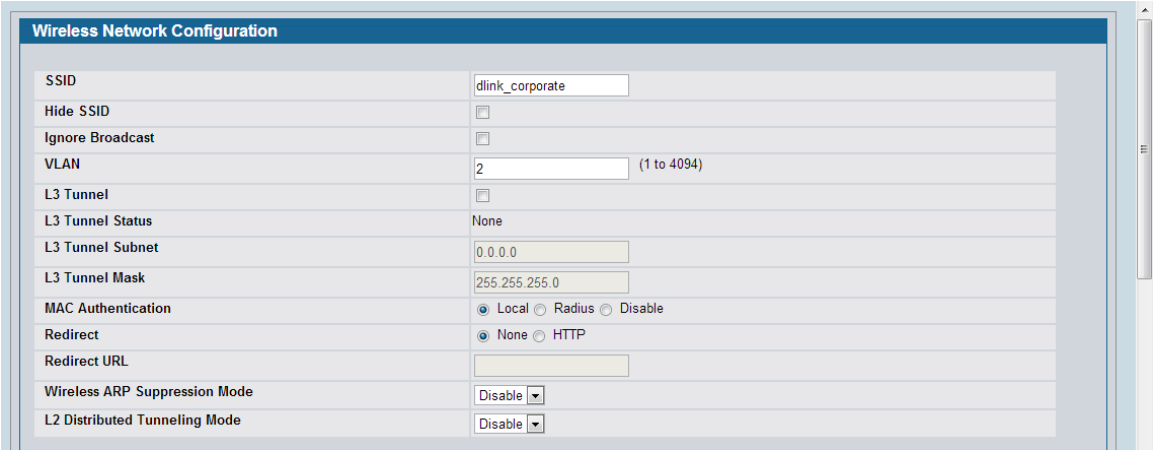


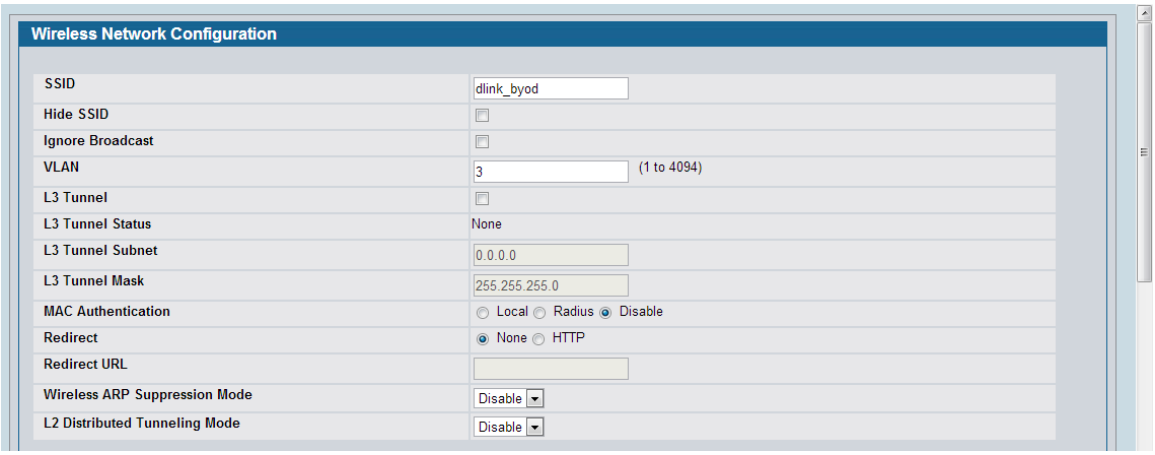


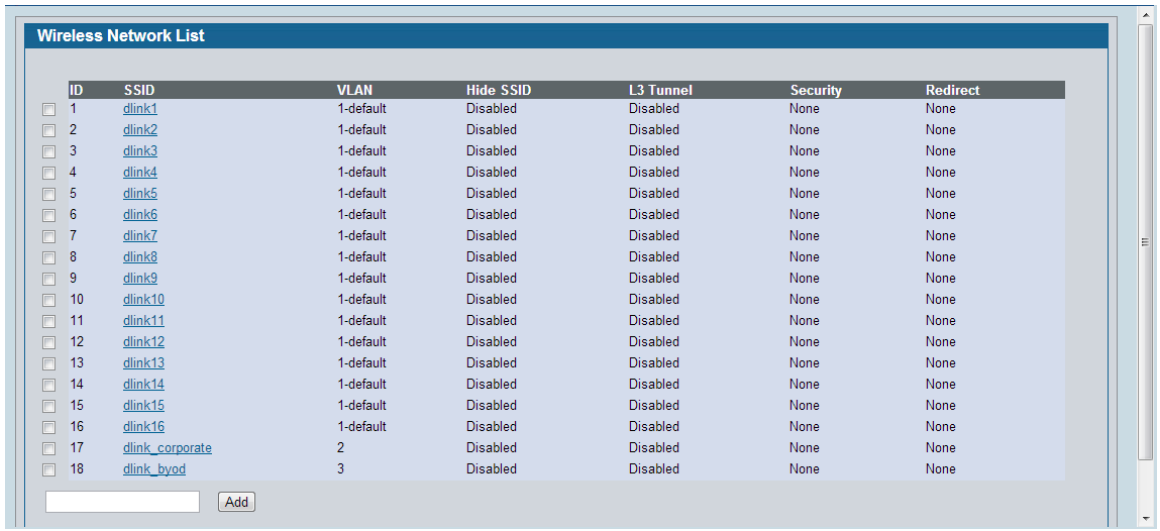


2. Create two SSIDs: SSID dlink_corporate and SSID dlink_byod, and assign VLAN 2 and 3 on these two SSIDs respectively. Enable MAC authentication on SSID dlink_corporate only. The MAC authentication database can be either (a) local database or (b) external RADIUS.

   Set up two SSIDs. For the MAC authentication, if the MAC authentication database is local database, select "Local" on MAC Authentication, if RADIUS, select "RADIUs" on MAC Authentication. In this case, use local database as authentication server. Navigate to WLAN> DWS-4026> Administration> Networks.



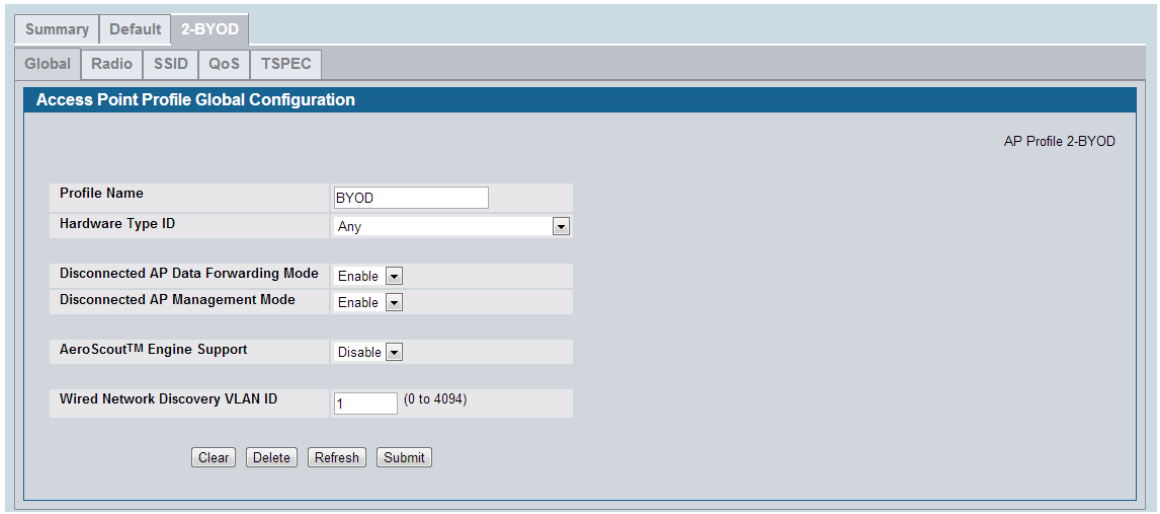




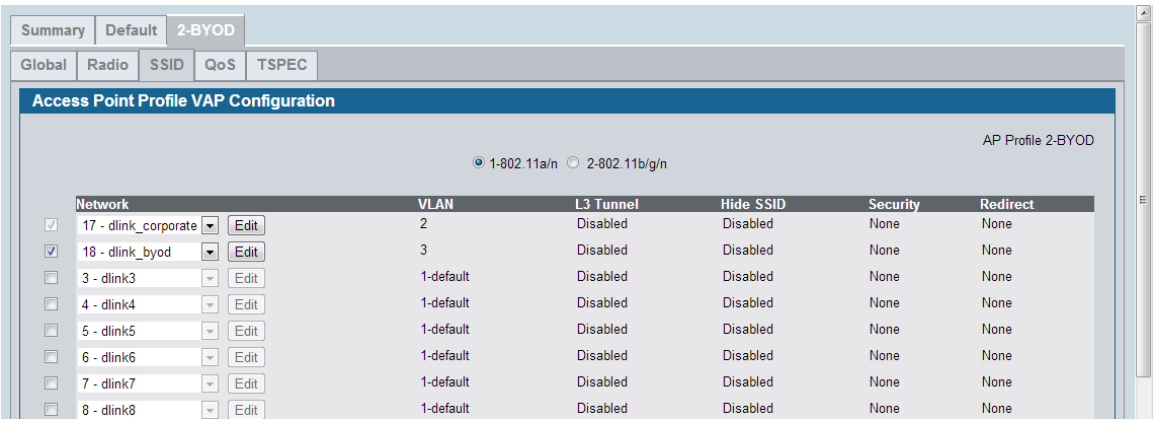
ID	SSID	VLAN	Hide SSID	L3 Tunnel	Security	Redirect
1	dlink1	1-default	Disabled	Disabled	None	None
2	dlink2	1-default	Disabled	Disabled	None	None
3	dlink3	1-default	Disabled	Disabled	None	None
4	dlink4	1-default	Disabled	Disabled	None	None
5	dlink5	1-default	Disabled	Disabled	None	None
6	dlink6	1-default	Disabled	Disabled	None	None
7	dlink7	1-default	Disabled	Disabled	None	None
8	dlink8	1-default	Disabled	Disabled	None	None
9	dlink9	1-default	Disabled	Disabled	None	None
10	dlink10	1-default	Disabled	Disabled	None	None
11	dlink11	1-default	Disabled	Disabled	None	None
12	dlink12	1-default	Disabled	Disabled	None	None
13	dlink13	1-default	Disabled	Disabled	None	None
14	dlink14	1-default	Disabled	Disabled	None	None
15	dlink15	1-default	Disabled	Disabled	None	None
16	dlink16	1-default	Disabled	Disabled	None	None
17	dlink_corporate	2	Disabled	Disabled	None	None
18	dlink_byod	3	Disabled	Disabled	None	None

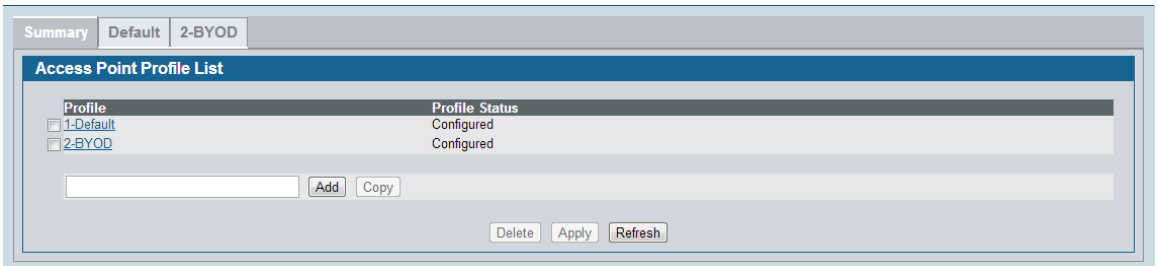
3. Create an AP Profile and associate SSIDs on it.

3-1. Create an AP Profile "BYOD". Navigate to WLAN> DWS-4026> Administration> Advanced Configuration> AP Profiles> BYOD> Global.



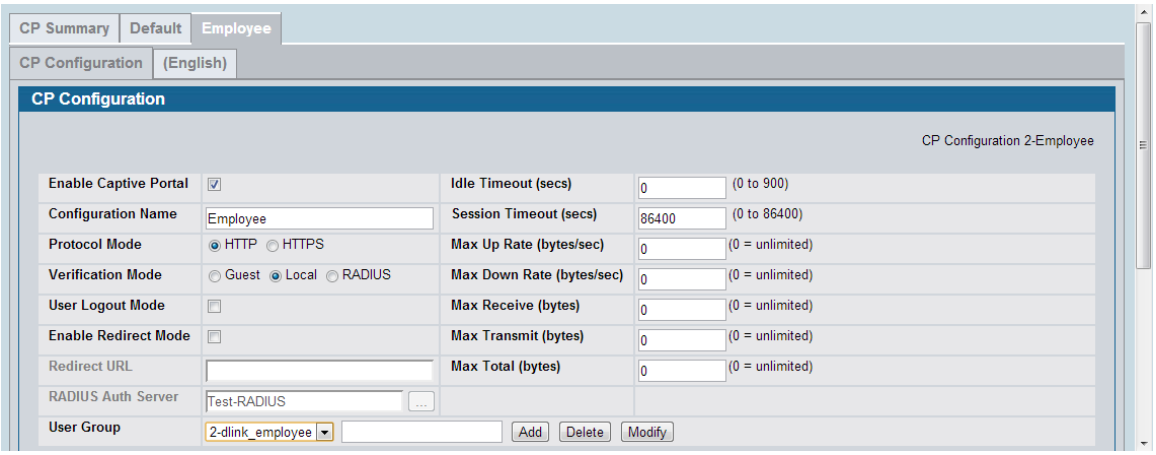
3-2. Associate SSID dlink_corporate and dlink_byod on this AP Profile. Navigate to WLAN> DWS-4026> Administration> Advanced Configuration> AP Profiles> BYOD> SSID.





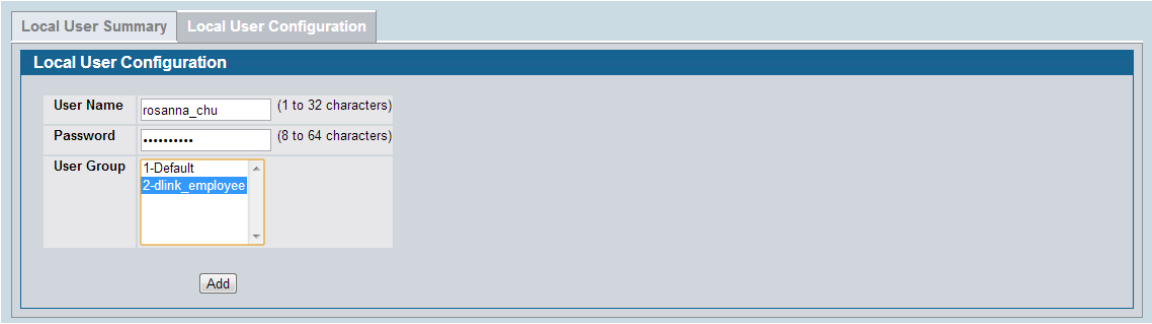
4. Create a CP Profile. Select the authentication server on the Captive Portal. The authentication server can be either (a) local database or (b) external RADIUS. In this case, use local database as authentication server.

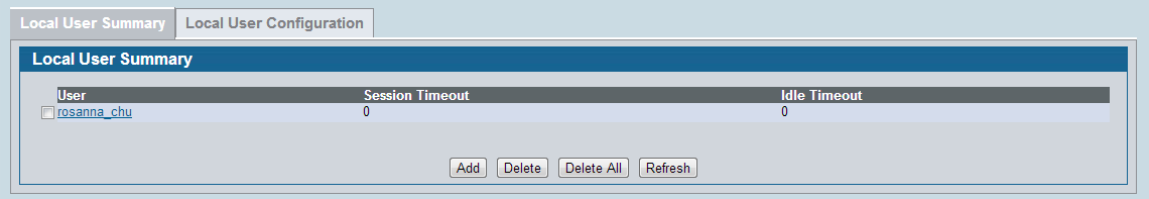
   Navigate to WLAN> DWS-4026> Security> Captive Portal> CP Configuration. There are three settings: (a) Create a CP Profile "Employee". (b) Select Verification Mode. If the user authentication database is local database, select "Local" on Verification Mode, if RADIUS, select "RADIUS" on Verification Mode. In this case, use local database as authentication server. (c) Add one User Group "dlink_employee", and then select it as User Group.



5. Create Captive Portal accounts on local database.

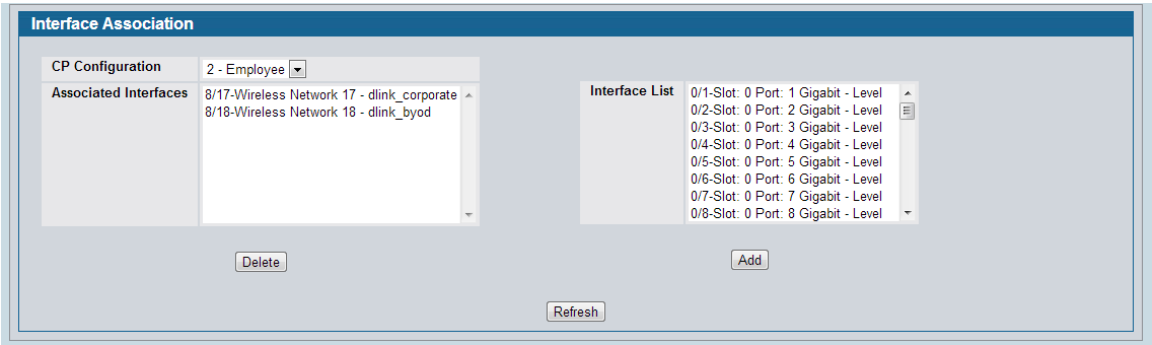
   Create user account under User Group "2-dlink_employee". Navigate to WLAN> DWS-4026> Security> Captive Portal> Local User.





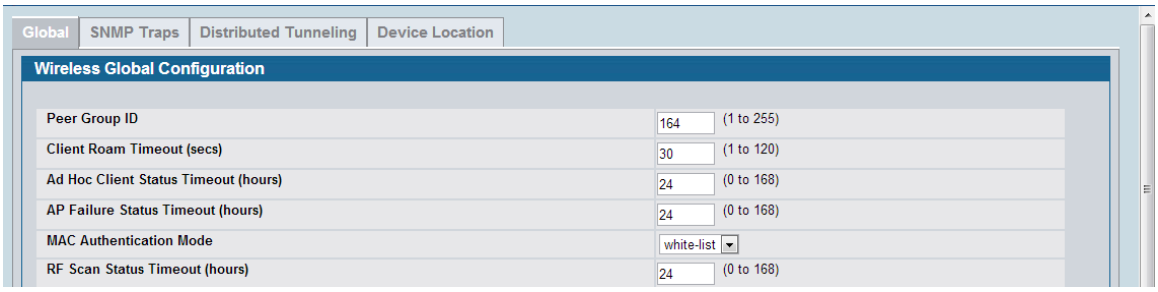
6. Associate these two SSID interfaces on CP Configuration "2-Employee".

   Select CP Configuration "2-Employee". Add interface SSID dlink_corporate and SSID dlink_byod on Associated Interfaces. Navigate to WLAN> DWS-4026> Security> Captive Portal> Interface Association.

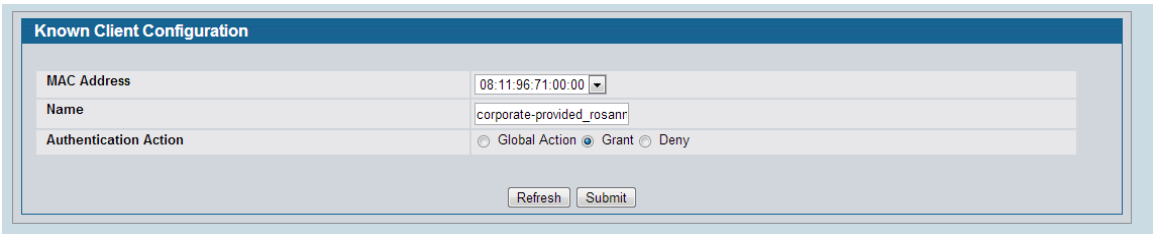


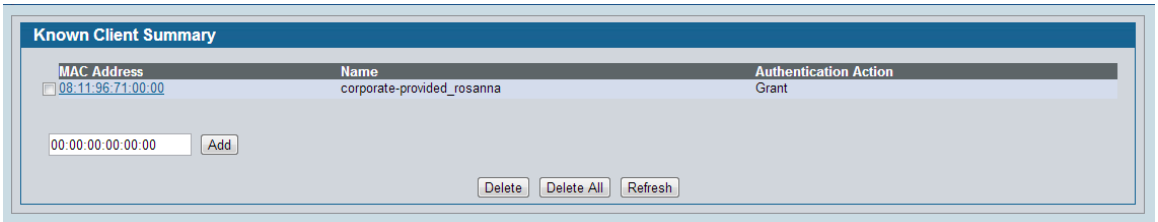
7. Create device MAC authentication database on local database.

7-1. Choose MAC Authentication Mode as "white-list". Navigate to WLAN> DWS-4026> Administration> Advanced Configuration> Global.



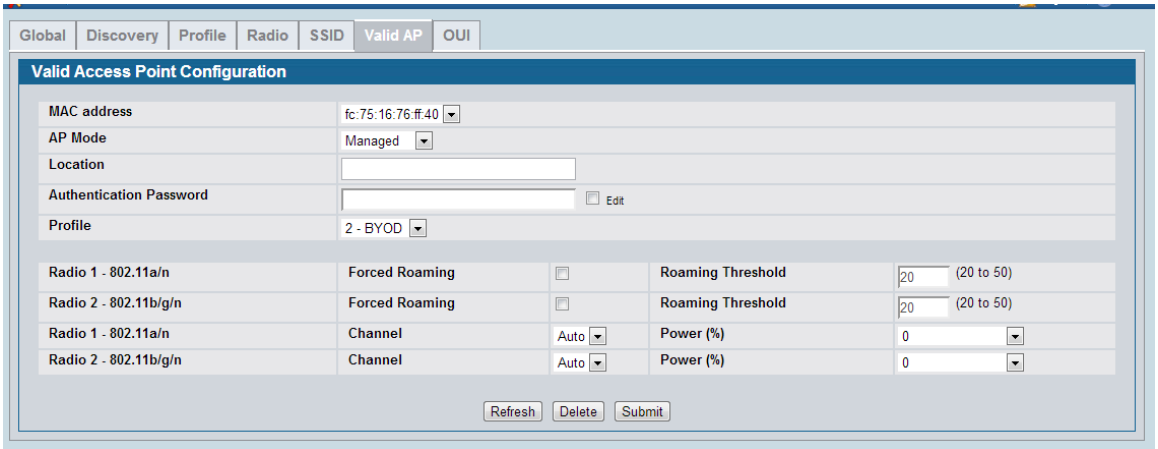
7-2. Create device MAC authentication accounts in the Known Client database. Add corporate-provided NB MAC 08:11:96:71:00:00 in the database. The Authentication Action is "Grant". Navigate to WLAN> DWS-4026> Administration> Advanced Configuration> Client> Known Clients.

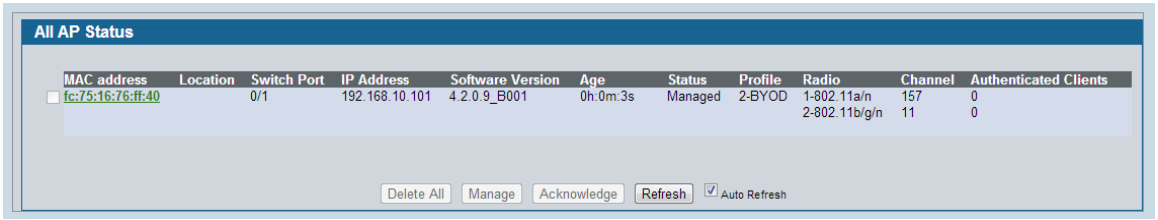




8. Discover and manage an AP from the network.

Manage AP. Navigate to WLAN> DWS-4026> Monitoring> Access Point> All AP Status.

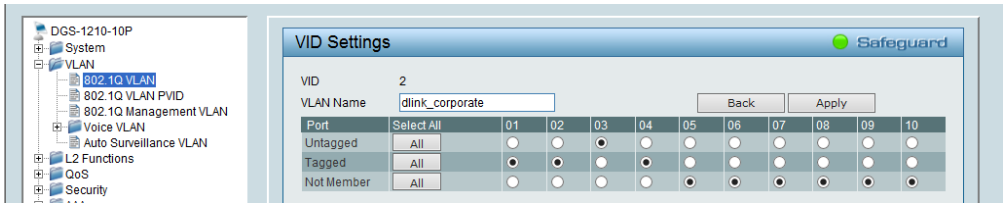


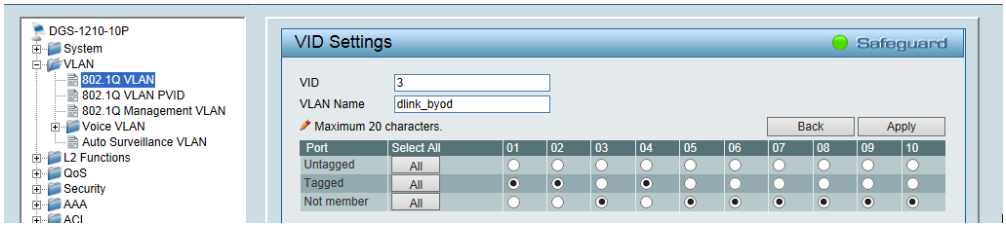


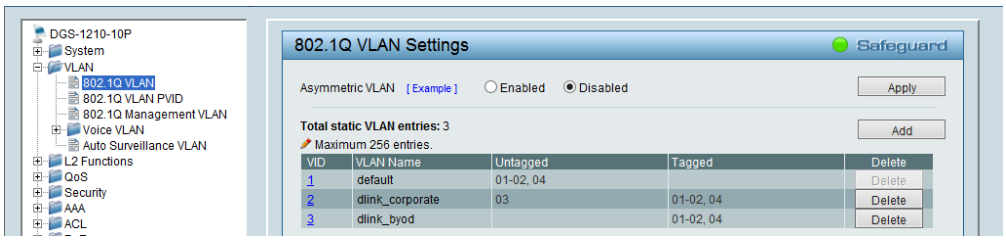
Configuration Steps (DGS-1210)

1. Set up VLANs based on the network architecture. Create three VLANs. VLAN1 is the default VLAN for AP management, VLAN2 is for the traffic associated from SSID dlink_corporate, and VLAN3 is for the traffic associated from SSID dlink_byod. As DWS-4026 VLAN1 is un-tag VLAN, set VLAN1 as un-tag VLAN on switch. The VLAN table is as below.

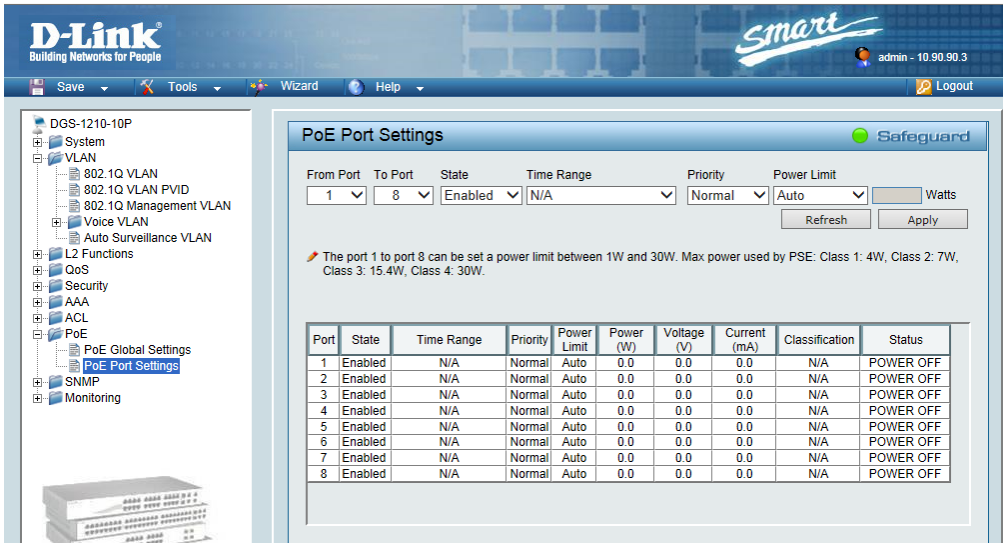
	Port1	Port2	Port3	Port4
VLAN1	Un-tag	Un-tag	-	Un-tag
VLAN2	Tag	Tag	Un-tag	Tag
VLAN3	Tag	Tag	-	Tag







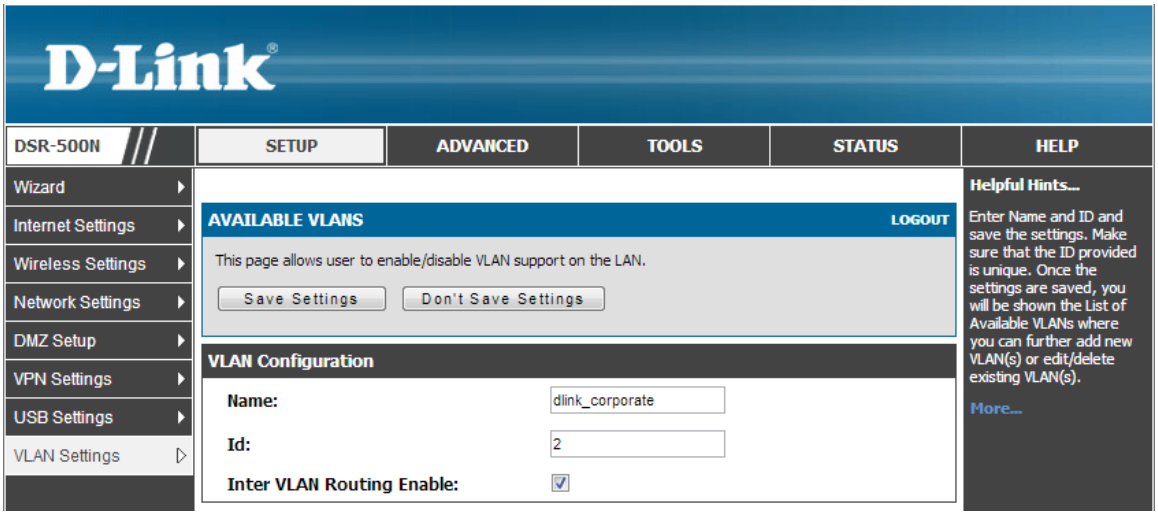
2. (Option) Enable PoE on the ports which connect with APs if needed. In default, all ports are enabled auto PoE detection.

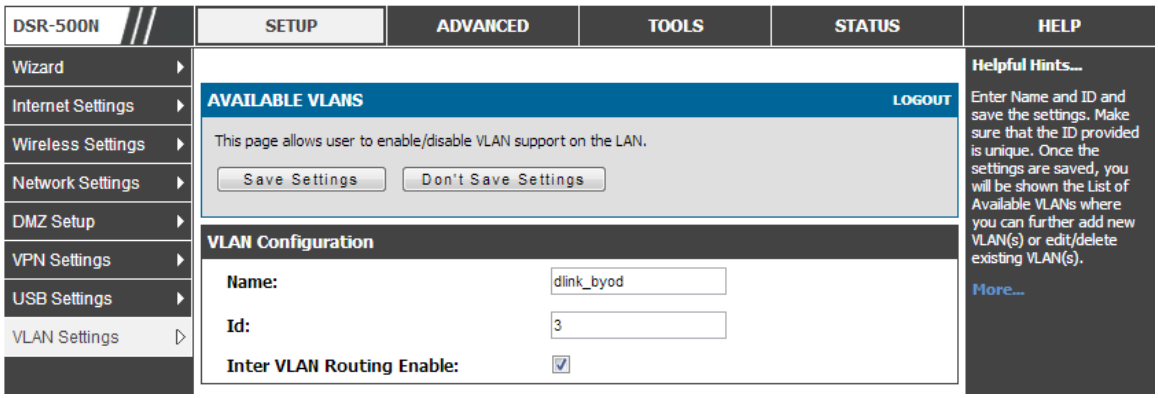


Configuration Steps (DSR-500N)

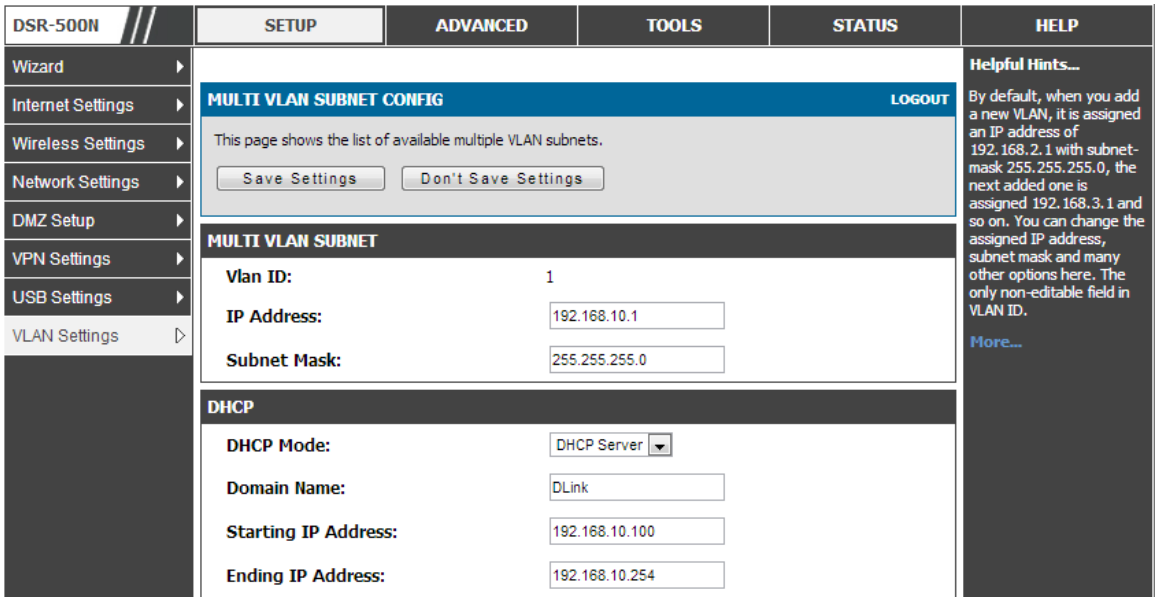
1. Set up VLANs based on the network architecture. Create three VLANs. VLAN1 is the default VLAN for AP management, VLAN2 is for the traffic associated from SSID dlink_corporate, and VLAN3 is for the traffic associated from SSID dlink_byod.

   1-1. Set up VLAN2 and VLAN3. Navigate to SETUP> VLAN Settings> Available VLANs.



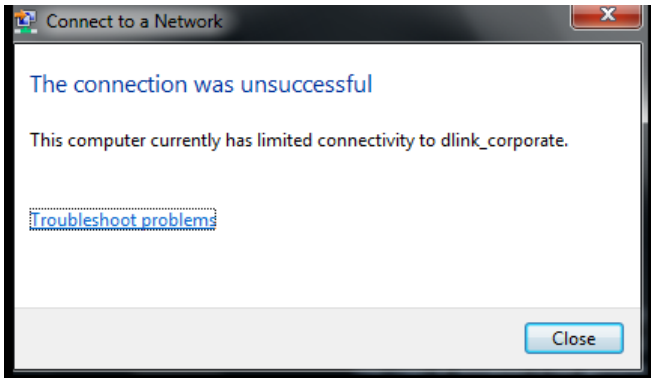


   1-2. Enable DHCP server on default VLAN, VLAN2 and VLAN3. Navigate to SETUP> VLAN Settings> Multiple VLAN Subnets.



Proof of Concept

1. The NB with MAC 08:11:96:71, which is the corporate-provided device, is allowed get IP address from both SSIDs. But for the NB with MAC 00:13:02:69:7F:E9, which is the private device, is allowed get IP address only from SSID dlink_byod. If it associates SSID dlink_corporate, it could not get IP address and would get error message as below. The MAC authentication forces the private device associate network from SSID dlink_byod



2. After NB associates with SSID and gets IP address, the system requires processing Captive Portal to identify the user.

3. While the corporate-provided NB associates SSID dlink_corporate and completes the authentication, it can access resources on VLAN2, for example, printer and internet.

4. While the corporate-provided or private NB associates SSID dlink_byod and completes the authentication, it can access resources on VLAN3, for example, internet.

www.dlink.com