## How to Setup Windows 2008 RADIUS Server for DWS-4026?

<u>Topology:</u>

Windows Server 2008 (RADIUS Server) ------ DWS-4026 Windows Server 2008 IP address: 10.90.90.100 DWS-4026 IP address: 10.90.90.90

## **RADIUS Server Settings:**

1-1. Setup the Radius client as your switch on NPS

Hie Action view Heip		
	RADIUS Clients         RADIUS Clients         RADIUS clients allow you to specify the network access servers, that provide access to y         ent       Configure RADIUS Clients         Configure RADIUS Server Groups         Aemote RADIUS server groups allow you to specify where to forward connection request         NPS server is configured as a RADIUS Proxy.         Configure Remote RADIUS Server Groups         Configure Remote RADIUS Server Groups	Actions RADIUS Cli A View Help
la de la companya de		his -

1-2. Enter the IP address of your wireless switch then click OK.

Enable this RADIUS client	<b>N</b>
Name and Address	
Friendly name:	
Wireless Switch	
Address (IP or DNS):	
10.90.90.90	Venfy
Vendor Specify RADIUS Standard for most RA vendor from the list. Vendor name:	DIUS clients, or select the RADIUS client
RADIUS Standard	×
<ul> <li>Manual</li> <li>C Genera</li> <li>Shared secret:</li> </ul>	te
Manual     C Genera Shared secret: Confirm shared secret:	te
Manual     Genera Shared secret: Confirm shared secret: Additional Options	te
Manual     Genera Shared secret: Confirm shared secret: Additional Options Access-Request messages must or RADIUS client is NAP-capable	ite

1-3. The RADIUS client item will be shown in the list.

Double click the item to configure it.



1-4. Enter the RADIUS secret into the *Shared secret* fields.

10000202020	
ettings	
Enable this RADIUS client	
Friendly name:	
Wireless Switch	
Address (IP or DNS):	
10.90.90.90	Verify
rrom the list. Vendor name:	RADIUS Standard
To manually type a shared secret, cli click Generate. You must configure ti here. Shared secrets are case-sensit	ck Manual. To automatically generate a shared secret, he RADIUS client with the same shared secret entered ive.
To manually type a shared secret, cli click Generate. You must configure t here. Shared secrets are case-sensit Manual C Ge	ck Manual. To automatically generate a shared secret, he RADIUS client with the same shared secret entered ive:
To manually type a shared secret, cli click Generate. You must configure t here. Shared secrets are case-sensit Manual G Ge Shared secret:	ck Manual. To automatically generate a shared secret, he RADIUS client with the same shared secret entered ive.
To manually type a shared secret, cli click Generate. You must configure t here. Shared secrets are case-sensit Manual Shared secret: Confirm shared secret:	ck Manual. To automatically generate a shared secret, he RADIUS client with the same shared secret entered ive.
To manually type a shared secret, cli click Generate. You must configure t here. Shared secrets are case sensit Manual Shared secret: Confirm shared secret: Access-Request messages must.	ck Manual. To automatically generate a shared secret, he RADIUS client with the same shared secret entered ive. enerate
To manually type a shared secret, cli click Generate. You must configure t here. Shared secrets are case sensit Manual Shared secret: Confirm shared secret: Access-Request messages must	ck Manual. To automatically generate a shared secret, he RADIUS client with the same shared secret entered ive.

DWS-4000 Settings:

2-1. Configure the RADIUS server.

Input the RADIUS server's IP address into Host Address field and click Submit.

11	Attiches Thidle A Base	
	D-LICK	1 3 5 7 9 11 13 15 17 19 21 23 Combot Comboo
D-Link	Power     O Link/ACT/Spec	
Ruilding Networks for Poople	o Console o RPS	
bunuing Networks for People	DW/S-4024 Concole	2 4 6 8 10 12 14 16 18 20 22 24 Combo& Combo&
	A STATE A STATE AND A STATE AN	
	Tool	
DWS-4024	Configuration Named Company Status	
	Configuration   Named Server Status	
Administration	RADIUS Authentication Server Configuration	
the L2 Features	Tendro Automatian der ver configuration	
E Cal L3 Features	PADILIS Server Host Address	(A 44 (44)
🖻 🧰 QoS	Replos Server Host Address	Add
🗄 🧰 Access Control Lists	Host Address	(10.90.90.100
(E Security	RADIUS Server Name	Default PADIUS Server
HEL Port Security Administ		Jueradie en de la constance
Port Security Interface		Submit
Port Security Static		
SSL Configuration		
SSH Configuration		
🗉 🧰 Captive Portal		
EL RADIUS Configurat		
E RADIOS Autoentica		
RADIUS Accounting		
Clear RADIUS Stati		
< · · · · · · · · · · · · · · · · · · ·		

2-2. Input the secret key into the *Secret* field and check *Apply* enabled. The secret key should be the same as the one you configured in step 1-4.Input a preferred RADIUS server name into *RADIUS Server Name* field.

D-Link Building Networks for People	D-Li K Power O Coscole O RPS DWS-4024 Coscole Coscole 2	3         5         7         9         11         13         15         17         13         21         23         Combot Combot           4         6         8         10         12         14         16         18         20         22         24         Combot Combot
	Tool	
3 DWS-4024	Configuration Named Server Status	
Administration	DADILLO Authoritica Construction	
r L2 Features	RADIOS Authentication Server Computation	
L3 Features	RADIUS Server Host Address	10 90 90 100 💌
QoS	Port	10:00:00:100
Access Control Lists		1812 (1 to 65535)
Security	Secret	( Apply )
Port Security Administ	Primary Server	No 🗸
Port Security Interface	Message Authenticator	Enable 🗸
Port Security Static	Secret Configured	No
SSL Configuration	Current	Yes
SSH Configuration	RADIUS Server Name	
		UDefault-RADIUS-Server
PADIUS Authentica		IDMIT Remove Refresh
RADIUS Accounting		

2-3. Confirm if the RADIUS Authentication Server Name in WLAN Global settings is the same as that you configured in step 2-2.



2-3. Confirm if the RADIUS Authentication Server Name in WLAN SSID settings is the same as that you configured in step 2-2.

Global Discovery Profile Radio SSID	Valid AP OUI
Wireless Network Configuration	
- COLD	
SSID	dlinkradius
Hide SSID	
VIAN	
13 Tunnel	(1 to 4094)
L3 Tunnel Status	None
L3 Tunnel Subnet	0.0.0
L3 Tunnel Mask	255 255 255 0
MAC Authentication	O Local O RADIUS @ Disable
Redirect	None ○ HTTP     None ○ HTTP
Redirect URL	
Wireless ARP Suppression Mode	Disable 💌
L2 Distributed Tunneling Mode	Disable 🛩
CRADUIC Authoritization Commonlying	
RADIUS Authentication Server Name	Default-RADIUS-Server
PADIUS Accounting Source Name	Configured
DADIUS Accounting Server Name	Default-RADIUS-Server
RADIUS Accounting Server status	Not Contigured
RADIUS Accounting	
	-
Security	ONone OWEP ⊙WPA/WPA2
MIDA Marsiana	O WPA Personal  O WPA Enterprise
WPA Versions WPA Cinhers	
Pre-Authentication	MIKP MCCMP(AES)
Pre-Authentication Limit	(0 to 102)
Key Caching Hold Time	(1 to 1440)
Bcast Key Refresh Rate	1 (1 to 1440)
Session Key Refresh Rate	0 to 86400
	j* [(v to obtoo)
Client QoS	
Client QoS Bandwidth Limit Down (bits-per-secon	d) 0 (0 to 4294967295, 0 - Disable)
Client QoS Bandwidth Limit Up (bits-per-second)	0 (0 to 4294967295, 0 - Disable)
Client QoS Access Control Down	<none> 💌</none>
Client QoS Access Control Up	<none> 💌</none>
Client QoS Diffserv Policy Down	<none> 🛩</none>
Client QoS Diffserv Policy Up	<none> M</none>

## Wireless Client Settings:

3-1. Change the Network Authentication to WPA2.

Association Authentication C	onnection	
Network name (SSID):	linkradius	
Connect even if this netw	vork is not broadcasti	ng
Wireless network key		1.63.53.63
This network requires a key f	or the following:	
Network Authentication:	WPA2	~
Data encryption:	AES	~
Network key:		
Confirm network key:		
Key index (advanced)		
The key is provided for m	e automatically	
This is a computer-to-computer	uter (ad hoc) network	; wireless

3-2. In the "Authentication" tab, select "Protected EAP (PEAP)" as the EAP type.

Association Authe Select this option wireless Ethemet r Enable IEEE 8 EAP type: Prote	entication to provide networks 02.1 x auth	Connection authenticated network access for hentication for this network
Select this option wireless Ethernet r	to provide networks 02,1x aut/	authenticated network access for nentication for this network
Enable IEEE 8	02,1x aut	nentication for this network
EAP type: Prote		
	cted EAP	(PEAP)
V Authenticate a	s compute	Properties
Authenticate a unavailable	s guest wl	hen user or computer information is

Click "Properties".

3-3. Check disabled "Validate server certificate".

Protec	ted EAP Properties	?	×
When	connecting:		
V	alidate server certificate		-ji
	Connect to these servers:	- 1	
Tro	sted Root Certification Authorities:		
	AddTrust External CA Root		
	C&W HKT SecureNet CA Root		
	CA I   Certinoste Classe A Personne		
	Certiposte Serveur		
	Certisign - Autoridade Certificadora - AC2		
	Certisign - Autoridade Certificadora - AC4		
	Do not prompt user to authorize new servers or trusted certification authorities.		
Select	Authentication Method:		
Secur	red password (EAP-MSCHAP v2)	Jre	
En	able Fast Reconnect		
En	able Quarantine checks		
Dis	connect if server does not present cryptobinding TLV		
	OK Car	icel	

Click "Configure".

3-4. Check disabled "Automatically use my Windows logon name and password (and domain if any)."

AP MSCI	1APv2 Prope	rties	
When co	nnecting:		
D Auto pas	matically use m word (and dom	y Windows lı ain if any).	ogon name and

Save the settings and try to connect the SSID you setup.

Input username and password which are setup in the server.

Then you can connect successfully.