

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

Topology:

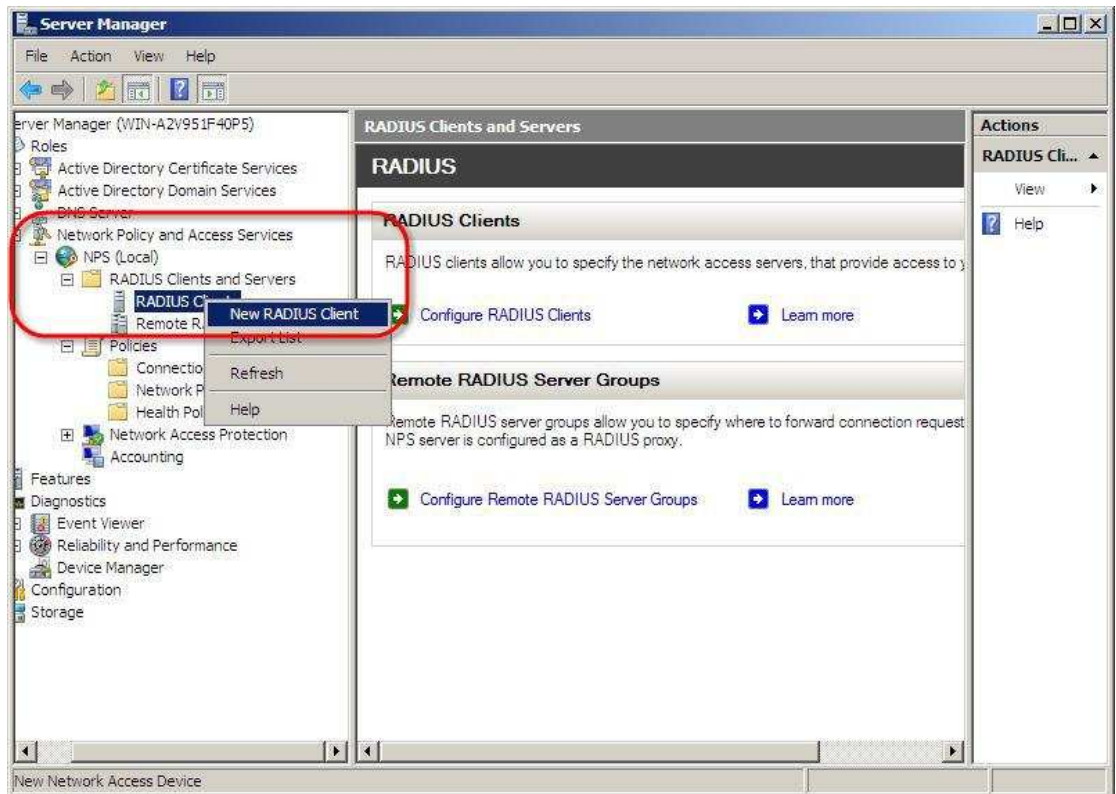
Windows Server 2008 (RADIUS Server) ----- DWS-4026

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



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

New RADIUS Client

Enable this RADIUS client

Name and Address

Friendly name:
Wireless Switch

Address (IP or DNS):
10.90.90.90

Verify...

Vendor

Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

Vendor name:
RADIUS Standard

Shared Secret

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

Manual Generate

Shared secret:
[Empty text box]

Confirm shared secret:
[Empty text box]

Additional Options

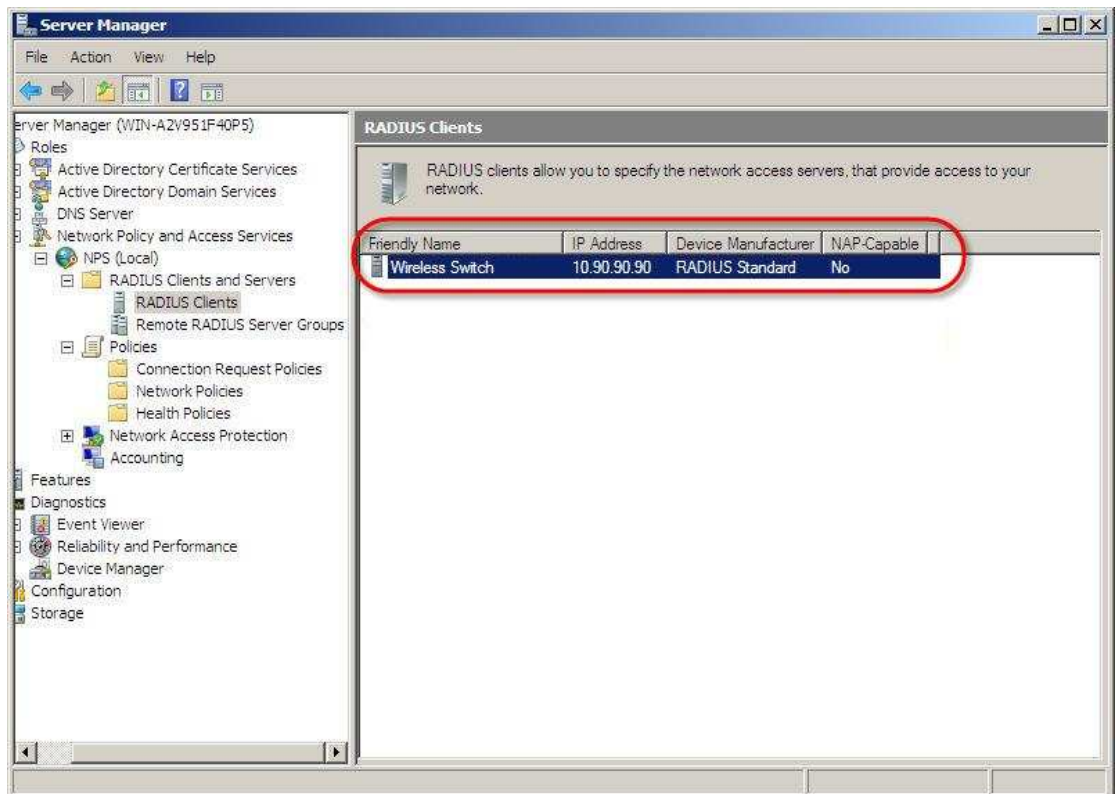
Access-Request messages must contain the Message-Authenticator attribute

RADIUS client is NAP-capable

OK Cancel

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

Double click the item to configure it.



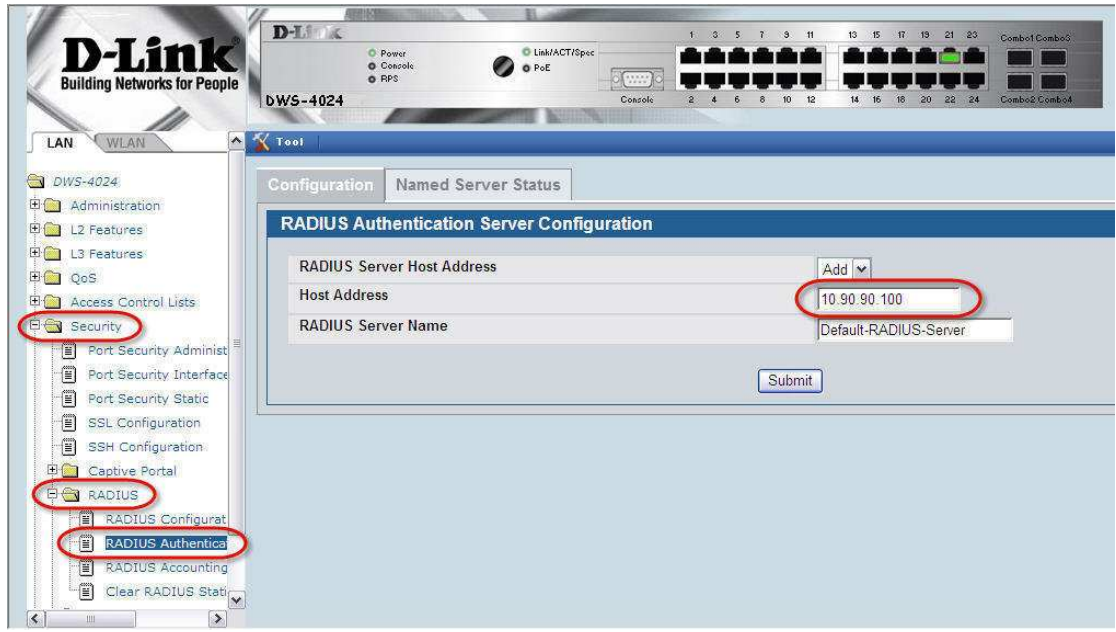
1-4. Enter the RADIUS secret into the *Shared secret* fields.

The image shows a Windows-style dialog box titled "Wireless Switch Properties" with a "Settings" tab. The "Enable this RADIUS client" checkbox is checked. The "Friendly name" field contains "Wireless Switch". The "Address (IP or DNS)" field contains "10.90.90.90" and has a "Verify..." button to its right. Below this, a dropdown menu for "Vendor name" is set to "RADIUS Standard". A text block explains that users can manually type or generate a shared secret. Two radio buttons, "Manual" (selected) and "Generate", are present. The "Shared secret" and "Confirm shared secret" fields are both filled with ten dots and are circled in red. At the bottom, there are "OK", "Cancel", and "Apply" buttons. Two checkboxes at the bottom are unchecked: "Access-Request messages must contain the Message-Authenticator attribute" and "RADIUS client is NAP-capable".

DWS-4000 Settings:

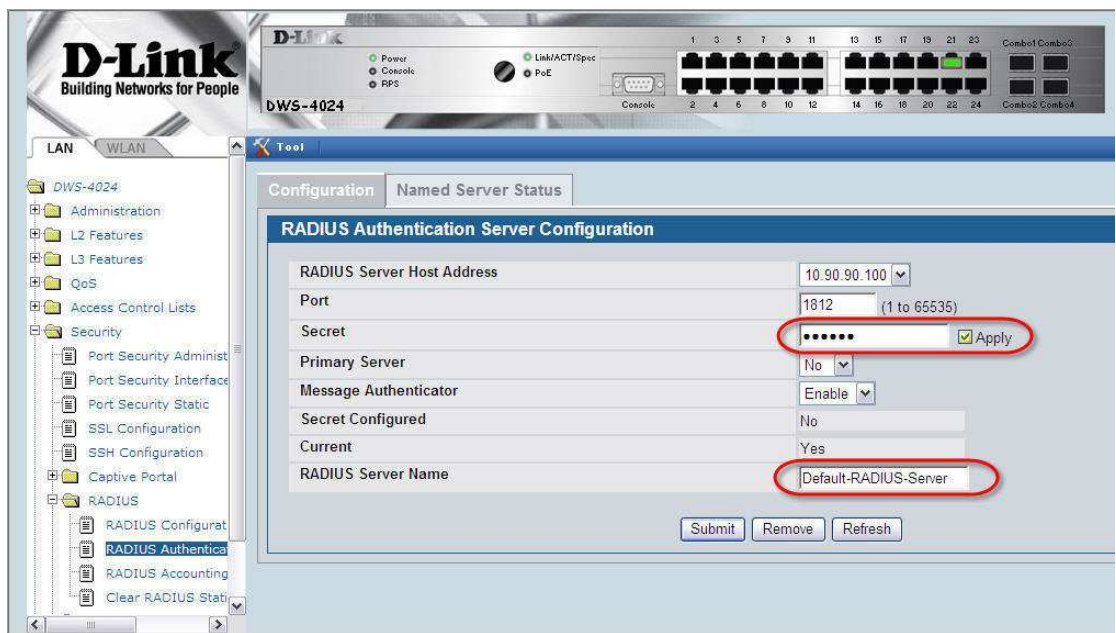
2-1. Configure the RADIUS server.

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



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.



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

The screenshot displays the D-Link web management interface for a DWS-4024 device. The left sidebar shows a navigation tree with 'WLAN' selected and 'Basic Setup' highlighted. The main content area is titled 'Wireless Global Configuration' and includes the following settings:

Setting	Value
Enable WLAN Switch	<input checked="" type="checkbox"/>
WLAN Switch Operational Status	Enabled
IP Address	10.90.90.90
AP Validation	
AP MAC Validation	<input checked="" type="radio"/> Local <input type="radio"/> RADIUS
Require Authentication Passphrase	<input type="checkbox"/>
RADIUS Server Configuration	
RADIUS Authentication Server Name	Default-RADIUS-Server
RADIUS Authentication Server Status	Configured
RADIUS Accounting Server Name	Default-RADIUS-Server
RADIUS Accounting Server Status	Not Configured
RADIUS Accounting	<input type="checkbox"/>
Country Code	US - United States

Buttons at the bottom of the configuration page include 'Refresh', 'Submit', and 'Next'.

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

The screenshot displays the D-Link DWS-4024 web interface, specifically the 'WLAN SSID' configuration page. The interface is divided into several sections, with the 'Wireless Network Configuration' section being the primary focus. The 'RADIUS Authentication Server Name' field is highlighted with a red circle and contains the value 'Default-RADIUS-Server'. The 'Security' section is also highlighted with a red circle, showing the following settings:

- Security: None WEP WPA/WPA2
- WPA Versions: WPA WPA2
- WPA Ciphers: TKIP CCMP(AES)

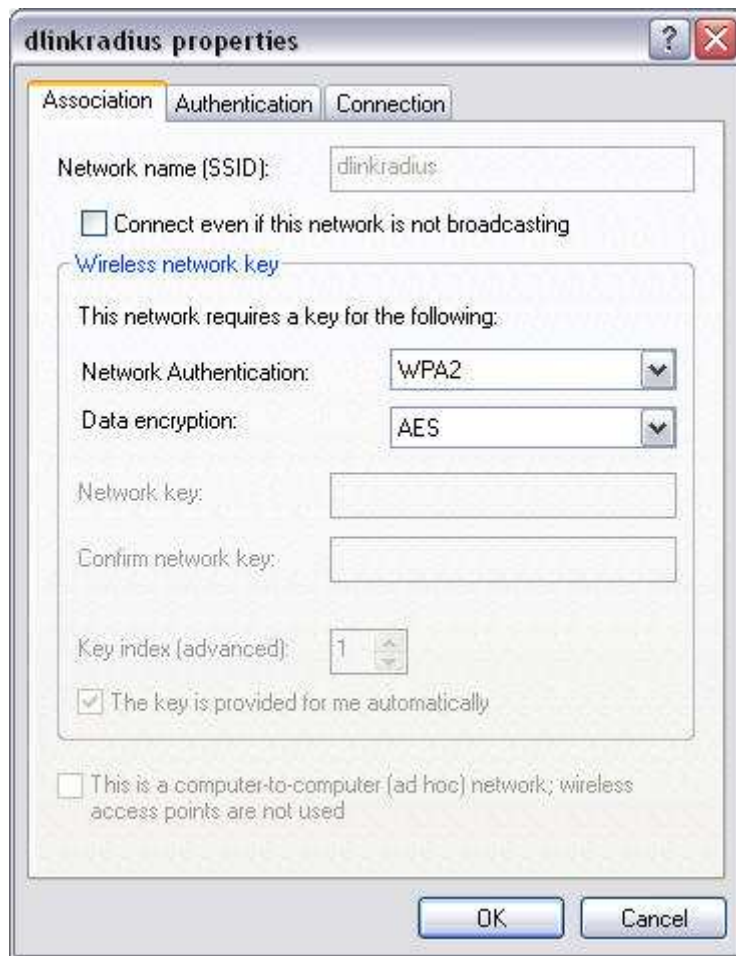
Other visible settings in the 'Wireless Network Configuration' section include:

- SSID: dlinkradius
- Hide SSID:
- Ignore Broadcast:
- VLAN: 1 (1 to 4094)
- L3 Tunnel:
- L3 Tunnel Status: None
- L3 Tunnel Subnet: 0.0.0.0
- L3 Tunnel Mask: 255.255.255.0
- MAC Authentication: Local RADIUS Disable
- Redirect: None HTTP
- Redirect URL:
- Wireless ARP Suppression Mode: Disable
- L2 Distributed Tunneling Mode: Disable
- RADIUS Authentication Server Status: Configured
- RADIUS Accounting Server Name: Default-RADIUS-Server
- RADIUS Accounting Server Status: Not Configured
- RADIUS Use Network Configuration: Enable
- RADIUS Accounting:

At the bottom of the configuration page, there are buttons for 'Submit', 'Refresh', and 'Clear'.

Wireless Client Settings:

3-1. Change the Network Authentication to WPA2.



The image shows a Windows-style dialog box titled "dlinkradius properties". It has three tabs: "Association", "Authentication", and "Connection". The "Authentication" tab is selected. The dialog contains the following fields and options:

- Network name (SSID): dlinkradius
- Connect even if this network is not broadcasting
- Wireless network key
- This network requires a key for the following:
- Network Authentication: WPA2 (dropdown menu)
- Data encryption: AES (dropdown menu)
- Network key: [empty text box]
- Confirm network key: [empty text box]
- Key index (advanced): 1 (spin box)
- The key is provided for me automatically
- This is a computer-to-computer (ad hoc) network; wireless access points are not used

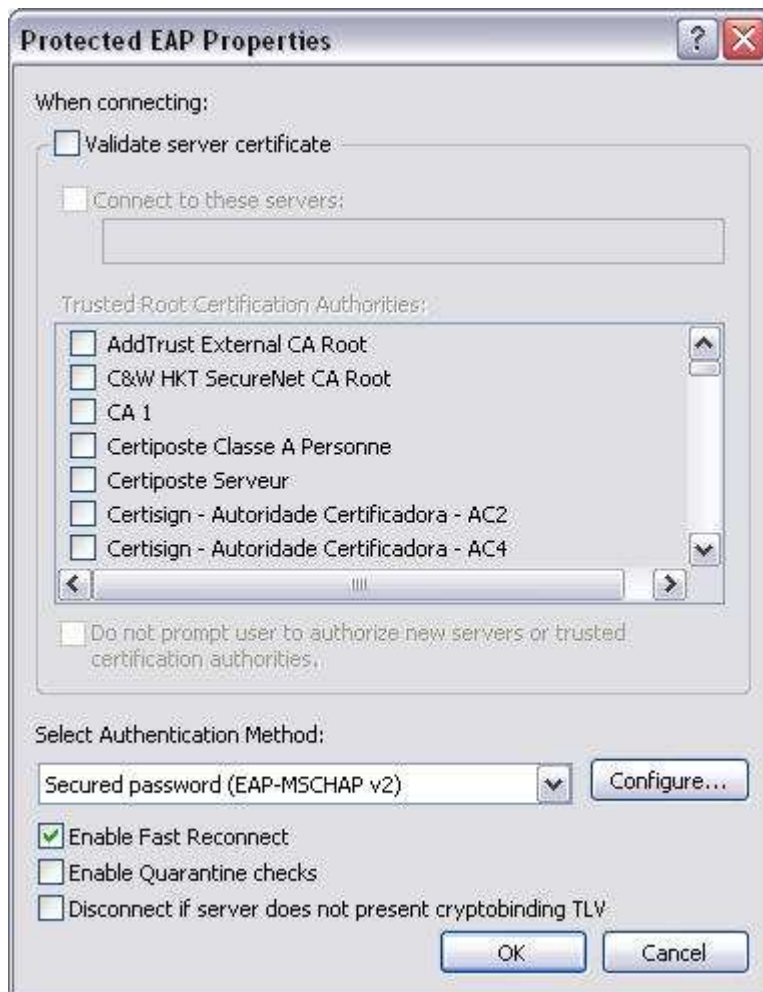
At the bottom of the dialog are "OK" and "Cancel" buttons.

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



Click “Properties”.

3-3. Check disabled “Validate server certificate”.



Click “Configure”.

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



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.