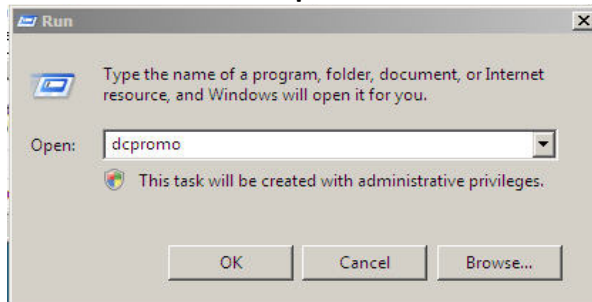


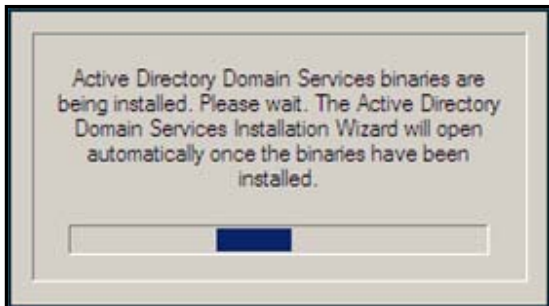
How To Use Microsoft 2008 Server With D-Link DFL-Series Firewall User Authentication Groups

- Create a DOMAIN NAME in this 2008 server, or you can use current DOMAIN. How to create a DOMAIN in the 2008 server:

A. Go to **Start > Run > “dcpromo”** command.



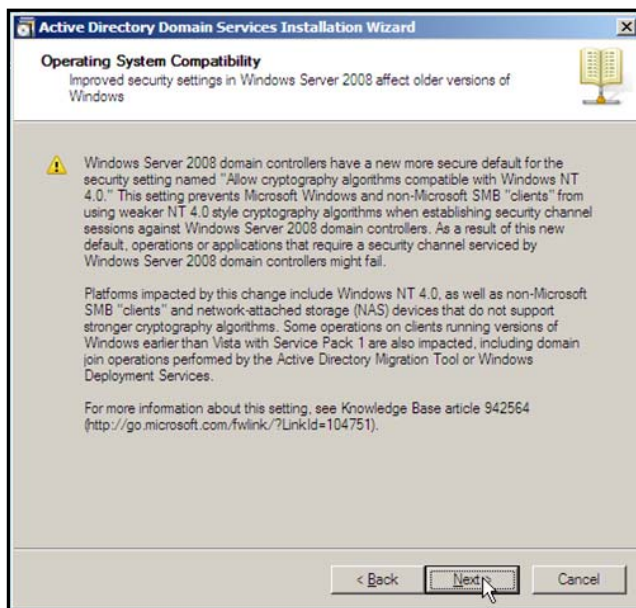
B.



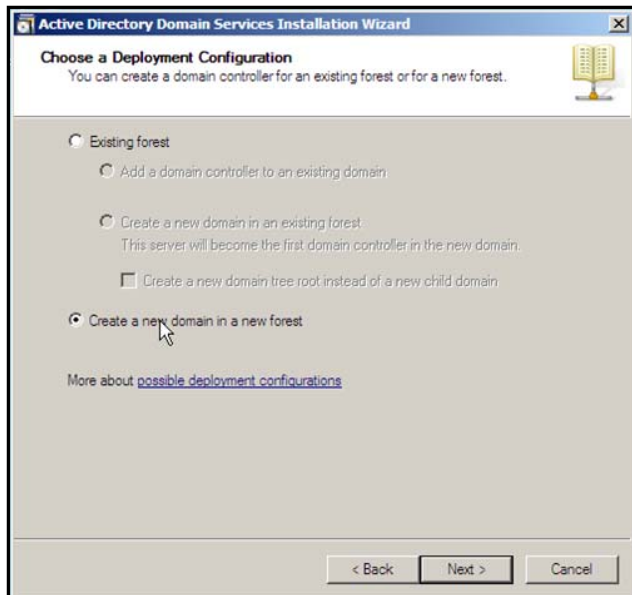
C.



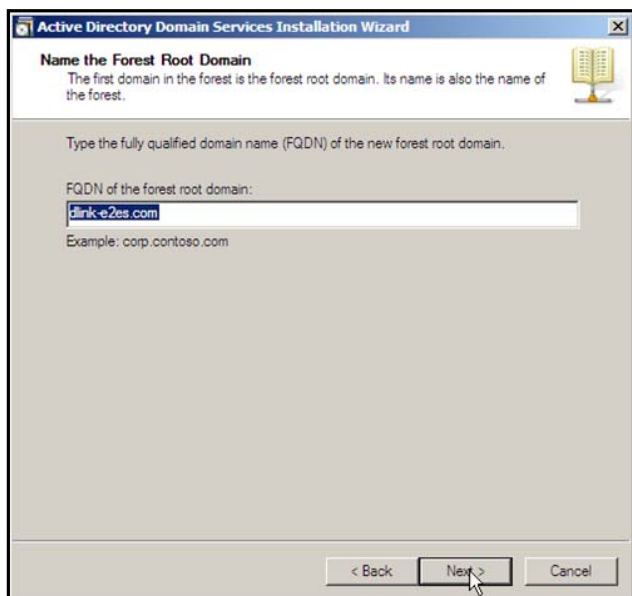
D.



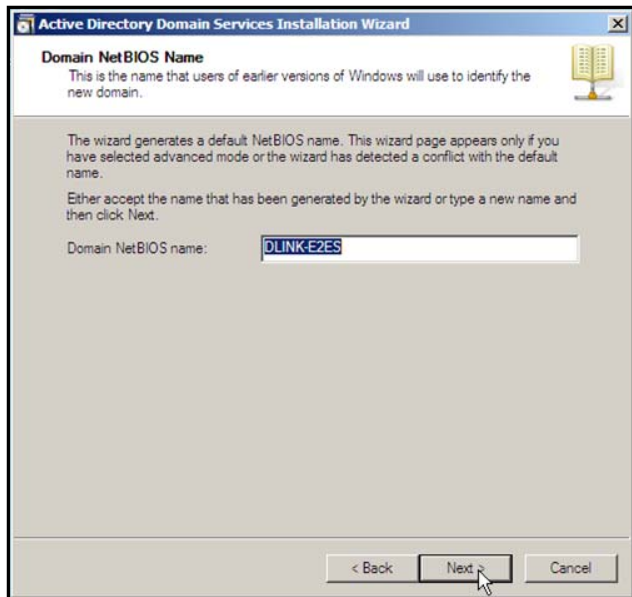
E.



F.



G.



Active Directory Domain Services Installation Wizard

Domain NetBIOS Name
This is the name that users of earlier versions of Windows will use to identify the new domain.

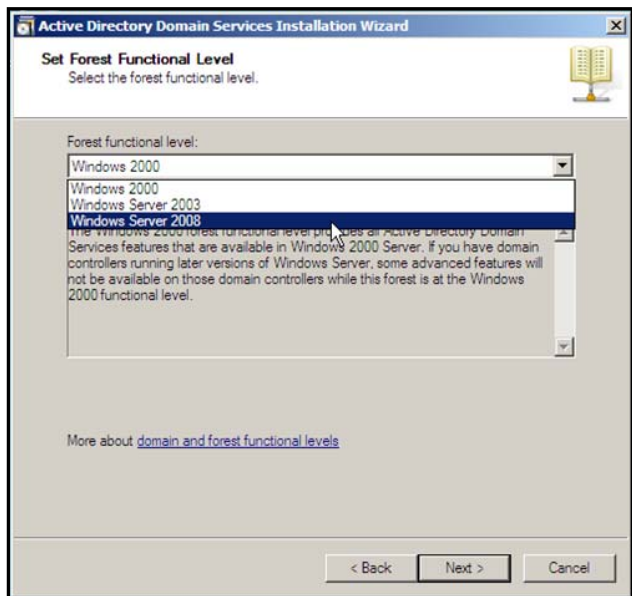
The wizard generates a default NetBIOS name. This wizard page appears only if you have selected advanced mode or the wizard has detected a conflict with the default name.

Either accept the name that has been generated by the wizard or type a new name and then click Next.

Domain NetBIOS name:

< Back Next > Cancel

H.



Active Directory Domain Services Installation Wizard

Set Forest Functional Level
Select the forest functional level.

Forest functional level:

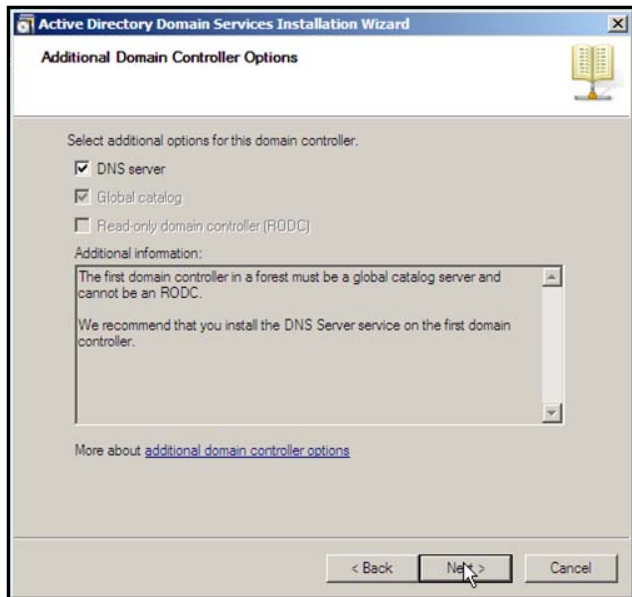
Windows 2000
Windows Server 2003
Windows Server 2008

Which forest functional level you select determines which Active Directory Domain Services features that are available in Windows 2000 Server. If you have domain controllers running later versions of Windows Server, some advanced features will not be available on those domain controllers while this forest is at the Windows 2000 functional level.

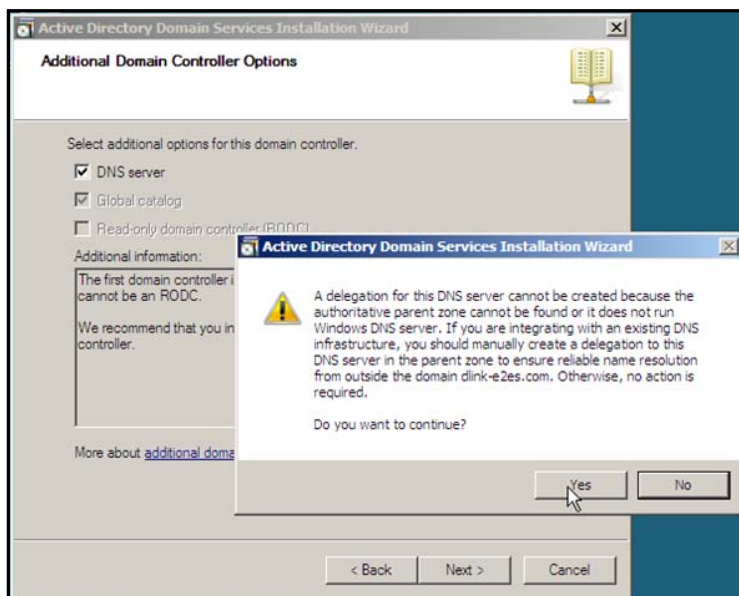
[More about domain and forest functional levels](#)

< Back Next > Cancel

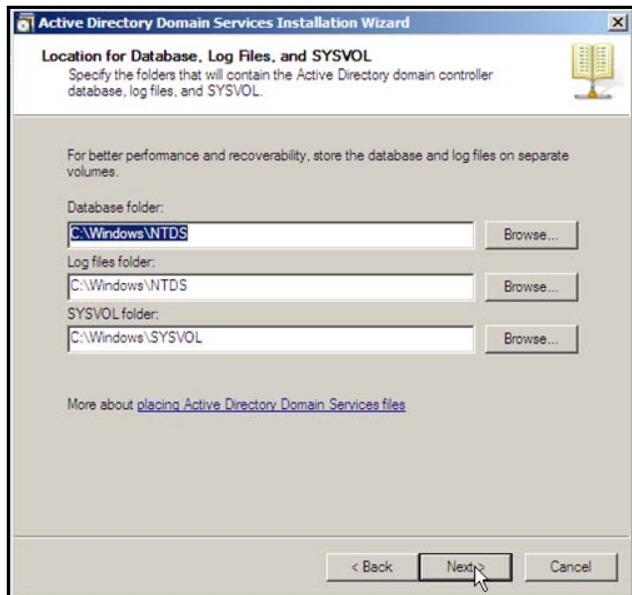
I.



J.



K.



Active Directory Domain Services Installation Wizard

Location for Database, Log Files, and SYSVOL

Specify the folders that will contain the Active Directory domain controller database, log files, and SYSVOL.

For better performance and recoverability, store the database and log files on separate volumes.

Database folder:

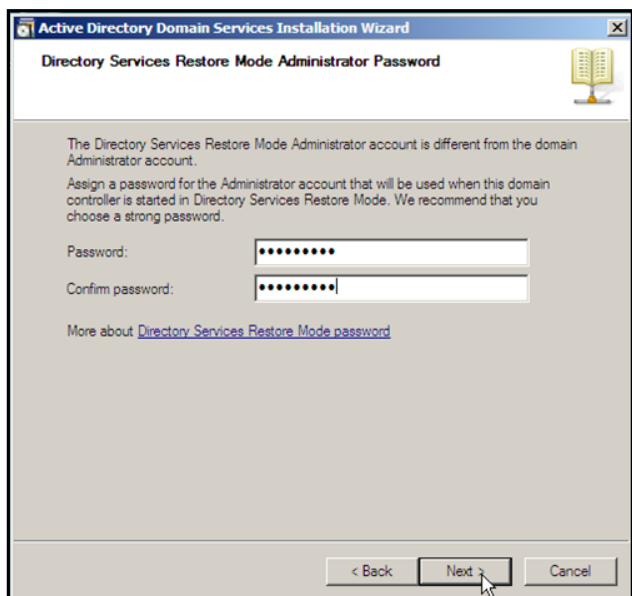
Log files folder:

SYSVOL folder:

[More about placing Active Directory Domain Services files](#)

< Back **Next >** Cancel

L.



Active Directory Domain Services Installation Wizard

Directory Services Restore Mode Administrator Password

The Directory Services Restore Mode Administrator account is different from the domain Administrator account.

Assign a password for the Administrator account that will be used when this domain controller is started in Directory Services Restore Mode. We recommend that you choose a strong password.

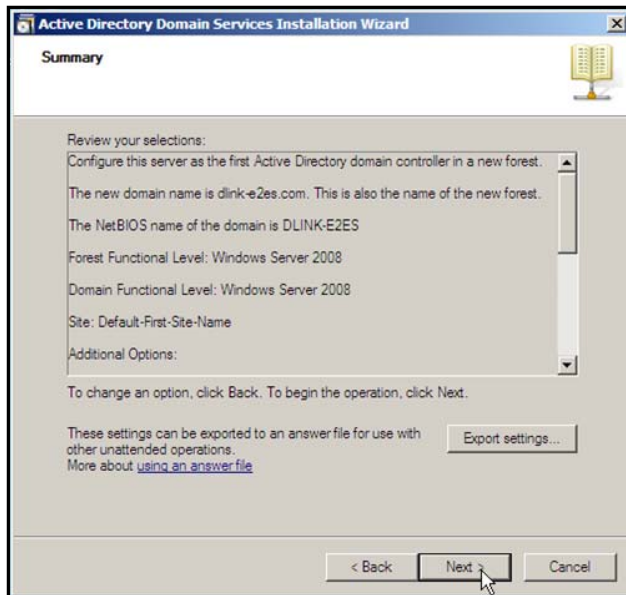
Password:

Confirm password:

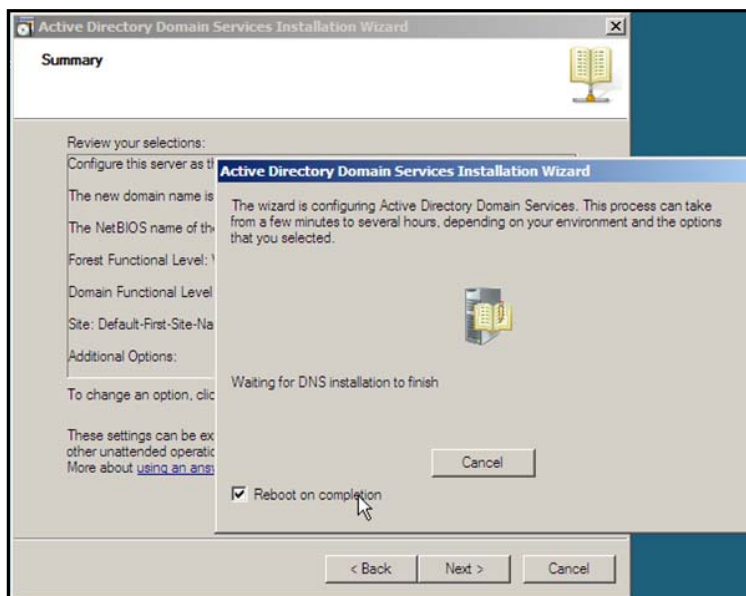
[More about Directory Services Restore Mode password](#)

< Back **Next >** Cancel

M.



N.

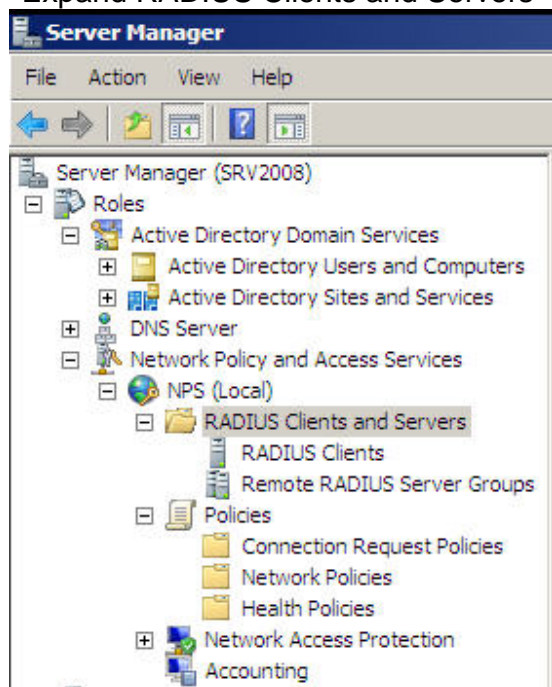


- Install NPS, please follow below instructions:

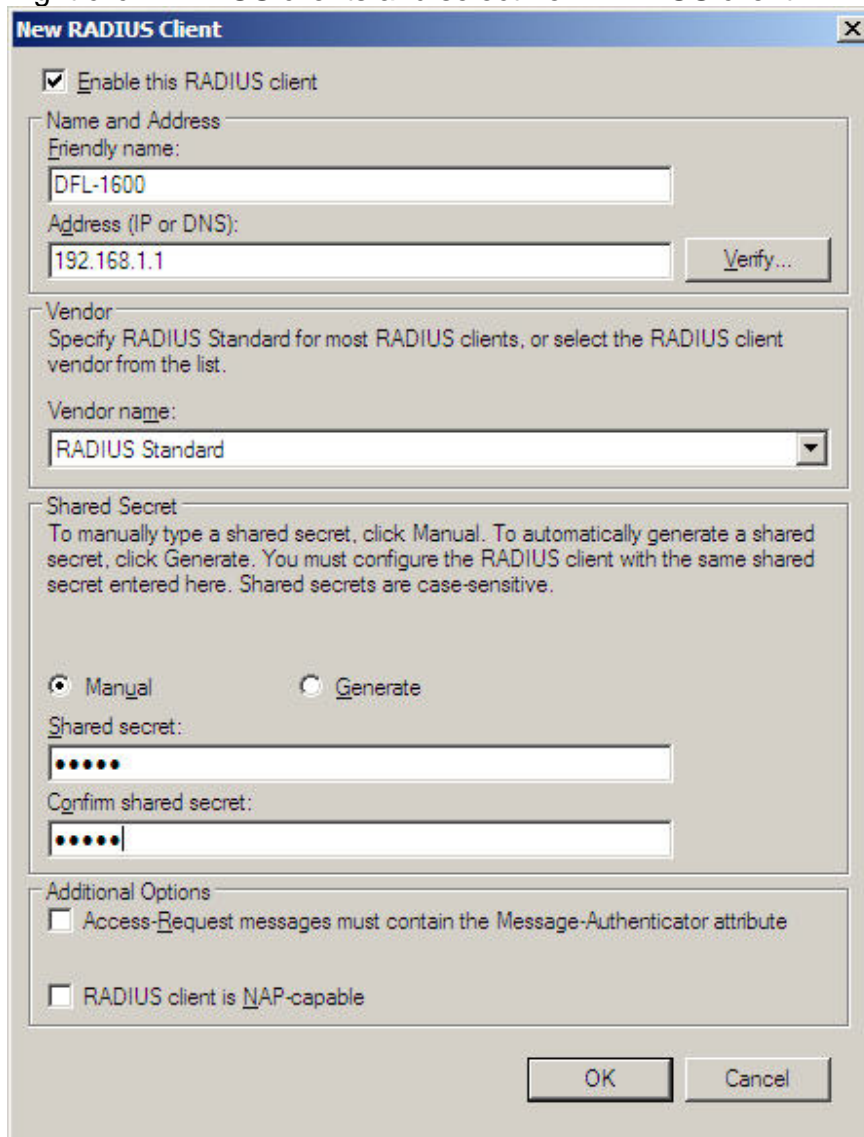
- A. Click start > Server Manager
- B. Select roles from the left hand panel
- C. Select Add Roles
- D. Click next on the welcome screen
- E. Tick the box labelled "Network Policy and Access Services" then click next
- F. Read the summary and click next
- G. Tick the box labelled "Network Policy Server" then click next
- H. Review the installation summary then click install.
- I. A progress bar will display the progress of the installation; once the progress reaches 100% NPS is installed and running, click close to exit the wizard. NPS can be accessed via Start > Administrative tools > Network Policy Server

- Configure NPS

- A. Click Start > Administrative tools > Network Policy Server to launch NPS
- B. Right click on NPS (local) and select "Register Server in Active Directory" and acknowledge the messages
- C. Expand RADIUS Clients and Servers



D. Right click RADIUS clients and select new RADIUS client.

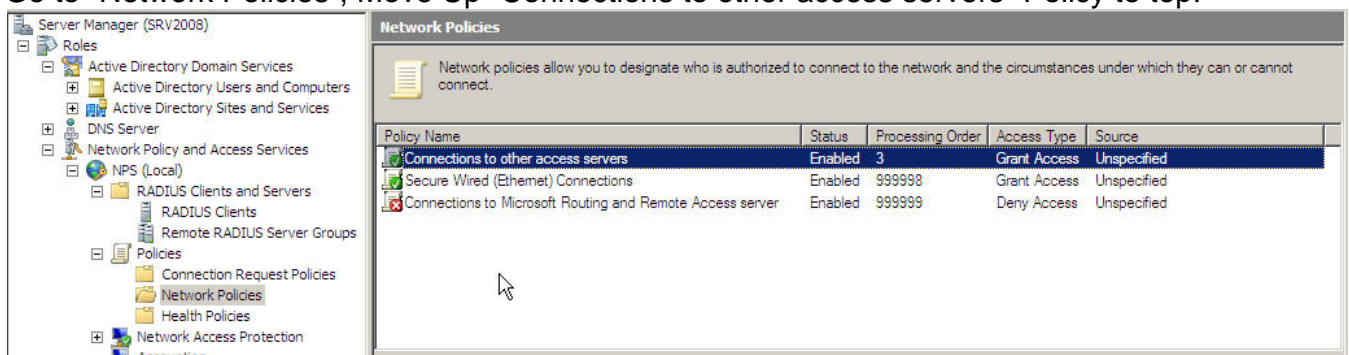


The "New RADIUS Client" dialog box is shown. It has a title bar with a close button. The main area is divided into several sections:

- Enable this RADIUS client:** A checkbox that is checked.
- Name and Address:** A section with two text boxes: "Friendly name:" containing "DFL-1600" and "Address (IP or DNS):" containing "192.168.1.1". There is a "Verify..." button to the right of the address box.
- Vendor:** A section with a description: "Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list." Below it is a "Vendor name:" label and a dropdown menu showing "RADIUS Standard".
- Shared Secret:** A section with a description: "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." Below this are two radio buttons: "Manual" (selected) and "Generate". Under "Manual" are two text boxes: "Shared secret:" and "Confirm shared secret:", both containing masked characters (dots).
- Additional Options:** A section with two checkboxes: "Access-Request messages must contain the Message-Authenticator attribute" (unchecked) and "RADIUS client is NAP-capable" (unchecked).

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

E. Go to "Network Policies", Move Up "Connections to other access servers" Policy to top.



The screenshot shows the "Server Manager (SRV2008)" console on the left and the "Network Policies" console on the right.

Server Manager (SRV2008) Tree View:

- Roles
 - Active Directory Domain Services
 - Active Directory Users and Computers
 - Active Directory Sites and Services
- DNS Server
- Network Policy and Access Services
 - NPS (Local)
 - RADIUS Clients and Servers
 - RADIUS Clients
 - Remote RADIUS Server Groups
 - Policies
 - Connection Request Policies
 - Network Policies
 - Health Policies
 - Network Access Protection
 - Accounting

Network Policies Console:

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
Connections to other access servers	Enabled	3	Grant Access	Unspecified
Secure Wired (Ethernet) Connections	Enabled	999998	Grant Access	Unspecified
Connections to Microsoft Routing and Remote Access server	Enabled	999999	Deny Access	Unspecified

F. Double click "Connections to other access servers" Policy and setup this policy.

The screenshot shows the 'Connections to other access servers Properties' dialog box with the 'Overview' tab selected. The 'Policy name' field contains 'Connections to other access servers'. The 'Policy State' section has the 'Policy enabled' checkbox checked. The 'Access Permission' section has the 'Grant access' radio button selected. The 'Network connection method' section has the 'Type of network access server' radio button selected, with a dropdown menu showing 'Unspecified'. The 'Vendor specific' radio button is unselected, and its associated text box contains '10'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Connections to other access servers Properties

Overview | Conditions | Constraints | Settings

Policy name: Connections to other access servers

Policy State
If enabled, NPS evaluates this policy while performing authorization. If disabled, NPS does not evaluate this policy.

☒ Policy enabled

Access Permission
If conditions and constraints of the network policy match the connection request, the policy can either grant access or deny access. [What is access permission?](#)

☒ Grant access. Grant access if the connection request matches this policy.
☐ Deny access. Deny access if the connection request matches this policy.
☐ Ignore user account dial-in properties.
If the connection request matches the conditions and constraints of this network policy and the policy grants access, perform authorization with network policy only; do not evaluate the dial-in properties of user accounts.

Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific.

☒ Type of network access server:
Unspecified

☐ Vendor specific:
10

OK Cancel Apply

The screenshot shows the 'Connections to other access servers Properties' dialog box with the 'Constraints' tab selected. The 'Constraints' list on the left includes 'Authentication Methods', 'Idle Timeout', 'Session Timeout', 'Called Station ID', 'Day and time restrictions', and 'NAS Port Type'. The 'Authentication Methods' constraint is selected, showing a list of EAP types: 'EAP Types:'. Below this list are 'Move Up' and 'Move Down' buttons. At the bottom of the list are 'Add...', 'Edit...', and 'Remove' buttons. The 'Less secure authentication methods' section has the following options: 'Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)' (unchecked), 'User can change password after it has expired' (unchecked), 'Microsoft Encrypted Authentication (MS-CHAP)' (unchecked), 'User can change password after it has expired' (unchecked), 'Encrypted authentication (CHAP)' (checked), 'Unencrypted authentication (PAP, SPAP)' (checked), 'Allow clients to connect without negotiating an authentication method' (unchecked), and 'Perform machine health check only' (unchecked). At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Connections to other access servers Properties

Overview | Conditions | Constraints | Settings

Configure the constraints for this network policy.
If all constraints are not matched by the connection request, network access is denied.

Constraints:

Constraints

- Authentication Methods
- Idle Timeout
- Session Timeout
- Called Station ID
- Day and time restrictions
- NAS Port Type

Authentication Methods

Allow access only to those clients that authenticate with the specified methods.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

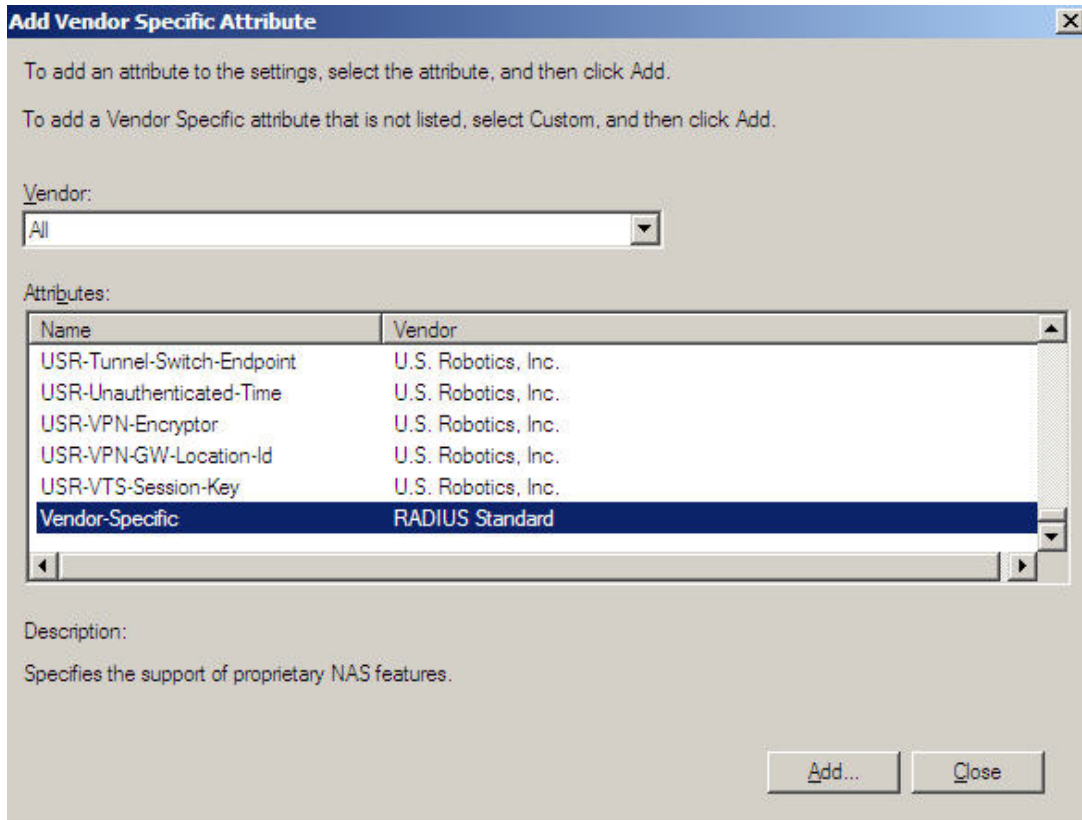
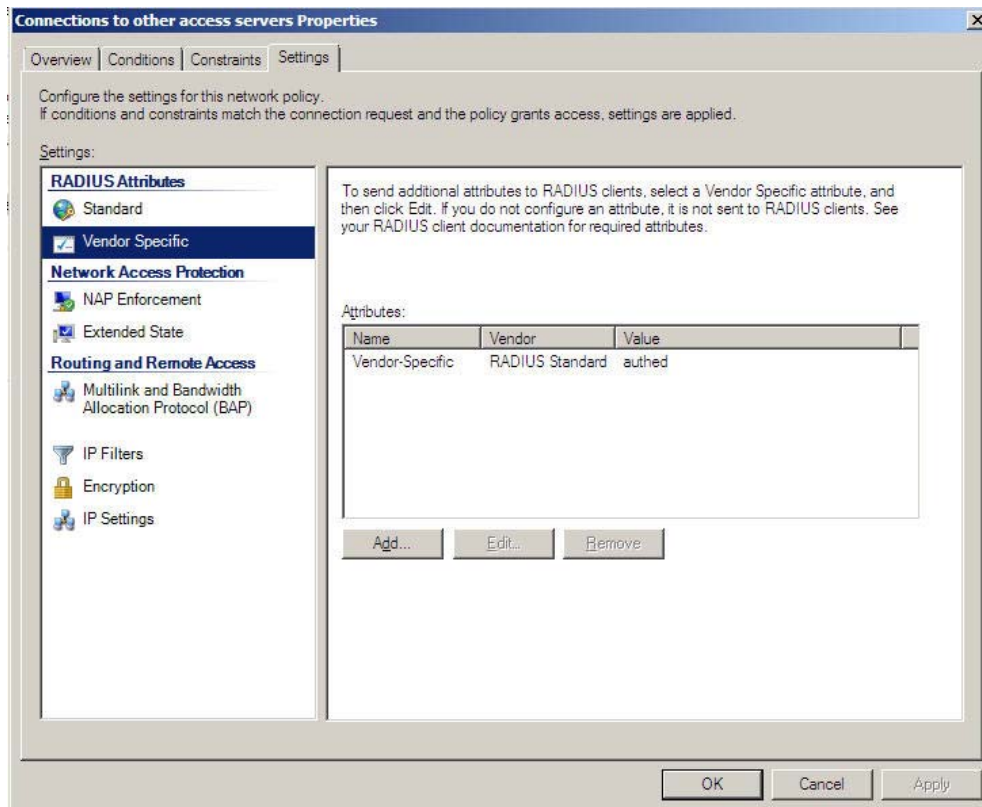
Move Up
Move Down

Add... Edit... Remove

Less secure authentication methods:

- ☐ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
☐ User can change password after it has expired
- ☐ Microsoft Encrypted Authentication (MS-CHAP)
☐ User can change password after it has expired
- ☒ Encrypted authentication (CHAP)
- ☒ Unencrypted authentication (PAP, SPAP)
- ☐ Allow clients to connect without negotiating an authentication method
- ☐ Perform machine health check only

OK Cancel Apply



Attribute Information [X]

Attribute name:
Vendor-Specific

Attribute number:
26

Attribute format:
OctetString

Attribute values:

Vendor	Value
Vendor Code: 5089	authed

[Add...]
[Edit...]
[Remove]
[Move Up]
[Move Down]

[OK] [Cancel]

Vendor-Specific Attribute Information [X]

Attribute name:
Vendor Specific

Specify network access server vendor.

☐ Select from list: [RADIUS Standard]

☒ Enter Vendor Code: [5089]

Specify whether the attribute conforms to the RADIUS RFC specification for vendor specific attributes.

☒ Yes. It conforms
☐ No. It does not conform

[Configure Attribute...]

[OK] [Cancel]

Configure VSA (RFC Compliant)

Vendor-assigned attribute number:
1

Attribute format:
String

Attribute value:
authenticated

OK Cancel

Connections to other access servers Properties

Overview Conditions Constraints Settings

Configure the settings for this network policy.
If conditions and constraints match the connection request and the policy grants access, settings are applied.

Settings:

RADIUS Attributes

- Standard
- Vendor Specific**

Network Access Protection

- NAP Enforcement
- Extended State

Routing and Remote Access

- Multilink and Bandwidth Allocation Protocol (BAP)
- IP Filters
- Encryption
- IP Settings

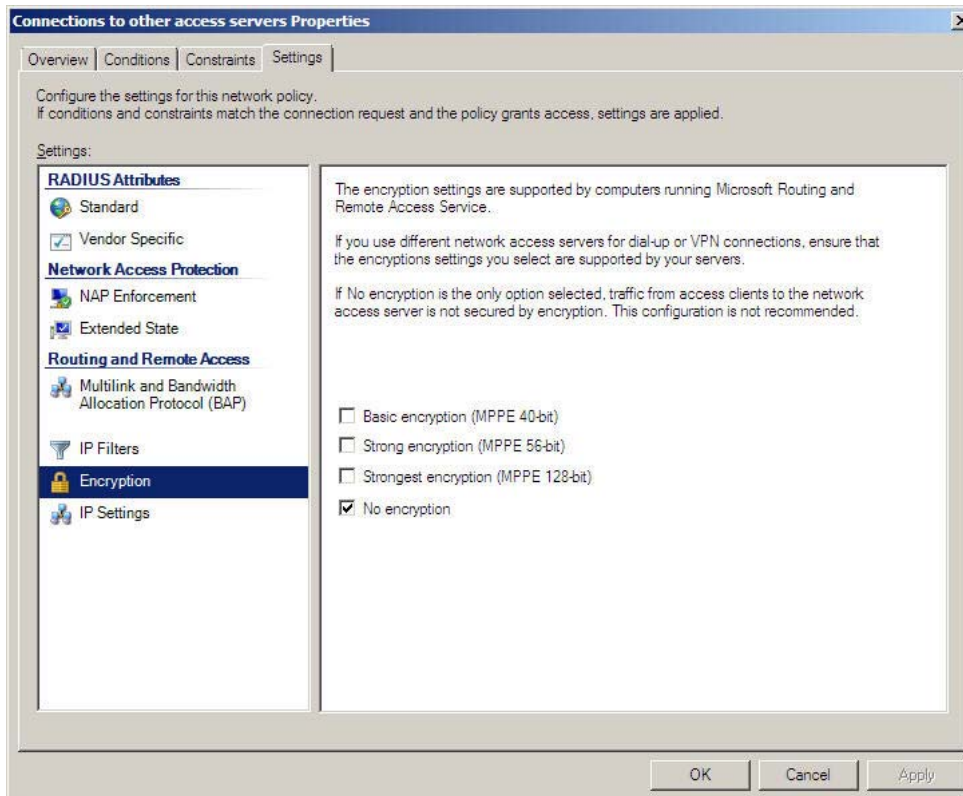
To send additional attributes to RADIUS clients, select a Vendor Specific attribute, and then click Edit. If you do not configure an attribute, it is not sent to RADIUS clients. See your RADIUS client documentation for required attributes.

Attributes:

Name	Vendor	Value
Vendor-Specific	RADIUS Standard	authenticated

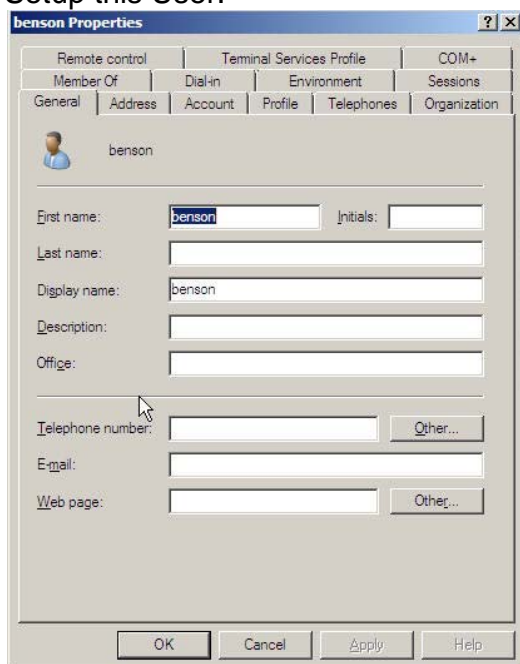
Add... Edit... Remove...

OK Cancel Apply



G. Go to Active Directory Domain Services > Active Directory Users and Computers > Users, right click “Users” and select New > User

H. Setup this User:



benson Properties [?] [X]

Remote control	Terminal Services Profile		COM+
Member Of	Dial-in	Environment	Sessions
General	Address	Account	Profile
		Telephones	Organization

User logon name: @dlink.com

User logon name (pre-Windows 2000):

☐ Unlock account

Account options:

- ☐ User must change password at next logon
- ☐ User cannot change password
- ☒ Password never expires
- ☐ Store password using reversible encryption

Account expires:

☒ Never

☐ End of:

benson Properties [?] [X]

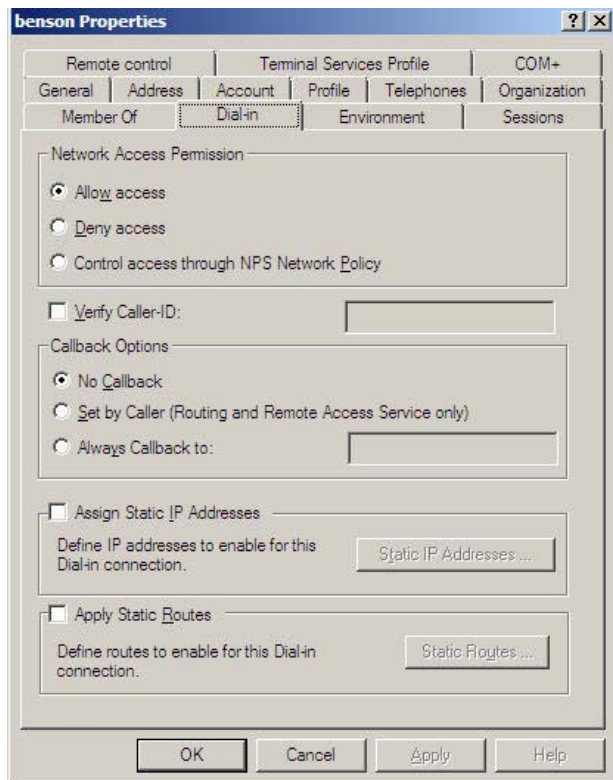
Remote control	Terminal Services Profile		COM+
General	Address	Account	Profile
Member Of	Dial-in	Environment	Sessions

Member of:

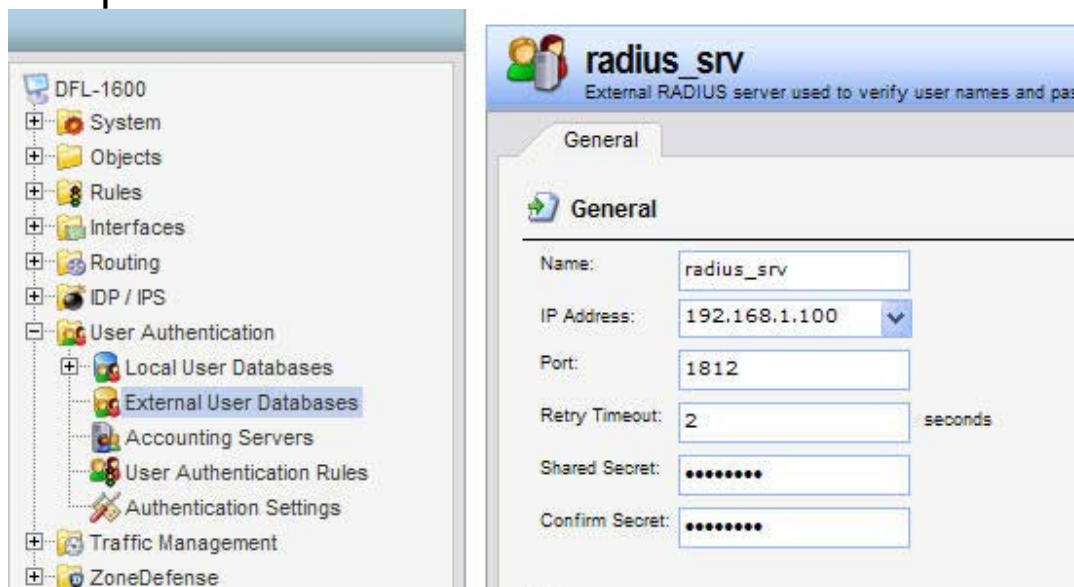
Name	Active Directory Domain Services Folder
Domain Users	dlink.com/Users
RAS and IAS Servers	dlink.com/Users

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.



● Setup DFL-Firewall RADIUS Server.



- Setup DFL Firewall User Authentication Rule.

The screenshot shows the DFL Firewall configuration interface. On the left is a tree view with the following items: DFL-1600, System, Objects, Rules, Interfaces, Routing, IDP / IPS, User Authentication (expanded), Local User Databases, External User Databases, Accounting Servers, User Authentication Rules (highlighted), Authentication Settings, Traffic Management, and ZoneDefense. The main panel is titled 'http_authed' with the subtitle 'The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.' It has tabs for General, Log Settings, Authentication Options, Accounting, Agent Options, and Restrictions. The 'General' tab is active, showing the following fields: Name (http_authed), Authentication agent (HTTP), Authentication Source (RADIUS), Interface (lan1), Originator IP (all-nets), and Terminator IP ((None)). A note states: 'For XAuth and PPP, this is the tunnel originator IP.' There is also a 'Comments' section at the bottom.

This screenshot shows the 'Authentication Options' tab of the 'http_authed' rule configuration. It includes the following sections:
1. A header instruction: 'Select one or more authentication servers. Also select the authentication method, which is used for encrypting the user password.'
2. 'RADIUS servers' section: An 'Available' list (empty) and a 'Selected' list containing 'radius_srv'. Between the lists are '>>' and '<<' buttons. Below the 'Selected' list are 'Move up' and 'Move down' buttons.
3. 'LDAP servers' section: An 'Available' list (empty) and a 'Selected' list (empty). Between the lists are '>>' and '<<' buttons. Below the 'Selected' list are 'Move up' and 'Move down' buttons.
4. At the bottom, there are two dropdown menus: 'RADIUS Method' set to 'Unencrypted password (PAP)' and 'Local User DB' set to '(None)'.

http_authed
The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

General Log Settings Authentication Options Accounting Agent Options Restrictions

General

Select one or more accounting servers. Also select the statistics for the authenticated user that should be sent to the accounting serv

Accounting servers

Available

Selected

radius_acc_srv

>>

<<

Move up Move down

User Statistics

☒ Bytes Sent ☒ Bytes Received

☒ Packets Sent ☒ Packets Received

☒ Enable reporting of the number of seconds the session lasted.

☒ Support Interim Accounting

☐ Server controlled value

Interim Value: 600 seconds The interval in seconds which the unit should send interim account

● Setup D-Link Firewall IP Rules

authed_rule
An IP Rule Folder can be used to group IP Rules into logical groups for better overview and simplified management.

Add Edit this object

#	Name	Action	Source interface	Source network	Destination interface	Destination network	Service
1	dns_allow	NAT	lan1	lan1net	pppoe	all-nets	dns-all
2	authed_allow	NAT	lan1	lan_authed	pppoe	all-nets	all_services
3	NO_authed_sat	SAT	lan1	lan1net	pppoe	all-nets	all_services
4	NO_authed_sat-allow	Allow	lan1	lan1net	pppoe	all-nets	all_services