1. Disable "password complexity requirements" from Group Policy Object Editor.



2. Create users





a. Create new user for MAC authentication. The logon name and client's MAC address has to be the same as each other.

New Object - User					×
Create in:	TSS2RADIU	S.com/Users			
<u>F</u> irst name:	DWA		Initials:		
Last name:	140				
Full n <u>a</u> me:	DWA 140				
<u>U</u> ser logon name:					
00-26-5a-07-9c-37		@TSS2RAI	DIUS.com	•	
User logon name (pre-	<u>W</u> indows 2000):			
TSS2RADIUS\		00-26-5a-07	-9c-37		
		< <u>B</u> ack	<u>N</u> ext >	C	ancel

b. The password has to be "NOPASSWORD"

New Object - User	×
Create in: TSS2RADIUS.com/Users	
Password: ••••••• Confirm password: •••••••	
 User must change password at next logon User cannot change password Password never expires Account is disabled 	
< <u>B</u> ack <u>N</u> ext>	Cancel

c. Create new user for WPA/WPA2-EAP. Just input username and password as what you want.

New Object - User		×
Create in: TSS2RADI	IUS.com/Users	
Eirst name: nolan	Initials:	
Last name: ouyang		
Full n <u>a</u> me: nolan ouyan	g	
<u>U</u> ser logon name: nolan	@TSS2RADIUS.com	
, User logon name (pre- <u>W</u> indows 200)0):	
TSS2RADIUS\	nolan	
	< <u>B</u> ack. <u>N</u> ext > Cancel	
New Object - User		×
Create in: TSS2RAD	IUS.com/Users	_
Password:	•••••	
Confirm password:	•••••	
User must change password at	next logon	
User cannot change password		
Password never expires		
I Account is disabled		
		_
	< <u>B</u> ack <u>N</u> ext > Cancel	

c. Enable **BOTH** accounts

RAS and : RAS and : Schema A SUPPORT TelnetClie	<u>C</u> opy Add to a group Di <u>s</u> able Account R <u>e</u> set Password	Right Click Servers in this group Designated administr his is a vendor's acc Members of this grou
ction.	Open Home Page Send Mail	
	Cu <u>t</u> Delete Rena <u>m</u> e	
	- Toborcion	
	<u>H</u> elp	

nolan ouyang Properties
Remote control Terminal Services Profile COM+ General Address Account Profile Telephones Organization Member Of Dial-in Environment Sessions
Remote Access Permission (Dial-in or VPN) Allow access Deny access
Control access through Hemote Access Policy Verify Caller-ID: Callback Options No Callback Set by Caller (Routing and Remote Access Service only)
Always Callback to:
Apply Static Routes Define routes to enable for this Dial-in connection. Static Routes
OK Cancel Apply

3. Create one Remote Access Policy for MAC Authentication.

🤣 Internet Authenticatio	on Service	_	
<u>File Action View Help</u>)		
← → 🗈 💽 🖗 🞚	3 3		
Internet Authentication S	ervice (Local) Right click	Order	
🗄 🚞 RADIUS Clients	Connections to Microsoft Routing and Remote	1	
🗄 💼 Remote Access Loggir	Connections to other access servers	2	
	New Remote Access Policy		
	New		
	<u>V</u> iew		
	Refresh		
	Export List		
	Help		
New Remote Access Po	licy Wizard X		
Policy Configuration	n Method		
The wizard can cre	eate a typical policy, or you can create a custom policy.		
How do you want to	o set up this policy?		
C Harden with			
© <u>∪</u> se the wiza	ra to set up a typical policy for a common scenario		
Set up a cus	tom policy		
Type a name that de	escribes this policy.		
Policy name: MA	\CAuth		
Exa	mple: Authenticate all VPN connections		
	< <u>B</u> ack <u>N</u> ext≻ Cancel		

Add Policy Conditions

- a."NAS-Identifier". And configure NAS- Identifier as DWS-4000's MAC address.
- b. "Client-IP-Address". And configure Client-IP-Address as DWS-4000's IP address.

New Remote Access Policy Wizard	×
Policy Conditions To be authenticated, connection requests must match the conditions you specify.	Ŷ
Specify the conditions that connection requests must match to be granted or denied access. Policy conditions:	
NAS-Identifier matches "00-09-38-27-30-24" AND Client-IP-Address matches "10.90.90.90"	
Add <u>E</u> dit <u>R</u> emove	
< <u>B</u> ack <u>N</u> ext > C	ancel

Edit Authentication methods and grant remote access permission.



New Remote Access Policy Wizard	×
Permissions A remote access policy can either grant or deny access to users who match the specified conditions.	Ŷ
If a connection request matches the specified conditions: Deny remote access permission Grant remote access permission 	
< <u>B</u> ack <u>N</u> ext > Ca	ncel

- 4. Create another one Remote Access Policy for WPA/WPA2-EAP.
 - a. Input Policy name as what you want.

New Remote Acces	is Policy Wizard 🗙	
Policy Configu The wizard c	an create a typical policy, or you can create a custom policy.	
How do you want to set up this policy?		
Use the	wizard to set up a typical policy for a common scenario	
⊂ <u>S</u> et up a	a custom policy	
Type a name that describes this policy.		
<u>P</u> olicy name:	PEAP	
	Example: Authenticate all VPN connections.	
	< <u>B</u> ack <u>N</u> ext > Cancel	

b. Chose "Wireless"

New Remote Access Policy Wizard
Access Method Policy conditions are based on the method used to gain access to the network.
Select the method of access for which you want to create a policy. © <u>V</u> PN Use for all VPN connections. To create a policy for a specific VPN type, go back to the
 Dial-up Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line. Wireless Use for wireless LAN connections only.
Ethernet Use for Ethernet connections, such as connections that use a switch.
< <u>B</u> ack <u>N</u> ext > Cancel

c. Chose "User"



d. Enable Fast Reconnect

ew Remote Access Policy Wizard	×		_ 🗆 ×
Authentication Methods EAP uses different types of security devices to authenticate users.	ŷ	Order	1
Select the EAP type for this policy. Iype: Protected EAP (PEAP)	Configure	1 2 ote 3 4	x 3 60
Pr	Ditected EAP Prope	rties self to callers before the connection is bet you want it to use as proof of iden	completed.
	Cartificate issued	nolan2003.TS52RADIUS.com	
I <u> </u>	Frendly name: (s:uer: Expiration date: IV Enable Fast Recon	T552RADIU5 2/11/2010 7:36:24 PM inect	
	Eap Types Secured password (E/	AP-M5CHAP ∨2)	Move Up Move Down
Image: Security Certificat 141.png 9 KB	Add	Edit Remove OK	Cancel

Note: If you get error when you click on "Configure...", please re-install CA or reboot your Windows 2003 and try again.

e. Enable Remote Access Policies

PInternet Authentication Service	
 ← → € ↑ × ↑ P Internet Authentication Service (Local) ↑ RADIUS Clients ↑ Remote Access Logging ♥ Remote Access Policies ● Connection Request Processing 	Name Order PEAP Right Click 1 Connections to N PEAP Properties ? × Connections to N Settings ? × Specify the conditions that connection requests must match. Policy gonditions: NAS-Poit-Type matches "Wireless - Other OF Wireless - IEEE 802.11" Add Edit Bemove If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection. Edit Profile Unless individual access permissions are specified in the user profile, this policy controls access to the network. If a connection request matches the specified conditions: If a connection request matches the specified conditions: Deny remote access permission
	Grant remote access permission OK Cancel Apply

f. Edit profile to enable MS-CHAP v2 for WPA/WPA2-EAP user.

Edit Dial-in Profile		? ×						
Dial-in Constraints	IP	Multilink						
Authentication	Encryption	Advanced						
Select the authentication methods you want to allow for this connection.								
EAP Methods								
Microsoft Encrypted /	Microsoft Encrypted Authentication version 2 (MS-CHAP v2)							
User can <u>c</u> hange 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)								
Unauthenticated access								
Allow clients to connect without negotiating an authentication method.								
	ОК (Cancel <u>Apply</u>						

5. Configuring DWS

a. Configuring Radius Server

🔄 DWS-4024	Configuration Named Server Status							
Administration L2 Features	RADIUS Authentication Server Configuration							
	RADIUS Server Host Address	10.90.90.7						
QoS Access Control Lists	Port	1812 (1 to 65535)						
Security Port Security Administ	Secret	Apply						
Port Security Administ Port Security Interface Port Security Static SSL Configuration	Primary Server Message Authenticator							
	Secret Configured	Yes						
SSH Configuration	Current	Yes						
Captive Portal ADIUS	RADIUS Server Name	Default-RADIUS-Server						
RADIUS Configurati	Submit Re	move Refresh						
RADIUS Authentical		_						

b. Enable MAC Authentication and WPA/WPA2-EAP

Global	Discovery	Profile	Radio	SSID	Valid AP	OUL		
Wirele	Wireless Network Configuration							
ccii								
330	SSID							
	Hide SSID							
	ignore Broadcast							
131	12 Tunnol				(1 to 4094)			
131	L3 Tunnel				News			
L3 T	13 Tunnel Subnet							
L3 T	13 Tunnel Mask							
MAG	CAuthenticatio	n				C Local @ RADIUS O Disable		
Red	Redirect				None C HTTP			
Red	Redirect URL							
Wire	eless ARP Supp	pression M	ode					
L2 0)istributed Tun	neling Mod	le			Disable V		
RADI	RADIUS Authentication Server Name				Default-RADIUS-Server			
RADI	RADIUS Authentication Server Status		Configured					
RADI	RADIUS Accounting Server Name		Default-RADIUS-Server					
RADI	RADIUS Accounting Server Status				Not Configured			
RADI	RADIUS Use Network Configuration				Enable 💌			
RADI	RADIUS Accounting							
- See	-14.							
Secu	Security		C None C WEP © WPA/WPA2					
WDA	WPA Versions		WPA Personal III WPA Enterprise					
WPA	WPA Cinhers							
Pre-4	Pre-Authentication							
Pre-4	Authentication	Limit				(D to 192)		
Key (Key Caching Hold Time		(1 to 1440)					
Bcast	Bcast Key Refresh Rate				300 (0 to 86400)			
Speel	Session Key Refresh Rate							
0033				10 10 10 864001				