Windows Vista wireless (WPA) setup - Detailed

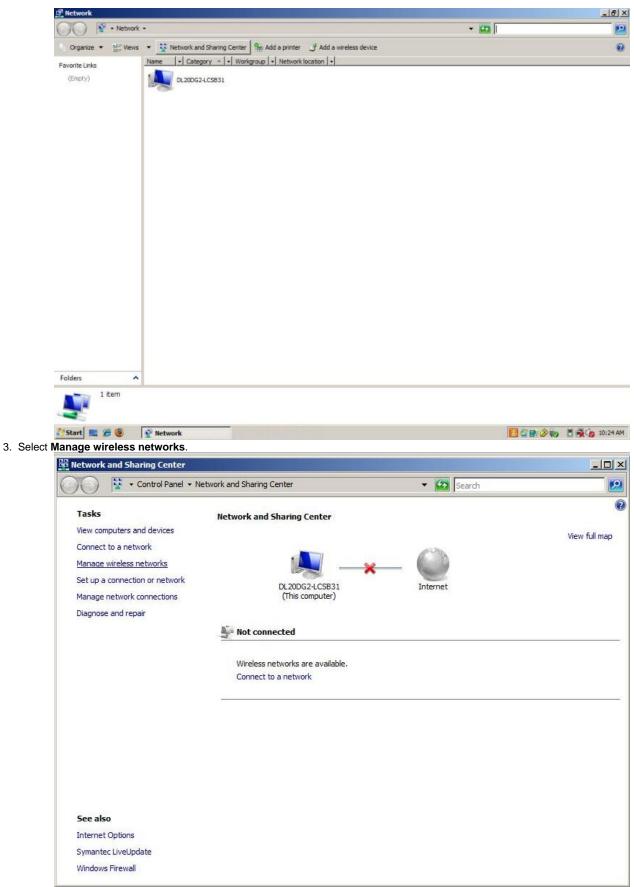
Wireless 802.1x Authentication - Windows Vista

Accessing and Configuring 802.1x Authentication for Windows Vista

1. Open the Start Menu and select Network.

Wozilla Firefox F-mail Microsoft Office Outlook	<u>.</u>
Backup and Restore Center	
Notepad	Documents
Show desktop	Search
	Computer
Windows Media Player	Network
Microsoft Office Word 2007	Connect To
	Control Panel
	Default Programs
	Printers
 All Programs 	Help and Support
Start Search	C. A >

2. Select Network and Sharing Center.



4. Select Add.

MI Manage Wireless Networks	
Aff + Control Panel + Manage Wireless Networks	▼ 🚱 Search
Manage wireless networks that use (Wireless Network Connection) Windows tries to connect to these networks in the order listed below. To change the	e order, drag a network up or down in the list. You can also add or
remove network profiles. To see networks that use a different wireless network adapter, dick Change adapte	r below.
👍 Add 📲 Change adapter 👻 🛞 Adapter properties 🔱 Profile types 😵 N	etwork and Sharing Center
0 items	
anually create a network profile. f Manually connect to a wireless network	
Manually connect to a wireless network	
<u> </u>	
How do you want to add a network?	
Add a network that is in range of this compu	ter
This shows you a list of networks that are currently a Once you connect, a profile for the network is saved	available and lets you connect to one.
Manually create a network profile This creates a new network profile or locates an exis	sting betwork and saves a profile for
the network on your computer. You need to know the key (if applicable).	ne network name (SSID) and security
key (ii applicable).	
Create an ad hoc network	
This creates a temporary network for sharing files or	an Internet connection
	Cancel

- 6. Enter UA_WPA (case sensitive) for Network Name, WPA2-Enterprise for Security type, and AES for Encryption type. Both boxes should
 - be checked, then select Next.
 NOTE: If WPA-Enterprise is not available in the Security type field, your wireless card is not supported or your card might require a firmware/driver update. Check with your card/PC manufacturer.

	reless network you want to add
Network name:	UA_WPA
Security type:	WPA2-Enterprise
Encryption type:	AES
Security Key/Passphrase:	Display characters
Start this connection a	utomatically
Connect even if the ne	twork is not broadcasting
Warning: If you select	this option, your computer's privacy might be at risk.

7. Select the Change connection settings option.

Manually connect to a wireless network	
Manually connect to a wireless network	
Successfully added UA_WPA	
Connect to Open the "Connect to a network" dialog so I can connect.	
Change connection settings Open the connection properties so that I can change the settings.	
	Close

8. Make sure the boxes are checked accordingly and then select the **Security** tab.

UA_WPA Wireless Net	work properties	×
Connection Security		
Name:	UA_WPA	
SSID:	UA_WPA	
Network Type:	Access point	
Network Availability:	All users	
Connect automat	ically when this network is in range	
Connect to a mor	e preferred network if available	
i connect even n	he network is not broadcasting	
	ОК	Cancel

9. Select Settings ..

Security type:	E Socuritu	twork properties	
Choose a network authentication method: Protected EAP (PEAP) Choose a network authentication method: Protected EAP (PEAP) Choose a network authentication for subsequent connections	nnection Security	1	
Choose a network authentication method: Protected EAP (PEAP) Choose a network authentication method: Protected EAP (PEAP) Choose a network authentication for subsequent connections			
Choose a network authentication method: Protected EAP (PEAP) Settings	Security type:	WPA2-Enterprise	
Protected EAP (PEAP) Settings	Encryption type:	AES	-
Protected EAP (PEAP) Settings			
Protected EAP (PEAP) Settings			
Protected EAP (PEAP) Settings			
Protected EAP (PEAP) Settings	Choose a network a	uthentication method:	
Cache user information for subsequent connections			
Cache user information for subsequent connections to this network	Protected EAP (PEA	(P)	Settings
	Cache user infor to this network	mation for subsequen	t connections
	Cache user infor to this network	mation for subsequen	it connections
	Cache user infor to this network	mation for subsequen	it connections
	Cache user infor to this network	mation for subsequen	it connections
	Cache user infor to this network	mation for subsequen	it connections
	Cache user infor to this network	mation for subsequen	it connections
	Cache user infor to this network	mation for subsequen	it connections
OK Cance	Cache user infor to this network	mation for subsequen	

Ensure the Validate server certificate box is checked. Place a check in the box for ALL VeriSign Trust Network instances in the Trusted Root Certificate Authorities list. Make sure Enable Fast Reconnect is checked, then select Configure...

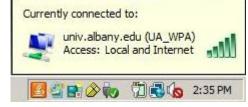
	Protected EAP Properties	×
	When connecting:	
	□ Validate server certificate	
	Connect to these servers:	
	Connect to these servers:	
	Trusted Root Certification Authorities:	
	VeriSign Trust Network	-
	VeriSign Trust Network	
	VeriSign Trust Network	-
	VeriSign Trust Network	
	Do not prompt user to authorize new servers or trusted	
	certification authorities.	
	Select Authentication Method:	
	Secured password (EAP-MSCHAP v2) Config	ure
	✓ Enable Fast Reconnect	
	Enable Quarantine checks	
	Disconnect if server does not present cryptobinding TLV	
	OK Car	ncel
11. Uncheck the box for Automa	tically use my Windows, then, click OK three times to close all three	windows.
	EAP MSCHAPv2 Properties	
	When connecting:	
	Automatically use my Windows logon name and password (and domain if any).	
	password (and domain if any).	
	OK Cancel	
	OK Cancel	
12. The following dialog should a	appear once again. Click on the yellow part of the bubble to open the n	ext step.
	Additional information is required to connect to UA_WPA.	x) +
	Click to provide additional information and connect	
Infi Mar	nage Wireless N 🛛 🚚 Manually connect t 🛛 🌃 📑 🔗 🌆 👘	10:02 AM

13. Enter your NetID and UNIX password and then select OK. Leave the Logon domain field blank.

Jser name: ab123456 Password: ••••••			
Password:		ab123456	ser name:
ussitor u		[•••••	
.ogon domain:	_		
Save this user name and password for future use		er name and password for future use	Save this u

A bubble will appear in the lower right hand corner. Click on the yellow part of the bubble to open the next step.
 Click OK.

The Root Certification Authority for the server's certificate is:
If this is the correct certificate, click OK to connect and you will not see this message again. Click CANCEL to drop connection.
, View Server Certificate
OK Cancel



If the search results do not provide an answer to your question, please submit a Service Desk Request