

NUS Network Configuration Guide for Windows non-domain System.

For Domain join PC please go to Step 20.

The steps in this guide applies to staff wireless SSID "NUS", "NUS_2-4GHz" and student wireless SSID "NUS STU" & "NUS STU 2-4GHz" as well.

1. Go to Windows > Type **RUN** > Select RUN > Type **services.msc** > Click OK

📨 Run	X
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	services.msc ×
	OK Cancel <u>B</u> rowse

2. Right click on WLAN AutoConfig. Choose Properties

				3	Services		
Action View Help							
📅 🖾 🙆 📓 🖬 🕨 🗷 🕪							
vices (Loca Services (Local)							
Wired AutoConfig	Name		Description	Status	Startup Type	Log On As	
_	🔍 Windows Firewall		Windows Fi	Running	Automatic	Local Servi	
Start the service	Windows Font Cache Servi	ce	Optimizes p	Running	Automatic	Local Servi	
	🔍 Windows Image Acquisitio	n (WIA)	Provides im		Manual	Local Servi	
Description	GWindows Installer	Start	, modi		Manual	Local Syst	
The Wired AutoConfig	🔍 Windows Managemen	Stan	des a c	Running	Automatic	Local Syst	
(DOT3SVC) service is	Windows Media Player	Dauro	s Win		Automatic (Network S	
responsible for performing	Windows Modules Inst	Pacumo	les inst		Manual	Local Syst	
IEEE 802.1X authentication on	🔍 Windows Remote Mar	Postart	ows R		Manual	Network S	
Ethernet interfaces. If your	Windows Search	Residit	des co	Running	Automatic (Local Syst	
deployment enforces 802.1X	Windows Store Service	All Tasks	des inf		Manual (Trig	Local Servi	
authentication, the DOT3SVC	Windows Time	Refresh	tains d		Manual (Trig	Local Servi	
service should be configured	🔍 Windows Update 🛛 🦯	Properties	les the		Manual (Trig	Local Syst	
to run for establishing Layer 2	WinHTTP Web Proxy A	Troperties	TTP i	Running	Manual	Local Servi	
connectivity and/or providing	Wired AutoConfig	Help	Vired		Manual	Local Syst	
Wired networks that do not	WLAN Autoconfig		The WLANS	Running	Automatic	Local Syst	
enforce 802.1X authentication	WMI Performance Adapter	r	Provides pe	-	Manual	Local Syst	
are unaffected by the	Workstation		Creates and	Running	Automatic	Network S	
DOT3SVC service.	WWAN AutoConfig		This service	-	Manual	Local Servi	



3. Change Startup type to Automatic and then click Start. Then click OK

General	Log On	Recovery Depende	ncies	
Service	e name:	WlanSvc		
Display	/ name:	WLAN AutoConfig		
Descrip	otion:	The WLANSVC se configure, discove	rvice provides the lo r, connect to, and dis	gic required to connect from a
Path to C:\Wind	executab dows\syst	le: tem32\svchost.exe -k L	ocalSystemNetworki	Restricted
Startup	typ <u>e</u> :	Automatic		~
Startup <u>Help m</u> Service	typ <u>e</u> : e configu a status:	Automatic re service startup optio	<u>ns.</u>	~
Startup Help m Service	typ <u>e</u> : e configu a status: Start	Automatic reservice startup optio Running Stop	ns. Pause	✓ <u>R</u> esume

4. Go to Desktop and press Shortcut Key **Control** + **R**. Type **control** in text box and Click **OK**.

Ru	in	×
Type the name of a pro- Internet resource, and W	gram, folder, do /indows will op	ocument, or en it for you.
control		~
ОК	Cancel	<u>B</u> rowse
	Ru Type the name of a pro- Internet resource, and W control	Run Type the name of a program, folder, do Internet resource, and Windows will op control OK Cancel



5. Double click on **Network and Internet**



6. Double click on **Network and Sharing Center**





7. Click on **Set up a new connection or network**

ц;	Network and Sharing Center 🛛 🗕 🗖 💌
(e) → ↑ ↓ Control Panel	▶ Network and Internet ▶ Network and Sharing Center
Control Panel Home Change adapter settings Change advanced sharing settings	View your basic network information and set up connections View your active networks View your active networks View your networking settings View your networking settings Set up a new connection or network Set up a broadband, dial-up, or VPN connection; or set up a router or access point. Toubleshoot problems Diagnose and repair network problems, or get troubleshooting information.
See also HomeGroup Internet Options Windows Firewall	

8. Click Manually connect to a wireless network





9. Type **NUS** as network name. Choose **WPA2-Enterprise** as Security type. Choose **AES** as Encryption type. Check *Start this connection automatically*. Check *Connect even if the network is not broadcasting*. Then click **Next**

		- 🗆 🗙
📀 🚊 Manually conr	nect to a wireless network	
Enter information	n for the wireless network you want to	o add
Network name:	NUS	
Security type:	WPA2-Enterprise	
Encryption type:	AES	
Security Key:	Hide c	haracters
✓ Start this conner	ction automatically	
Connect even if	the network is not broadcasting	
Warning: If you	select this option, your computer's privacy might	t be at risk.
		2
		<u>N</u> ext Cancel

10. Click Change connection settings





11. Click on **Connection** tab. Check *Connect automatically when this network is in range*. Check *Connect even if the network is not broadcasting its name (SSID)*

onnection Security	
N	NUC
Name:	NUS
SSID:	NUS
Network type:	Access point
Network availability:	All users
<u></u>	
✓ Connect automati	cally when this network is in range
	remetwork is not broadcasting its name (3310)

12. Click on **Security** tab. Choose **WPA2-Enterprise** as Security type. Choose **AES** as Encryption type. Check *Remember my credentials for this connection each time I'm logged on*. Choose **Microsoft Protected EAP** (**PEAP**) as network authentication method. Then click **Settings**

Please note: if you are using a common or shared notebook, you should Uncheck **Remember my credential for this connection each time I'm logged on**.

Security type:	WPA2-Enterprise	> 、	
Encryption type:	AES		/
Choose a network	authentication method	:	-
Microsoft: Protect	ed EAP (PEAP)	Settings	
Microsoft: Protect	ed EAP (PEAP)	Settings	
Microsoft: Protect	ed EAP (PEAP) credentials for this co d on	Settings	
Microsoft: Protect	ed EAP (PEAP)	Settings	
Microsoft: Protect	ed EAP (PEAP) credentials for this co d on	Settings	
Microsoft: Protect	ed EAP (PEAP)	Settings	



- 13. Check on *Validate server certificate* and *Connect to these servers*. Enter **auth01.nw.nus.edu.sg** at the field box. Check **DigiCert Global Root CA**.
- 14. Choose Secured password (EAP-MSCHAP v2) as Authentication Method & Check Enable *Fast Reconnect*. Then click Configure...

men connecung:	
Verify the server's identity by validating the certi	ficate
1.40	*i
Connect to these servers (examples:srv1;srv2;.	-\.srv3\.com):
auth01.nw.nus.edu.sg	
Trusted Root Certification Authorities:	
Class 3 Public Primary Certification Authority	^
COMODO RSA Certification Authority	
DigiCert Assured ID Root CA	
🗹 DigiCert Global Root CA	
DigiCert Global Root G2	
DigiCert High Assurance EV Root CA	
DST Root CA X3	¥
<	>
Notifications before connecting:	
Tell user if the server's identity can't be verified	~
elect Authentication Method:	
Secured password (EAP-MSCHAP v2)	Configure
Enable Fast Reconnect	
Disconnect if server does not present cryptobindin	a TLV
Enable Identity Privacy	

15. Uncheck Automatically use my Windows logon name and password (and domain if any). Then click **OK**



16. Click OK



17. Click Advanced settings

NUS W	ireless Networ	k Propert	ies	×
Connection Security				
S <u>e</u> curity type: E <u>n</u> cryption type:	WPA2-Enterprise		~	
Ch <u>o</u> ose a network a Microsoft: Protecte	uthentication metho d EAP (PEAP)	d: <u>S</u> ettir	igs	
Remember my o time I'm logged	credentials for this co on	onnection eac	h	
A <u>d</u> vanced setting	js			
	Γ	01		

18. Check **Specify authentication mode**, Select **User or computer authentication** from the dropdown menu and Click **OK**

Specify authentication mode: User or computer authentication Delete credentials for all user: Enable gingle sign on for this network Perform immediately before user logon Perform immediately after user logon Maximum delay (seconds): 10 Allow additional dialogs to be displayed during sing sign on This network uses separate virtual LANs for machin and user authentication	02.1X settings	802.11 settings		
User or computer authenticatior ∨ Save gredent Delete credentials for all user: Enable gingle sign on for this network ● Perform immediately before user logon Perform immediately after user logon ● Perform immediately after user logon Maximum delay (seconds): ▲ Allow additional dialogs to be displayed during sing sign on This network uses separate virtual LANs for machinand user authentication	✓ Specify a	authentication mode:		
	User or	computer authenticatior	✓ Save <u>c</u>	redentials
Enable gingle sign on for this network Perform immediately before user logon Perform immediately after user logon Maximum delay (seconds): 10 Allow additional dialogs to be displayed during sing sign on This network uses separate virtual LANs for machin and user authentication	Delet	e credentials for all user		
Perform Immediately bgfore user logon Perform immediately after user logon Maximum delay (seconds): I0 Allow additional dialogs to be displayed during sing sign on This network uses separate virtual LANs for machin and user authentication	Enable s	ingle sign on for this netv	vork	
Perform immediately after user logon Maximum delay (seconds): 10 Allow additional dialogs to be displayed during sing sign on This network uses separate virtual LANs for machin and user authentication	Perfo	orm immediately b <u>e</u> fore u	iser logon	
Maximum delay (seconds): 10	Perfo	orm immediately a <u>f</u> ter use	er logon	
 Allow additional dialogs to be displayed during sing sign on This network uses separate yirtual LANs for machin and user authentication 	Maximu	m delay (seconds):	10	*
This network uses separate virtual LANs for machin and user authentication	Allov sign	v additional dialogs to be on	displayed durin	g single
and User authentication	This	network uses separate v	rtual LANs for r	machine
	anu	user authentication		



19. Click **802.11 settings** tab. Check **Enable Pairwise Master Key (PMK) caching** and Click **OK**.

Advanced settir	ngs	×
802.1X settings 802.11 settings		
Fast roaming		
nable Pairwise Master Key (PMK) ca	ching	
PMK time to live (minutes):	720	-
Number of entries in PMK cache:	128	-
This network uses pre-authentication		
Maximum pre-authentication	3	*
Enable Eederal Information Processing : compliance for this network	Standards (FIP	S)
Enable Eederal Information Processing : compliance for this network	Standards (FIP	s)

20. Go to your taskbar on the bottom right hand of your taskbar and double click on the wireless icon



21. Click on NUS Wireless Profile and Click on Connect.



- 22. Enter Username and Password and Click **OK**
 - Username : (Enter your "Domain\Username") (E.g. of Domain: NUSSTF/NUSSTU/NUSEXT)
 - **Password** : (Enter your Password)



23. Connected to SSID NUS

