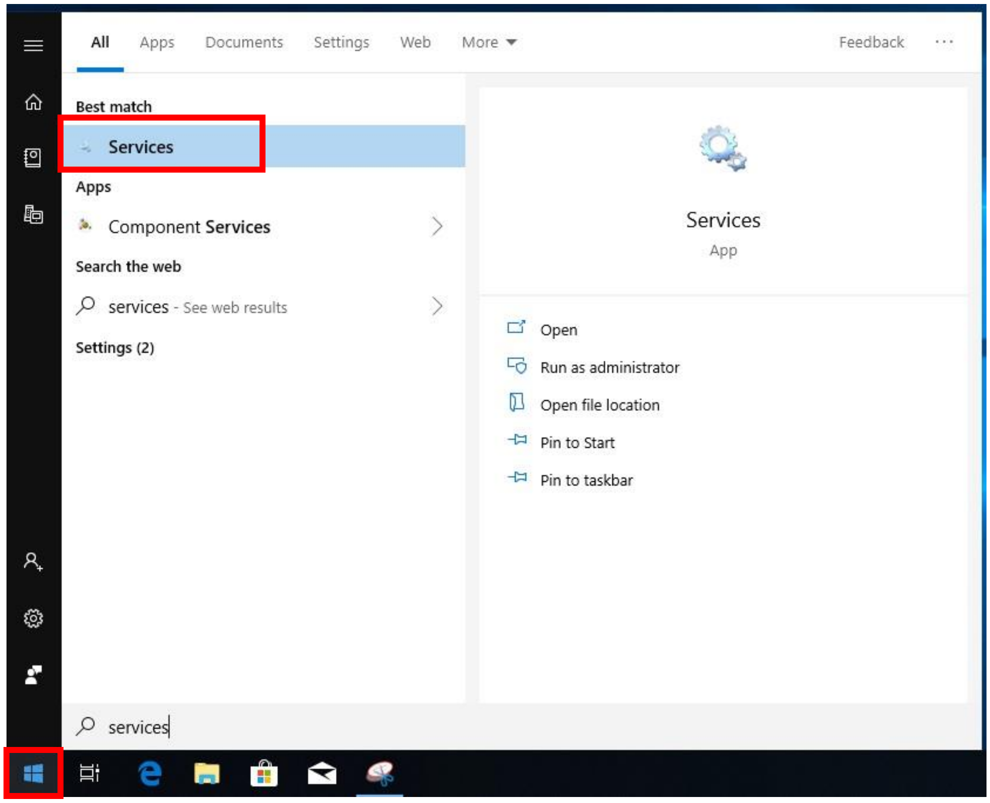
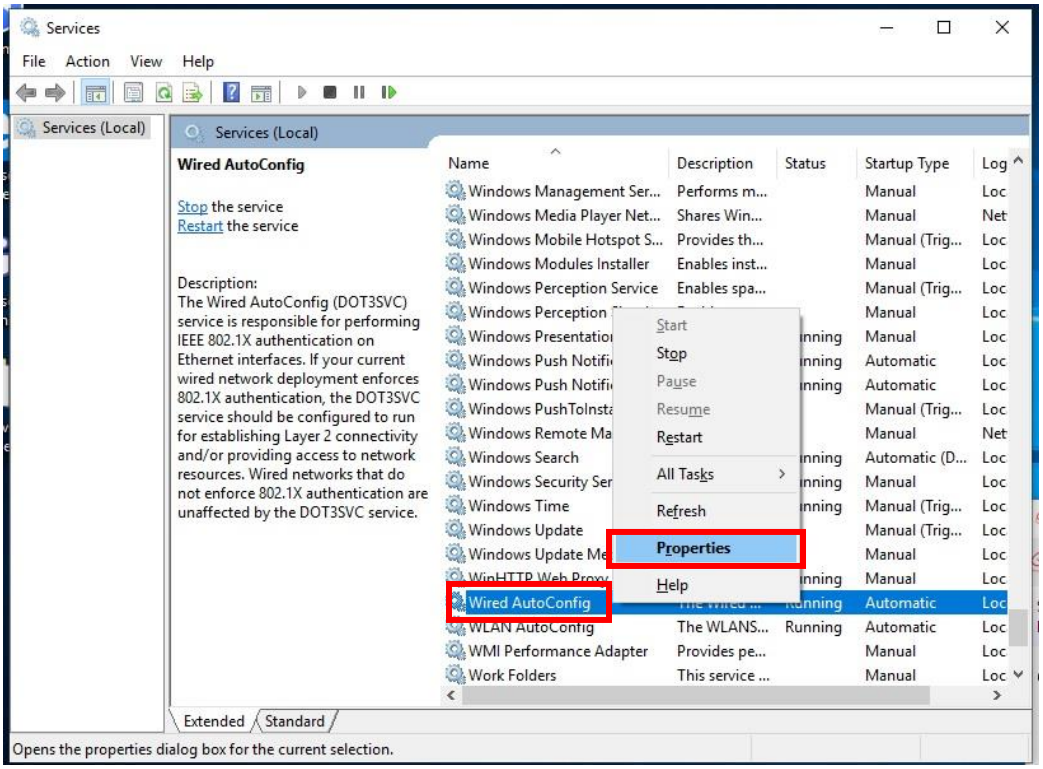
NANYANG
TECHNOLOGICAL
UNIVERSITY
SINGAPORE

[BYOD] Windows 10 802.1x Network Adapter Settings

1. Go to **Windows 10 Start Menu**, type “**Services**” and open it.



2. “**Services**” window will be displayed. Right click on “**Wired AutoConfig**” and click “**Properties**” from pop up menu.



Wired AutoConfig

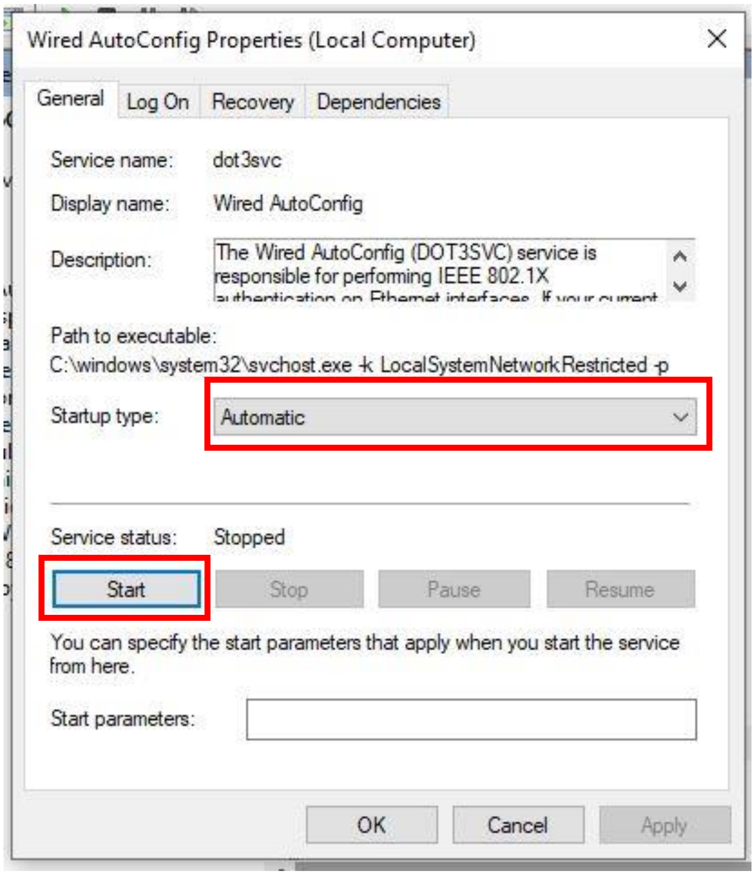
Stop the service
Restart the service

Description:
The Wired AutoConfig (DOT3SVC) service is responsible for performing IEEE 802.1X authentication on Ethernet interfaces. If your current wired network deployment enforces 802.1X authentication, the DOT3SVC service should be configured to run for establishing Layer 2 connectivity and/or providing access to network resources. Wired networks that do not enforce 802.1X authentication are unaffected by the DOT3SVC service.

Name	Description	Status	Startup Type	Log
Windows Management Ser...	Performs m...		Manual	Loc
Windows Media Player Net...	Shares Win...		Manual	Net
Windows Mobile Hotspot S...	Provides th...		Manual (Trig...	Loc
Windows Modules Installer	Enables inst...		Manual	Loc
Windows Perception Service	Enables spa...		Manual (Trig...	Loc
Windows Perception			Manual	Loc
Windows Presentatio		nning	Manual	Loc
Windows Push Notifi		nning	Automatic	Loc
Windows Push Notifi		nning	Automatic	Loc
Windows PushToInsta			Manual (Trig...	Loc
Windows Remote Ma			Manual	Net
Windows Search		nning	Automatic (D...	Loc
Windows Security Ser		nning	Manual	Loc
Windows Time		nning	Manual (Trig...	Loc
Windows Update			Manual (Trig...	Loc
Windows Update Me			Manual	Loc
WinHTTP Web Proxy		nning	Manual	Loc
Wired AutoConfig	The Wired ...	Running	Automatic	Loc
WLAN AutoConfig	The WLANS...	Running	Automatic	Loc
WMI Performance Adapter	Provides pe...		Manual	Loc
Work Folders	This service ...		Manual	Loc

Opens the properties dialog box for the current selection.

3. “**Wired AutoConfig Properties**” window will be displayed. Change “**Startup type**” to “**Automatic**” and click “**Start**” to enable 802.1x service. Then, click “**OK**”.



Wired AutoConfig Properties (Local Computer)

Service name: dot3svc

Display name: Wired AutoConfig

Description: The Wired AutoConfig (DOT3SVC) service is responsible for performing IEEE 802.1X authentication on Ethernet interfaces. If your current

Path to executable:
C:\windows\system32\svchost.exe -k LocalSystemNetworkRestricted -p

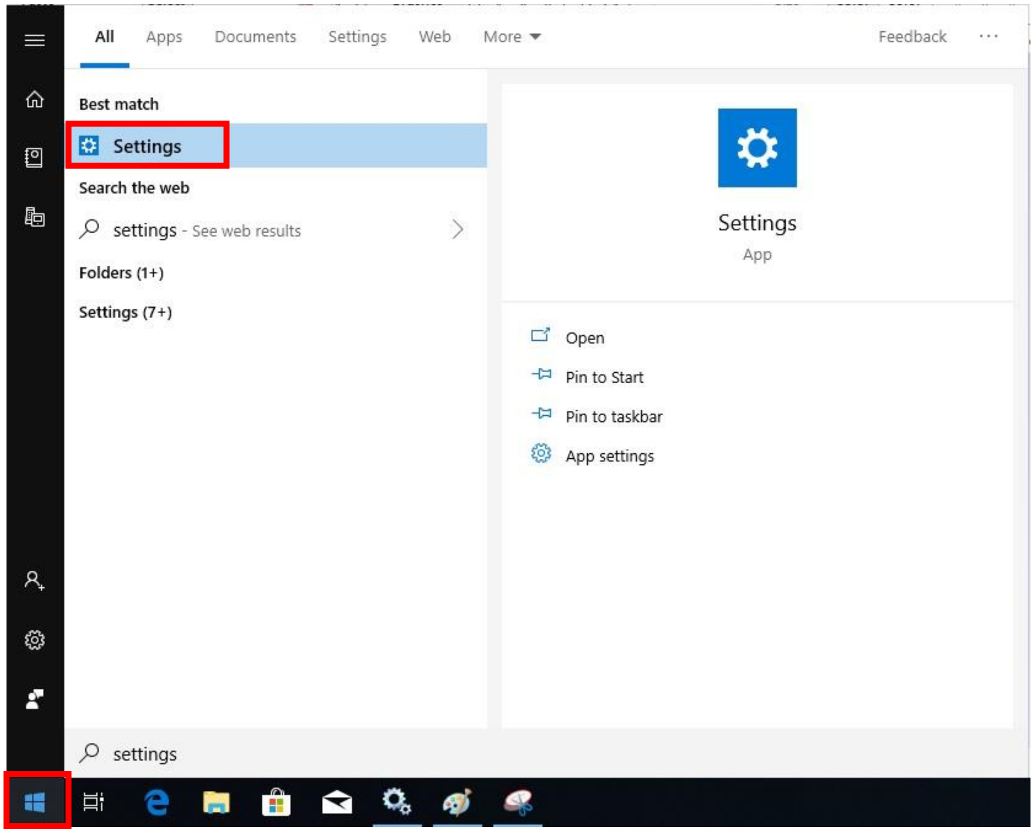
Startup type: Automatic

Service status: Stopped

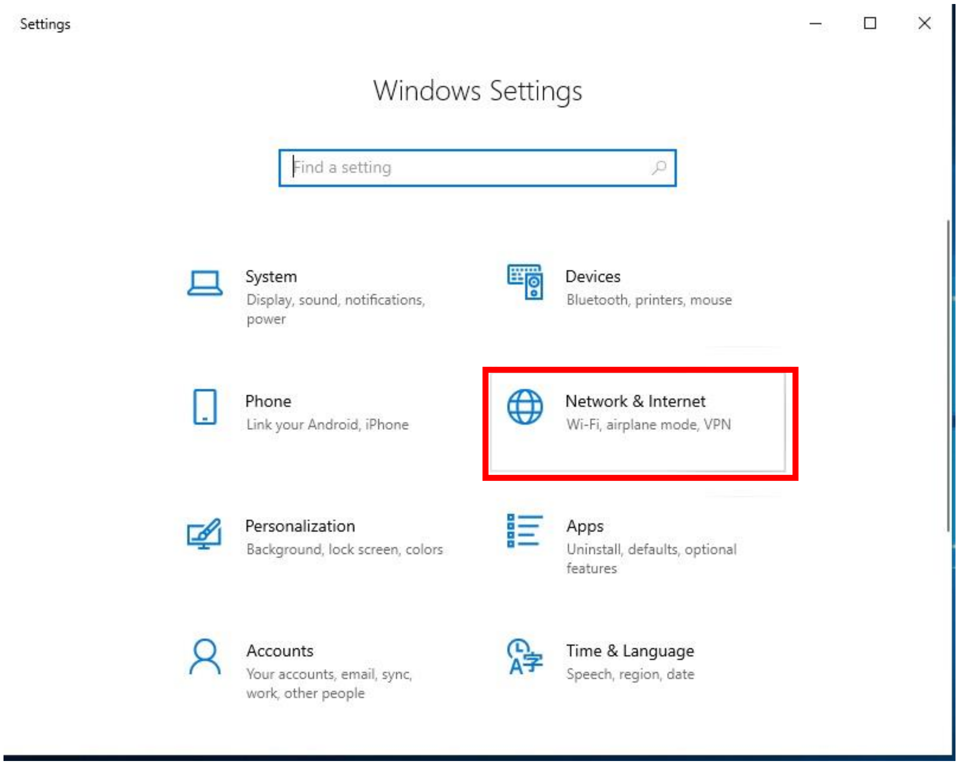
You can specify the start parameters that apply when you start the service from here.

Start parameters:

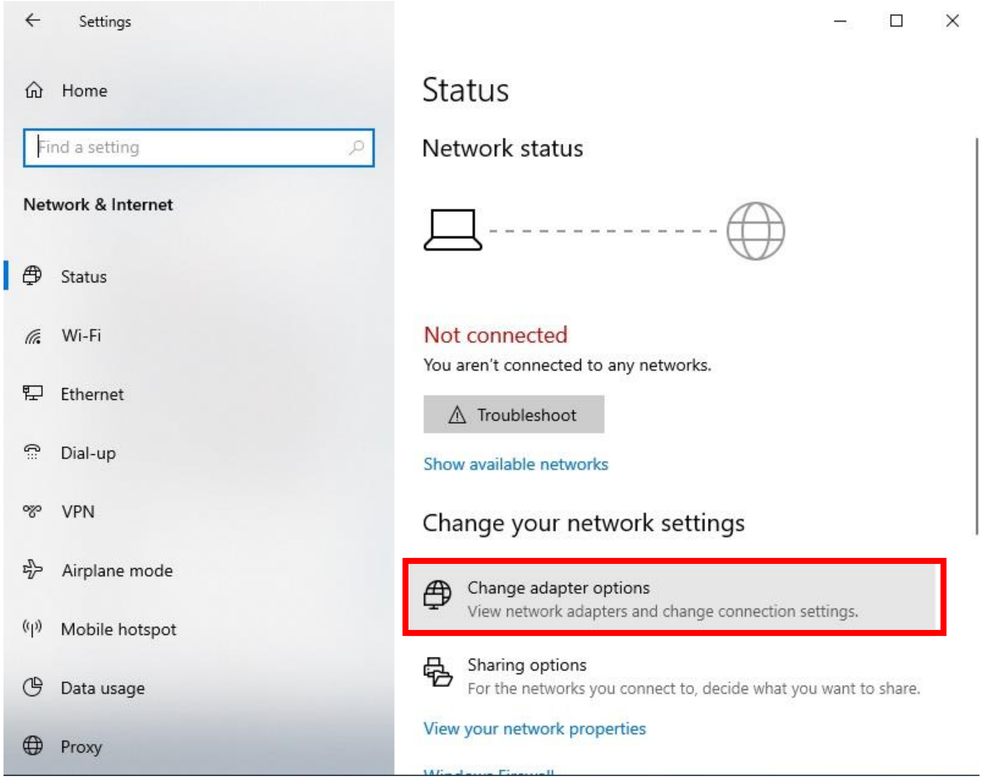
4. Go to **Windows 10 Start Menu**, type “**Settings**” and open it.



5. “**Windows Settings**” window will be displayed and click “**Network & Internet**”.


Settings
Windows Settings
Find a setting
System
Display, sound, notifications, power
Devices
Bluetooth, printers, mouse
Phone
Link your Android, iPhone
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Apps
Uninstall, defaults, optional features
Accounts
Your accounts, email, sync, work, other people
Time & Language
Speech, region, date

6. Next, click “**Change adapter options**”.



Settings

Home

Find a setting

Network & Internet

Status

Wi-Fi

Ethernet

Dial-up

VPN

Airplane mode

Mobile hotspot

Data usage

Proxy

Status

Network status

Not connected

You aren't connected to any networks.

Troubleshoot

Show available networks

Change your network settings

Change adapter options

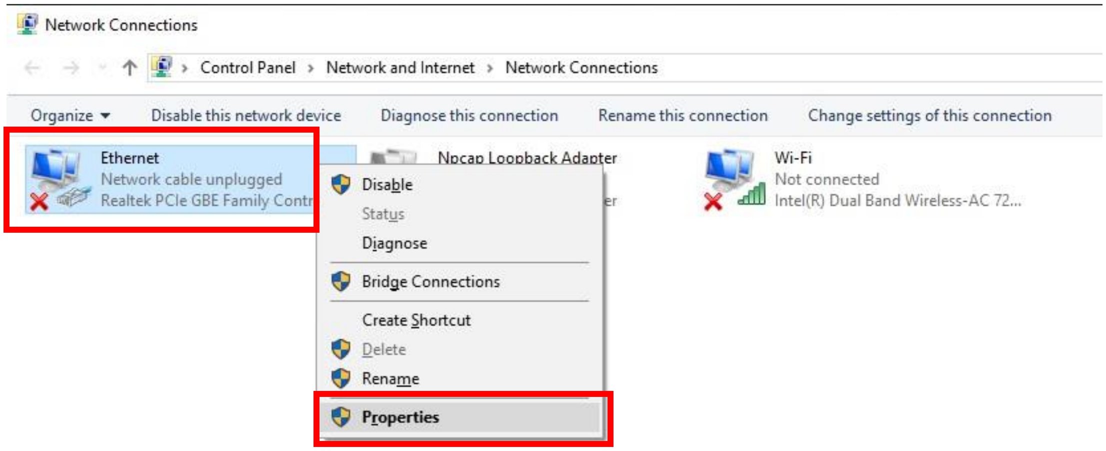
View network adapters and change connection settings.

Sharing options

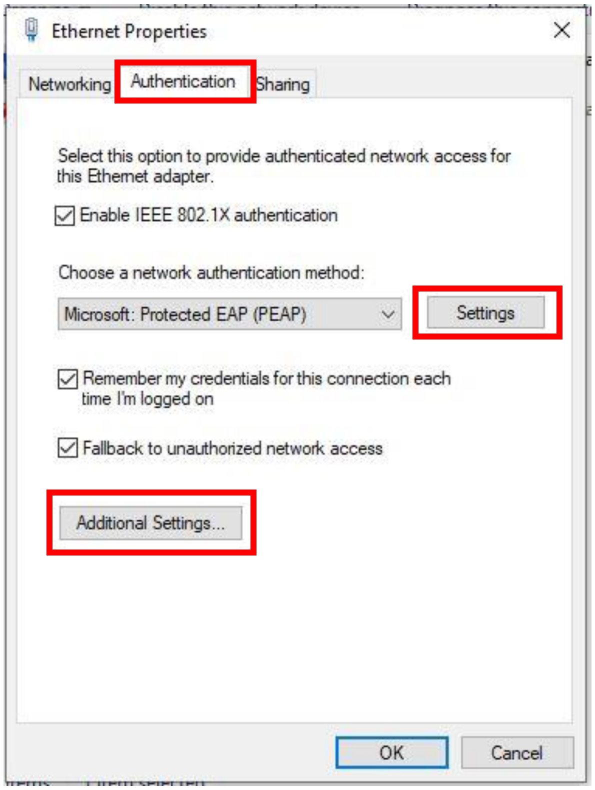
For the networks you connect to, decide what you want to share.

View your network properties

7. “**Network and Connections**” window will be displayed. Right click on correct wired network adapter and click “**Properties**” from pop up menu.



8. “**Ethernet Properties**” window will be displayed and click “**Authentication**” tab.
   Tick “**Enable IEEE 802.1x authentication**”, “**Remember my credentials for this connection each time I’m logged on**”, and “**Fallback to unauthorized network access**”.
   Change network authentication method to “**Microsoft: Protected EAP (PEAP)**”.
   Next, click “**Settings**”.



Select this option to provide authenticated network access for this Ethernet adapter.

☑ Enable IEEE 802.1X authentication

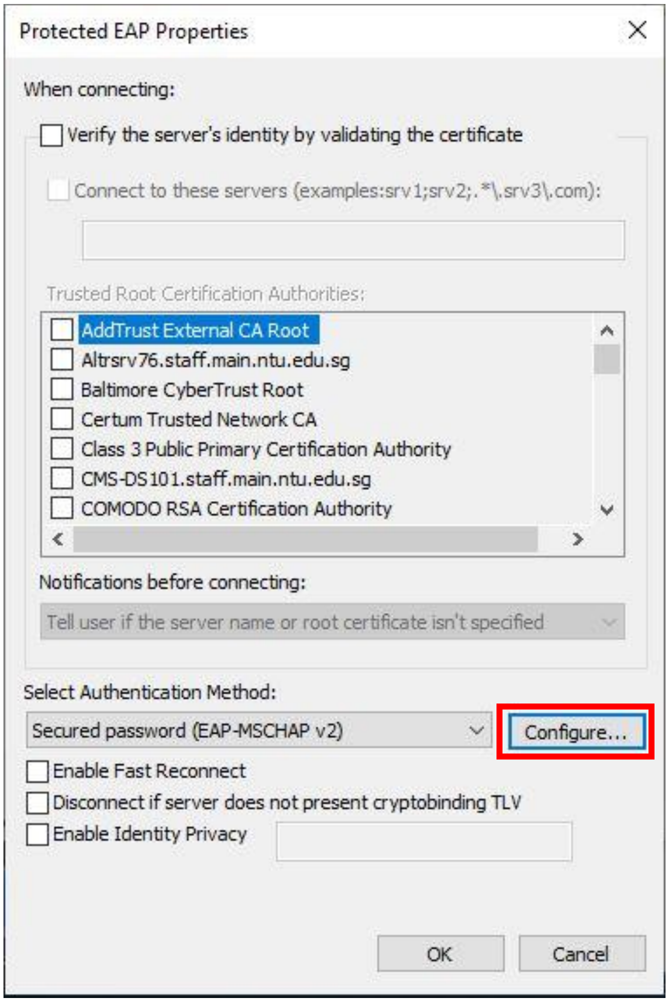
Choose a network authentication method:

Microsoft: Protected EAP (PEAP)

☑ Remember my credentials for this connection each time I'm logged on

☑ Fallback to unauthorized network access

9. “**Protected EAP Properties**” window will be displayed.
   Uncheck “**Verify the server’s identity by validating the certificate**”, “**Enable Fast Reconnect**”, “**Disconnect if server does not present cryptobinding TLV**”, and “**Enable Identity Privacy**”.
   Select “**Secure password (EAP-MSCHAP v2)**” as authentication method.
   Next, click “**Configure**”.



Protected EAP Properties

When connecting:

□ Verify the server's identity by validating the certificate

□ Connect to these servers (examples:srv1;srv2;.*\.srv3\.com):

Trusted Root Certification Authorities:

□ AddTrust External CA Root
□ Altrsrv76.staff.main.ntu.edu.sg
□ Baltimore CyberTrust Root
□ Certum Trusted Network CA
□ Class 3 Public Primary Certification Authority
□ CMS-DS101.staff.main.ntu.edu.sg
□ COMODO RSA Certification Authority

Notifications before connecting:

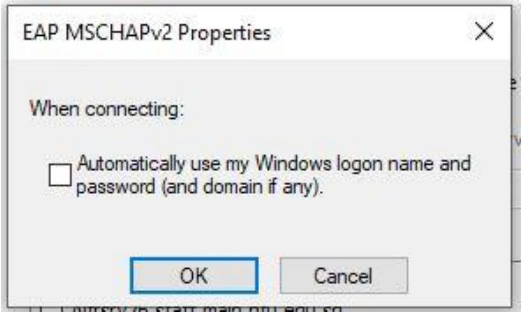
Tell user if the server name or root certificate isn't specified

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

□ Enable Fast Reconnect
□ Disconnect if server does not present cryptobinding TLV
□ Enable Identity Privacy

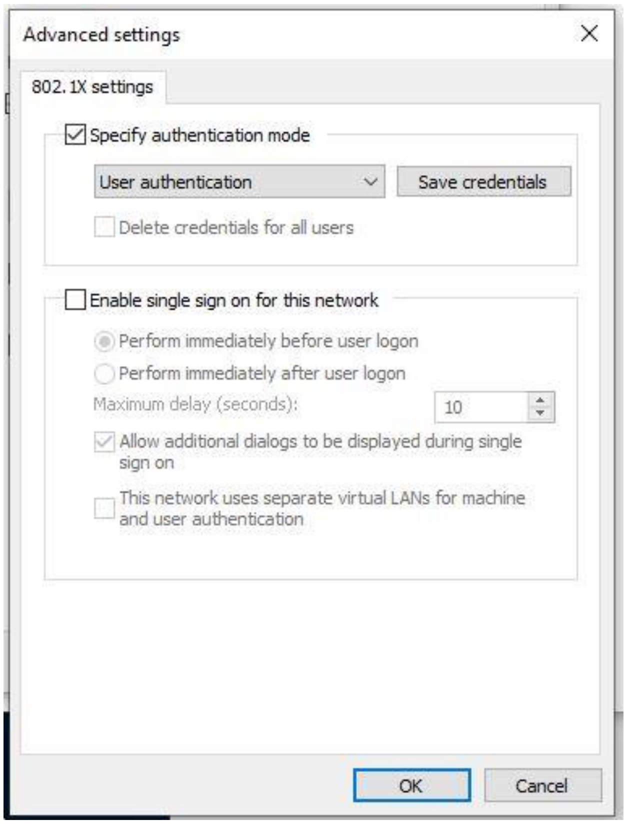
10. “**EAP MSCHAPv2 Properties**” window will be displayed.
    Uncheck “**Automatically use my Windows logon name and password (and domain if any)**” and click “**OK**”.


EAP MSCHAPv2 Properties

When connecting:

□ Automatically use my Windows logon name and password (and domain if any).

11. Go back to “**Ethernet Properties**” window and click “**Advanced Settings**”.
    “**Advanced Settings**” window will be displayed.
    Check “**Specify authentication mode**” and select “**User authentication**” from drop down menu.
    Next, click “**OK**”.


Advanced settings

802.1X settings

☑ Specify authentication mode

User authentication

□ Delete credentials for all users

□ Enable single sign on for this network

● Perform immediately before user logon

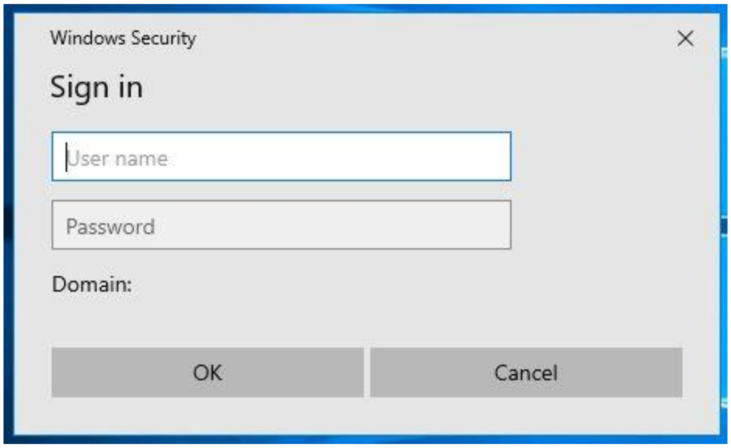
○ Perform immediately after user logon

Maximum delay (seconds): 10

☑ Allow additional dialogs to be displayed during single sign on

□ This network uses separate virtual LANs for machine and user authentication

12. Connect endpoint device to network point. 802.1x login window will be prompted and ask for login credentials.
    For staff user group, enter “**STAFF**” following by username and password. Then, click “**OK**”.
    For student user group, enter “**STUDENT**” following by correct username and password. Then, click “**OK**”.
    For assoc user group, enter “**ASSOC**” following by correct username and password. Then, click “**OK**”.



----- End of Document -----