Manual of 802.1x Authentication for Wired Access

These instructions are for any CUHK-Shenzhen user trying to make a wired connection with 802.1x Authentication while on campus. It is suggested to apply 802.1x authentication to Linux system using command line.

This manual includes 6 parts.

- Check before your start
- Operating systems included
- Operating systems with 802.1x Authentication
- Troubleshooting Steps
- Need help?

Check before your start

- You have CUHK(SZ) username and password.
- Connect your device to the data jack, it should resemble this:

Operating systems included

Windows : Windows 10

Macintosh: macOS Catalina, 10.15

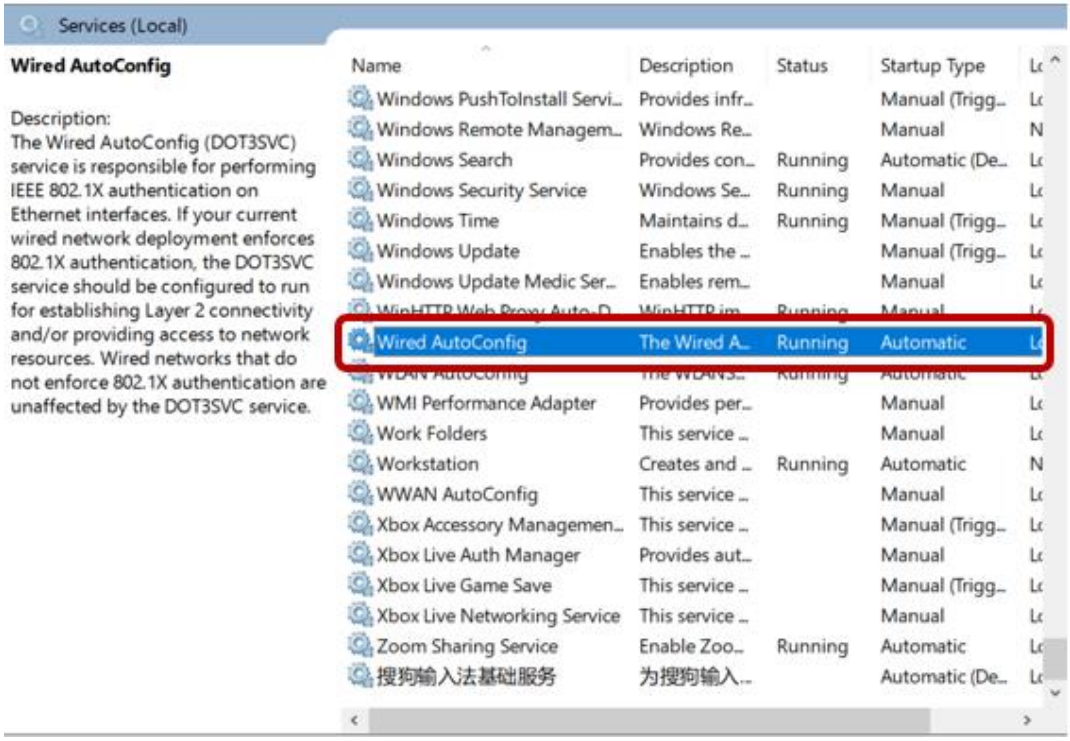
Linux: Red Hat 7, 8 (64-bit), Ubuntu 18.04 (LTS)

Operating systems with 802.1x Authentication

Windows 10:

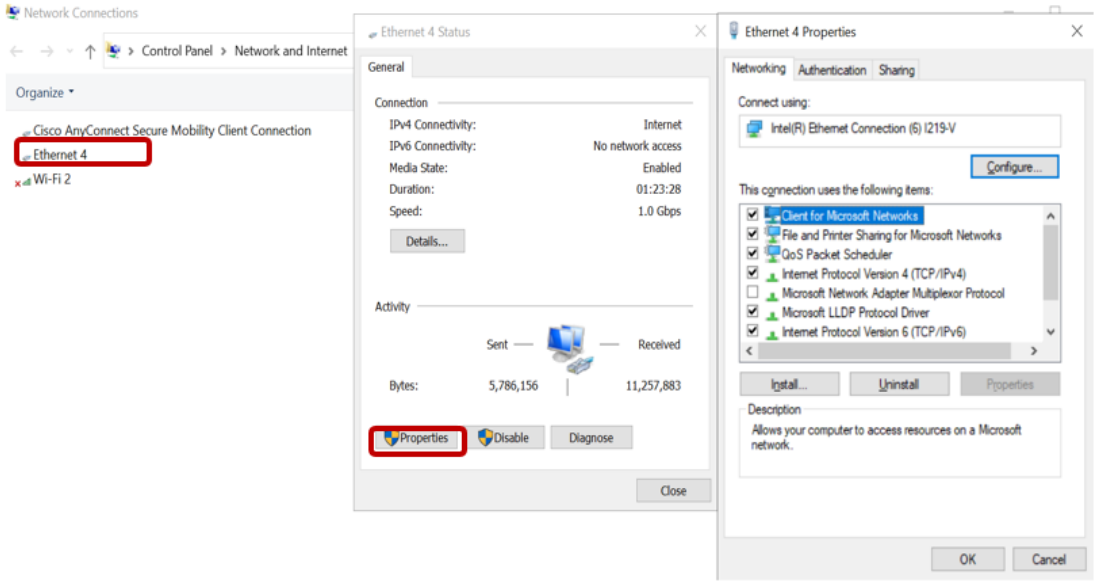
Step 1: Enable the required windows service

1. Type the word **Services** in the search box next to the Start button.
2. Click on the **Services** app.
3. Scroll down until you reach **Wired Autoconfig** and then double-click it.
4. Click **Startup** Type and select **Automatic.**
5. Click **Start** and then click **OK**.



Step 2: Open the Manage Network Connections window

1. Type the words **Control Panel** in the search box next to the Start button.
2. Click on the **Control Panel** app.
3. Click **Network and Sharing Center**, then **Change adapter settings**.
4. Right-click **Ethernet** and then select **Properties**.



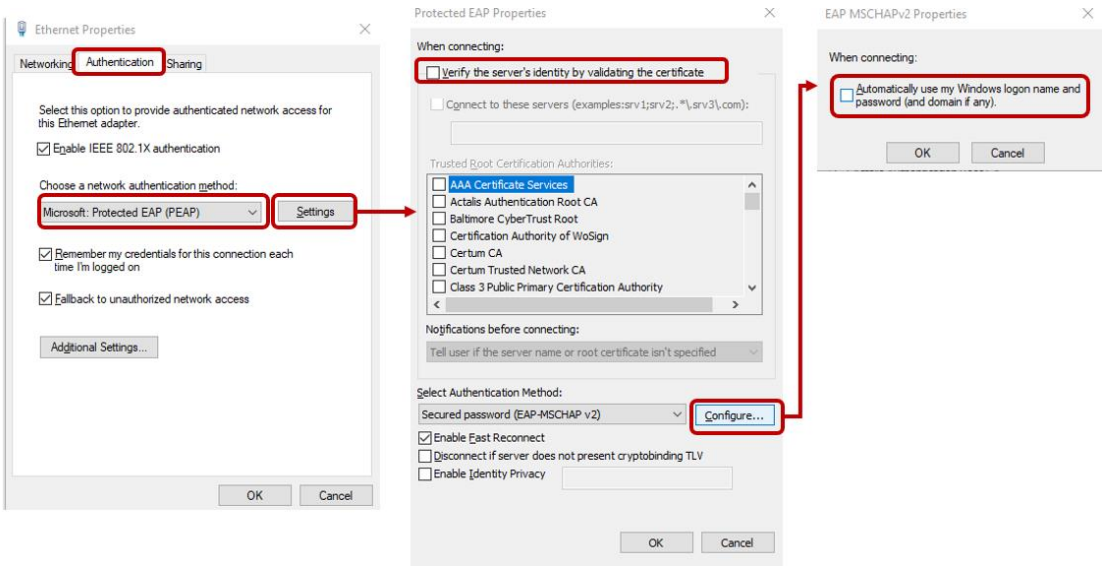
Step3: Local Area Connection Properties Window

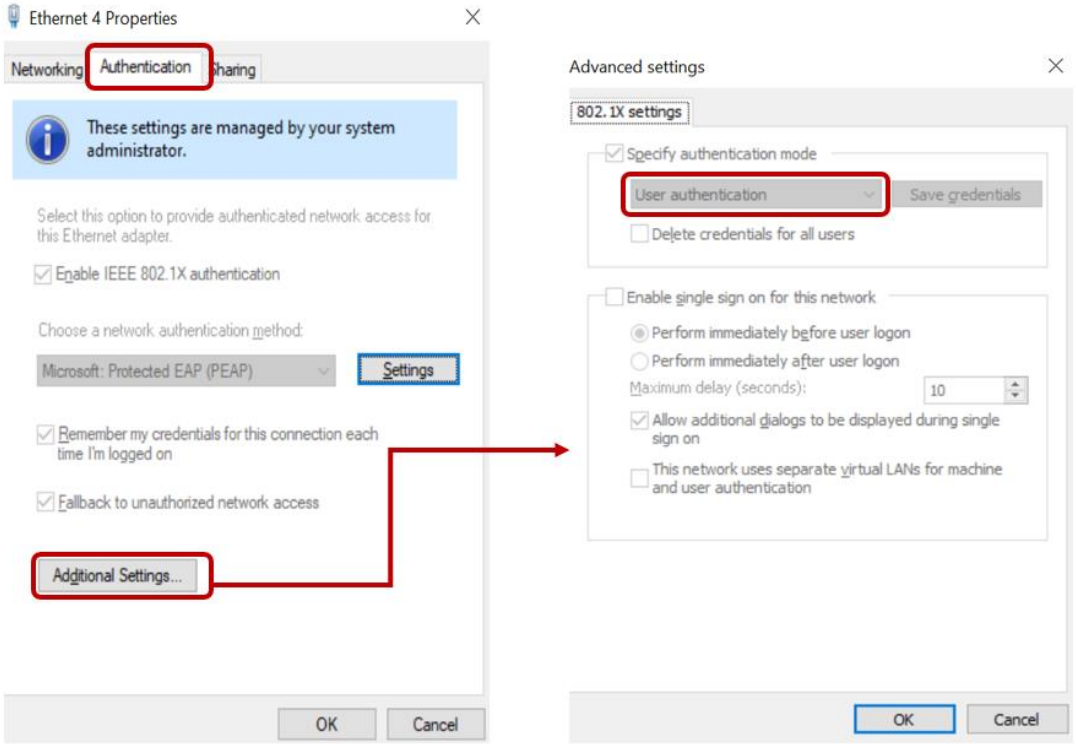
1. Click the **Authentication** tab.
   - Tick Enable **IEEE 802.1X authentication**.
   - Select Microsoft: **Protected EAP (PEAP)**
2. Click **Settings** (next to Choose a network authentication method) to move to the

next section.

3. Under Protected EAP Properties:
   - select **Secured password (EAP-MSCHAP v2)**.
4. Under EAP MSCHAPv2 Properties:
   - Un-tick **Automatically use my Windows logon name and password.**
5. Click Additional Settings.
   - Tick **Specify authentication mode**.
   - Select **User authentication** from the drop-down list.
   - Click **Save credentials.**
   - Enter your CUHK(SZ) **username** and **password.**

Please note: username is not including @cuhk.edu.cn

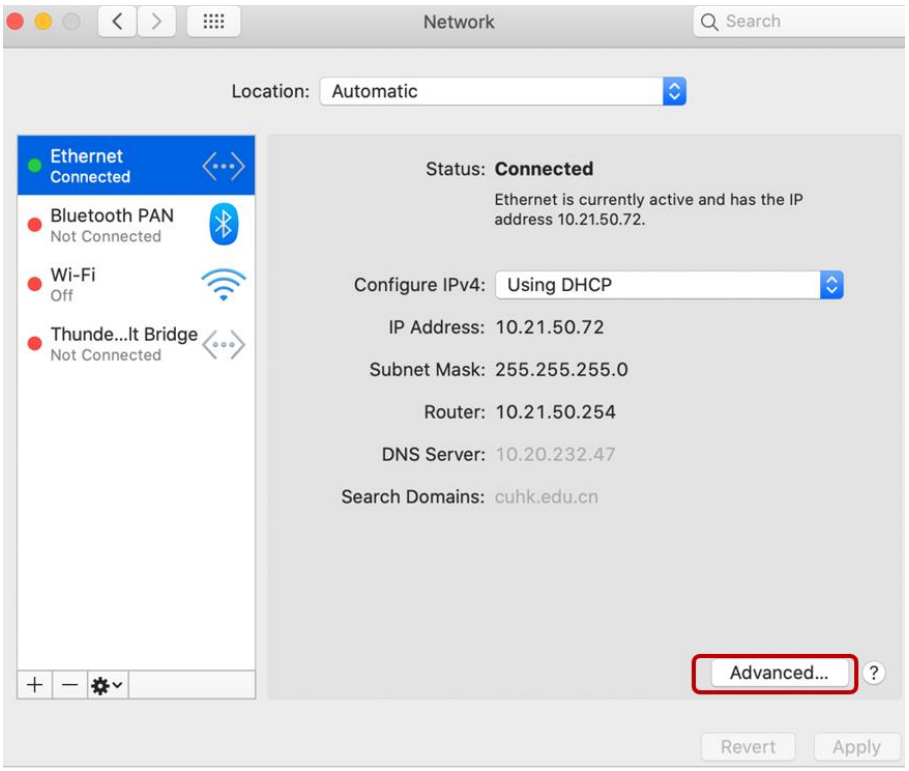




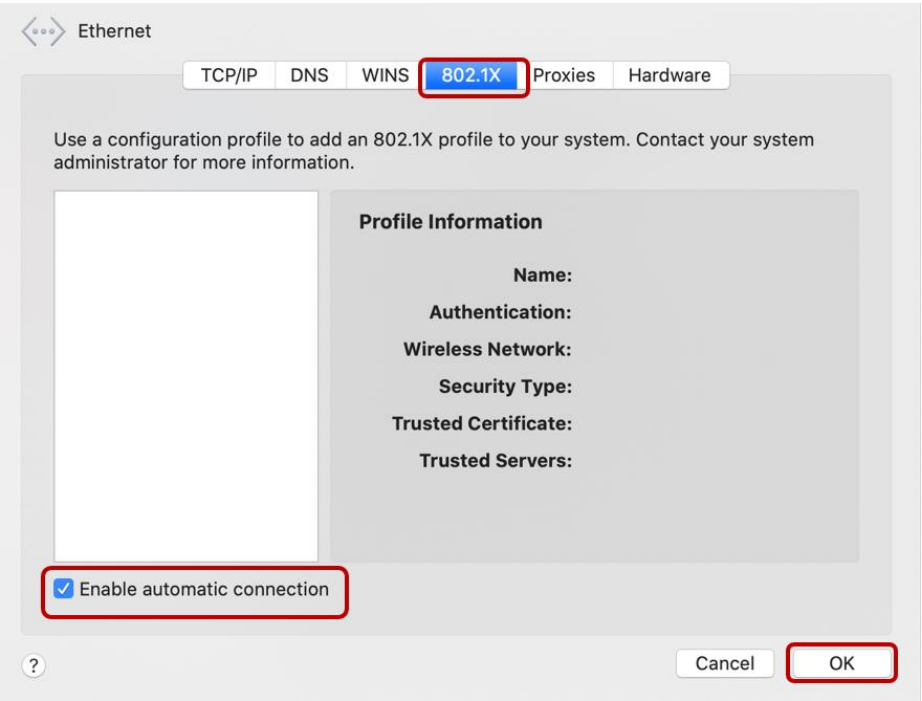
MacOS Catalina, 10.15

1. Choose **Apple menu** > System Preferences

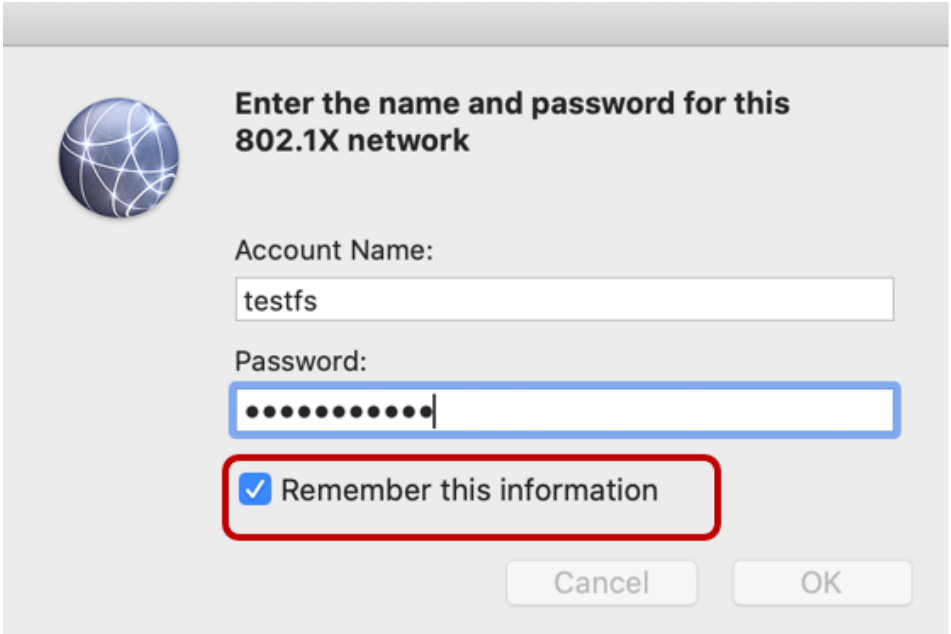
2. Choose **Network under Network & Wireless**
   - Click **Advanced…**



3. Choose the **802.1X** tab
   - Tick **Enable automatic connection**



4. Enter your CUHK(SZ) **username** and **password**
   - Tick **Remember this information**
   - Create 802.1x Password key automatically.



Name	Kind	Date Modified	Expires	Key
<key>	public key	--	--	logi
<key>	private key	--	--	logi
Apple Persistent State Encryption	application password	Today, 14:35	--	logi
Chrome Safe Storage	application password	May 8, 2021 at 15:44:01	--	logi
com.apple.assistant	application password	Apr 2, 2021 at 14:25:19	--	logi
com.apple.assistant	application password	Yesterday, 10:16	--	logi
com.apple.assistant	application password	Yesterday, 10:16	--	logi
com.apple.assistant	application password	Yesterday, 10:16	--	logi
com.apple.assistant	application password	Today, 16:25	--	logi
com.apple.sc...okmarksagent.xpc	application password	Jul 9, 2021 at 09:44:40	--	logi
com.microsof...pdater.HockeySDK	application password	May 8, 2021 at 15:42:14	--	logi
Default	802.1X Password	Today, 16:16	--	logi
DKEYAM	certificate	--	May 23, 2071 at 09:48:42	logi
iMessage Encryption Key	public key	--	--	logi
iMessage Encryption Key	private key	--	--	logi
iMessage Signing Key	public key	--	--	logi
iMessage Signing Key	private key	--	--	logi
MetadataKeychain	application password	Apr 2, 2021 at 14:25:57	--	logi
Safari Session State Key	application password	Jul 9, 2021 at 09:32:19	--	logi

Red Hat 7

Using the nmcli utility, you can configure the client to authenticate itself to the network. This procedure describes how to configure Protected Extensible Authentication Protocol (PEAP) authentication with the Microsoft Challenge-Handshake Authentication Protocol version 2 (MSCHAPv2) in an existing NetworkManager Ethernet connection profile named enp1s0.

- nmcli connection modify enp1s0 802-1x.eap peap 802-1x.phase2-auth mschapv2 802-1x.identity user_name
- nmcli connection modify enp1s0 802-1x.password password
- nmcli connection up enp1s0

```
[root@localhost system-connections]# nmcli connection modify ens192 802-1x.eap peap 802-1x.phase2-auth mschapv2 802-1x.ident
ity testfs
[root@localhost system-connections]# nmcli connection modify ens192 802-1x.password ZZcuhk12345
[root@localhost system-connections]# nmcli connection up ens192
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/3)
[root@localhost system-connections]# nmcli con show
NAME    UUID                                  TYPE           DEVICE
ens192  7b02dd62-ad03-4ce0-80c5-c3daf88bf065  802-3-ethernet  ens192
[root@localhost system-connections]# nmcli dev show
GENERAL.DEVICE:                         ens192
GENERAL.TYPE:                           ethernet
GENERAL.HWADDR:                         00:0C:29:F2:2C:04
GENERAL.MTU:                            1500
GENERAL.STATE:                          100 (connected)
GENERAL.CONNECTION:                     ens192
GENERAL.CON-PATH:                       /org/freedesktop/NetworkManager/ActiveConnection/3
WIRED-PROPERTIES.CARRIER:               on
IP4.ADDRESS[1]:                         10.21.50.73/24
IP4.GATEWAY:                            10.21.50.254
IP4.DNS[1]:                             10.20.232.47
IP4.DOMAIN[1]:                          cuhk.edu.cn
IP6.ADDRESS[1]:                         fe80::9f8:3347:205e:17bc/64
IP6.GATEWAY:                            --
```

Please note: By default, NetworkManager stores the password in clear text in the /etc/sysconfig/network-scripts/keys-connection_name file, which is readable only by the root user. However, clear text passwords in a configuration file can be a security risk.

Please refer: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/configuring_and_managing_networking/authenticating-a-rhel-client-to-the-network-using-the-802-1x-standard_configuring-and-managing-networking

Ubuntu 18.04 (LTS)

You can connect with one of two ways. Before you start, please check NetworkManager or wpa_supplicant has been installed.

- WPA-Supplicant

Step 1: Edit the network interface configuration file: /etc/network/interfaces

- auto lo
- iface lo inet loopback
- auto ens160
- iface ens160 inet dhcp
- wpa-driver wired
- wpa-conf /etc/wpa_supplicant/wpa_wired.conf

Step2: Edit wpa_supplican configuration file: /etc/wpa_supplicant/wpa_wired.conf

```
network={
        key_mgmt=IEEE8021X
        eap=PEAP
        identity="username@cuhk.edu.cn"
        anonymous_identity="username@cuhk.edu.cn"
        password="password"
        phase2="autheap=MSCHAPV2"
}
```

Please note: username@cuhk.edu.cn

```
test@test-virtual-machine:~$ cat /etc/network/interfaces
auto lo
iface lo inet loopback
auto ens160
iface ens160 inet dhcp
wpa-driver wired
wpa-conf /etc/wpa_supplicant/wpa_wired.conf

test@test-virtual-machine:~$ cat /etc/wpa_supplicant/wpa_wired.conf
network={
        key_mgmt=IEEE8021X
        eap=PEAP
        identity="testfs@cuhk.edu.cn"
        anonymous_identity="testfs@cuhk.edu.cn"
        password="[redacted]"
        phase2="autheap=MACHAPV2"
}
```

Step 3: Restart network service

- sudo service networking restart
- sudo service NetworkManager restart

Get Configure Files from SFTP: You can get Configure Files from the SFTP server.

sudo sftp cuhkszsftp@10.20.215.141
password:cuhksz^2021

Password Hash:

You can generate the NtPasswordHash (aka NTLM password hash) yourself as follows:

echo -n plaintext_password_here | iconv -t UTF-16LE | openssl md4

Prefix it with "hash:" in the wpa_supplicant.conf file, i.e.

password=hash:6602f435f01b9173889a8d3b9bdcfd0b

Please refer:https://help.ubuntu.com/community/Network802.1xAuthentication

- nmcli command

Step1: Create a new connection

You can use nmcli con edit to Edit an existing connection or add a new one, using an interactive editor.

- nmcli con edit
  nmcli> set ipv4.method auto
  nmcli> set 802-1x.eap peap
  nmcli> set 802-1x.identity USERNAME
  nmcli> set 802-1x.phase2-auth mschapv2
  nmcli> save nmcli> quit

Step2: Verify your changes in connection configuration file

Add password in /etc/NetworkManager/system-connections/CONNECTION_NAME.
[802-1x] password=YOUR_8021X_PASSWORD

Step3: Restart network service

- sudo service networking restart
- sudo service NetworkManager restart

```
test@test-virtual-machine:~$ sudo nmcli con edit
[sudo] password for test:
Valid connection types: adsl, bluetooth, bond, bridge, cdma, dummy, generic, gsm, infiniband, ip-tunnel, macsec, macvlan, 802-11-olpc
-mesh (olpc-mesh), ovs-bridge, ovs-interface, ovs-port, pppoe, team, tun, vlan, vpn, vxlan, wimax, 802-3-ethernet (ethernet), 802-11-
wireless (wifi), bond-slave, bridge-slave, team-slave
Enter connection type: 802-3-ethernet

===| nmcli interactive connection editor |===

Adding a new '802-3-ethernet' connection

Type 'help' or '?' for available commands.
Type 'describe [<setting>.<prop>]' for detailed property description.

You may edit the following settings: connection, 802-3-ethernet (ethernet), 802-1x, dcb, ipv4, ipv6, tc, proxy
nmcli> set ipv4.method auto
nmcli> set 802-1x.eap peap
nmcli> set 802-1x.identity testfs
nmcli> set 802-1x.phase2-auth mschapv2
nmcli> save
Saving the connection with 'autoconnect=yes'. That might result in an immediate activation of the connection.
Do you still want to save? (yes/no) [yes] yes
Connection 'ethernet-1' (c0de823c-73a7-43a1-a8d2-b3c569faa55d) successfully saved.
nmcli> quit
```

```
test@test-virtual-machine:/etc/NetworkManager/system-connections$ sudo cat ethernet
[sudo] password for test:
[connection]
id=ethernet
uuid=2c3824bb-c893-49c2-91df-fbc14aa0730d
type=ethernet
permissions=

[ethernet]
mac-address-blacklist=

[802-1x]
eap=peap;
identity=testfs
phase2-auth=mschapv2
password=[redacted]

[ipv4]
dns-search=
method=auto

[ipv6]
addr-gen-mode=stable-privacy
dns-search=
method=auto
```

Troubleshooting Steps

Please try the following steps to see if the issue can be resolved on your end.

1. Make sure the Ethernet cable on the computer and the wall ethernet jack is securely connected.
2. Check that you have entered the correct username and password.
3. Ensure you follow all the instructions in this guide.
4. Restart the machine.

Need help?

If you weren't able to connect your device to the campus wired network, please have the following information on hand:

1. Building, Floor, Room
2. MAC address
3. Type of Device

Contact Details

Location: First Floor TD which near the Property Customer Service Office

Office hours: 8:30 a.m.-12:00a.m., 1:00p.m.-5:30p.m. Closed on weekends and public holidays

Online Service Desk: https://itsm.cuhk.edu.cn (Campus Only)

Website: http://itso.cuhk.edu.cn

Email: isupport@cuhk.edu.cn

Hotline: 0755-84273333