Configuring and connecting to the Software-Defined Access (SDA) network

University of Manitoba | Information Services and Technology

Configuring and connecting to the Software-Defined Access (SDA) network

The University of Manitoba is updating our network service to improve performance and security. Use this guide to help you configure and connect to the SDA network on a laptop or desktop in supported facilities.

Table of Contents

1. Setting up the 802.1x client

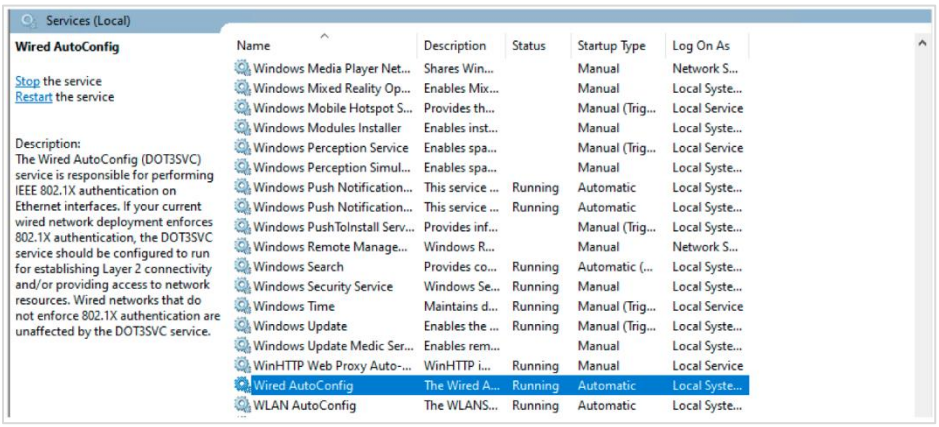
To connect to an 802.1x network, you must first set up the 802.1x client software on your computer. Any departmental IT administrator, IST Service Desk staff or individual who chooses to bring their own device (BYOD) and plug it into an 802.1x-enabled port can perform the 802.1x client configuration.

Note to IT administrators: The procedure of connecting to uofm-secure SSID under a Software-Defined Access (SDA) wireless network is the same as connecting to uofm-secure under a legacy/existing network. Staff and students will be put into their respective virtual networks when connected. For example, when a wireless staff end user connects to uofm-secure under SDA, they will be put into the same virtual network as a wired staff end user. Restrictions between the two virtual networks can be altered as needed. Roaming between SDA and non-SDA wireless networks is transparent to the end user. Re-authentication is performed in the background when roaming between the two.

Windows 10

How to configure the 802.1x client on your Windows 10 workstation.

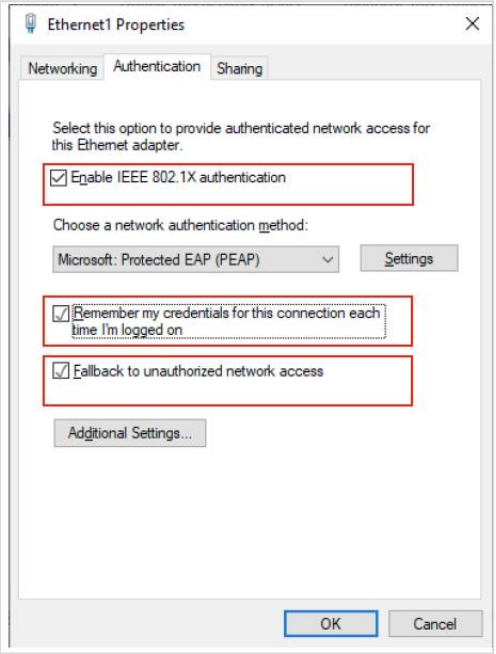
1. Go to **Windows Services** > **Wired Autoconfig**. It must be set to **Automatic** and **Running**.



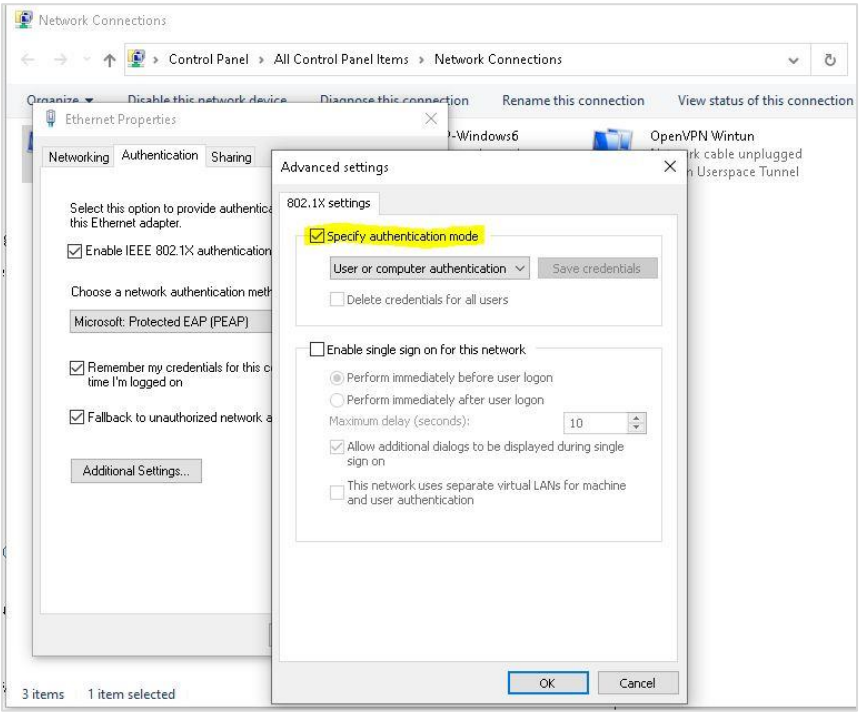
2. To open Network Connections, go to **Windows Settings** > **Network and Internet**> **Ethernet** > **Change adapter options**.
3. Open **Ethernet**.

4. In Ethernet Properties, select the **Authentication** tab.
   a. Check **Enable IEEE 802.1X Authentication**.

b. Select **Microsoft: Protected EAP (PEAP)** for the network authentication method.
c. Check **Remember my credentials for this connection each time I'm logged on**.
d. Check **Fallback to unauthorized network access**.

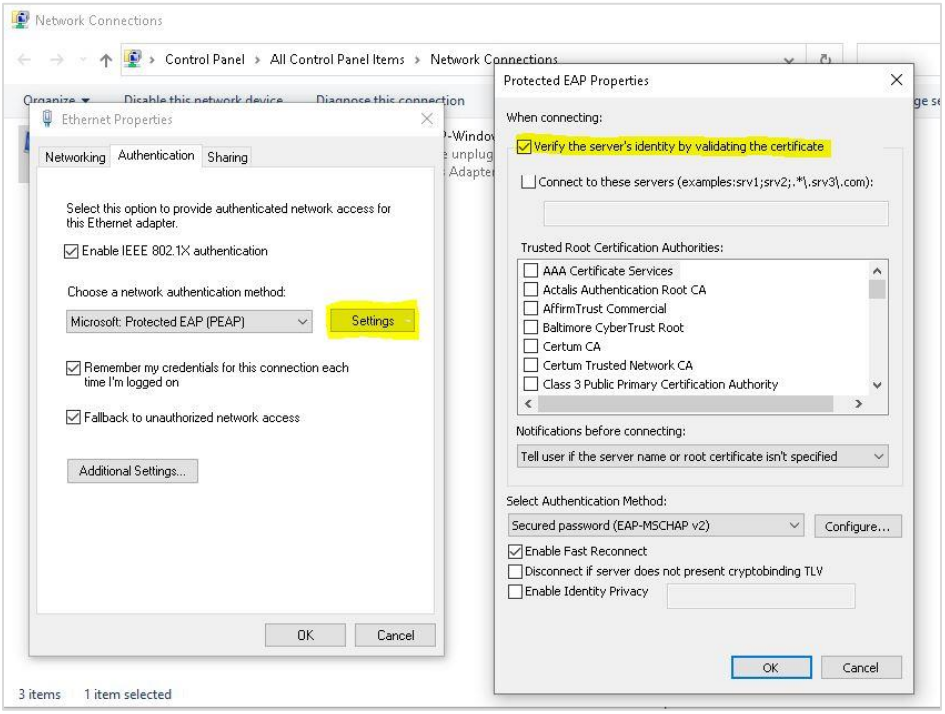


5. In the Authentication tab, select **Additional Settings…** to open **Advanced settings**.
6. In Advanced settings, check **Specify authentication mode**, select **User or computer authentication**, and click **OK**.



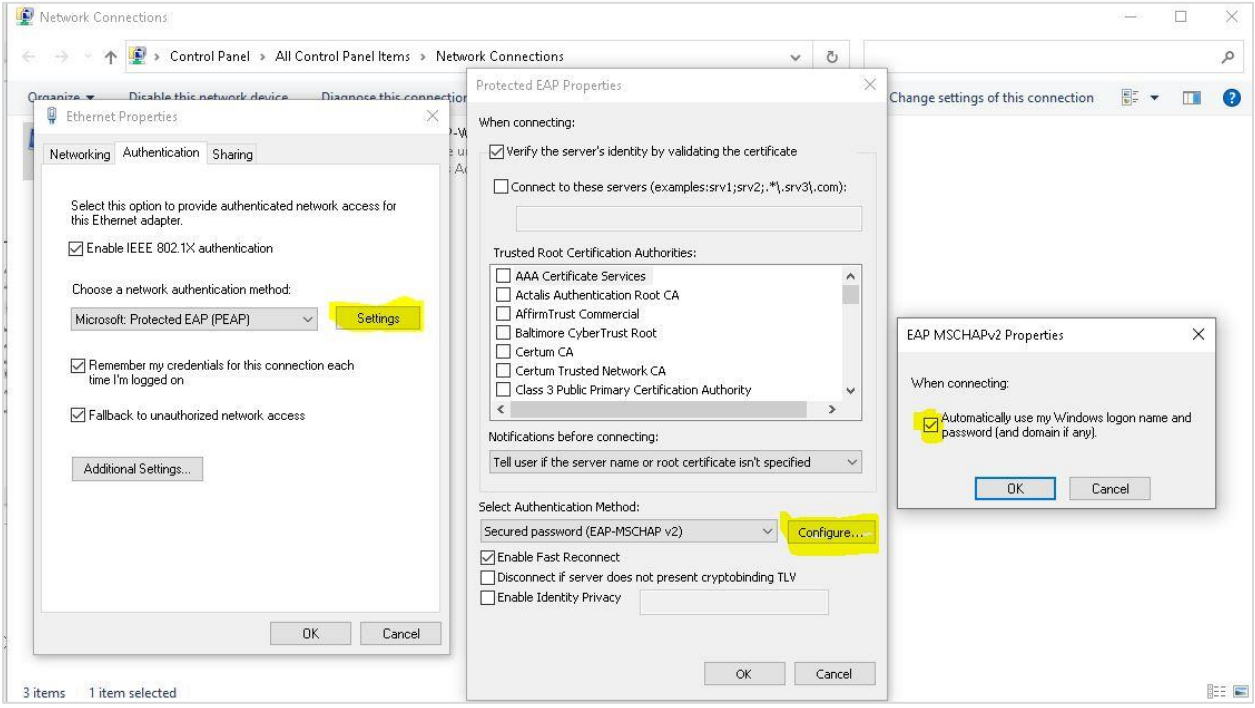
7. In the Authentication tab, select **Settings** to open Protected EAP Properties.

8. In Protected EAP Properties, check **Verify the server's identity by validating the certificate**.



9. In Protected EAP Properties, click **Configure**.

10. In EAP MSCHPv2 Properties, check **Automatically use my Windows logon name and password (and domain if any)** and click **OK**. *Note: This may not apply to a personal device using a local account.*



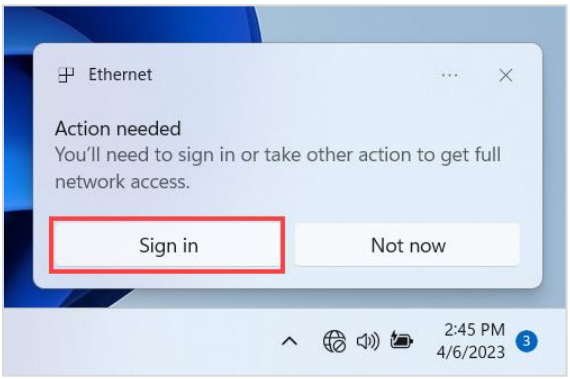
11. Close **Ethernet Properties**.

> Note to IT administrators: This setting may not be applicable if the backend authentication user database for Windows logon and 802.1x is different.

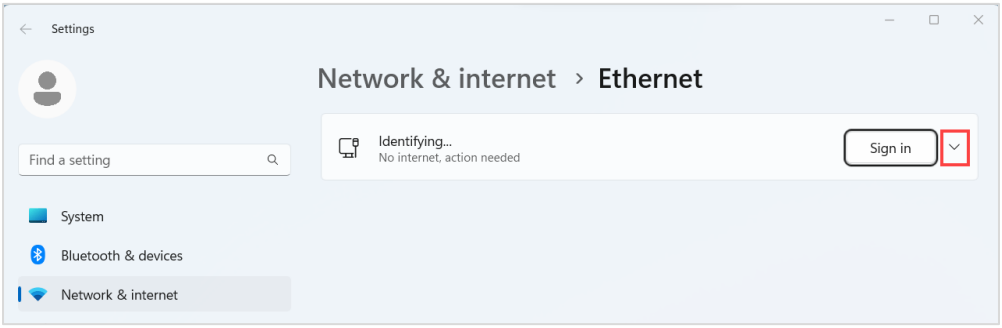
Windows 11 (non-domain joined)

How to configure the 802.1x client and connect to the network on your Windows 11 workstation. Follow these instructions if you are using a desktop or laptop computer that is not managed by Information Services and Technology (IST) and/or is not authenticated to the ad.umanitoba.ca network.

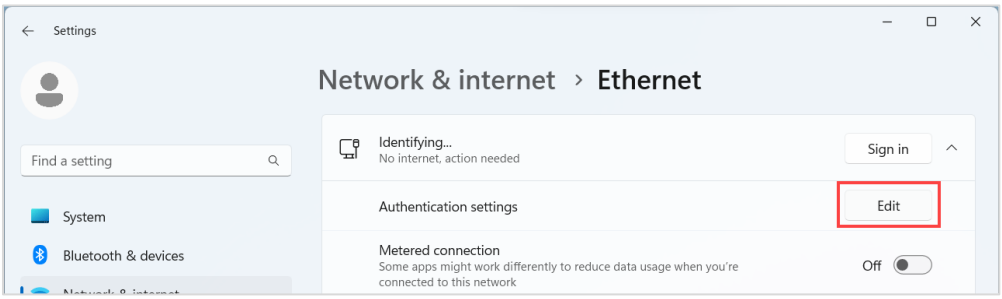
1. Plug your computer into the network outlet on the wall and turn it on. An **Ethernet** pop-up window opens.
2. Select **Sign in** if you want to log in to the network. The **Settings > Network & internet > Ethernet** window opens.



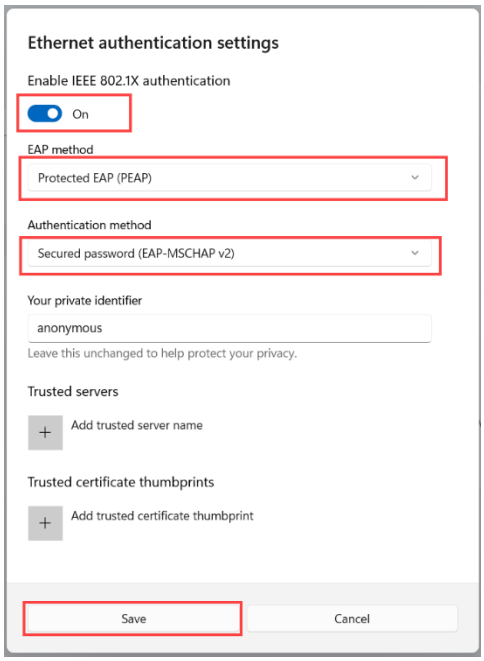
3. You may notice the word "Identifying…" next to the Ethernet icon in your list of networks. Select the arrow next to the Sign In button to open the connection settings.



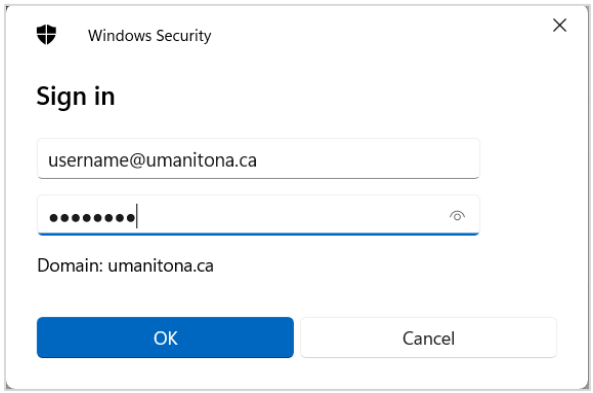
4. Select **Edit** next to Authentication settings. The Ethernet authentication settings window opens.



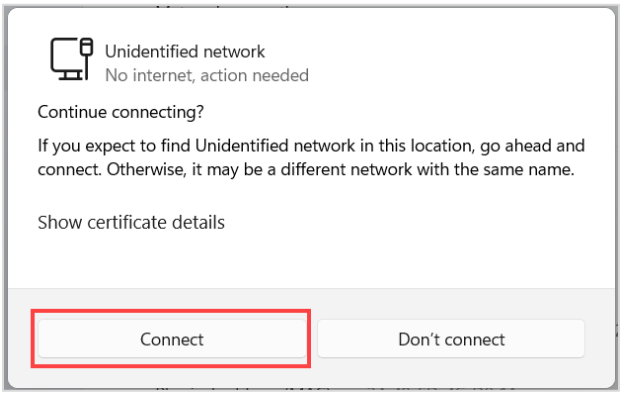
5. In Ethernet authentication settings:
   a. Toggle IEEE 802.1X authentication to **On**.
   b. Under WAP method, select **Protected EAP (PEAP)**.
   c. Under Authentication method, select **Secured password (EAP-MSCHAP v2)**.
   d. Select **Save**.



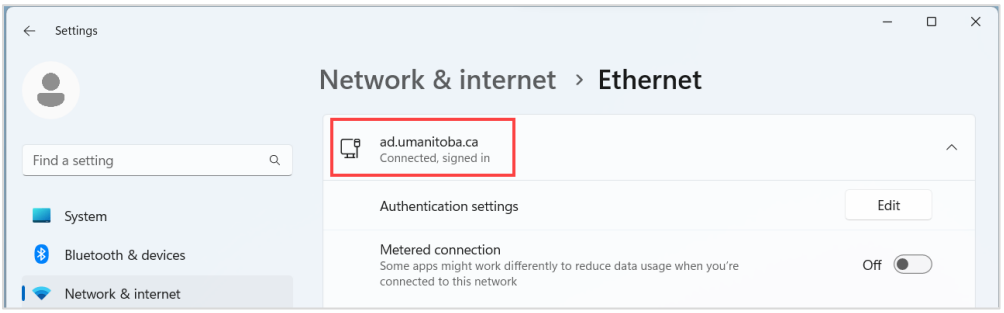
6. In the **Sign in** pop-up window, enter your UM email (umanitoba.ca or myumanitoba.ca) account and password, and select **OK**.



7. Select **Connect** to accept the certificate.



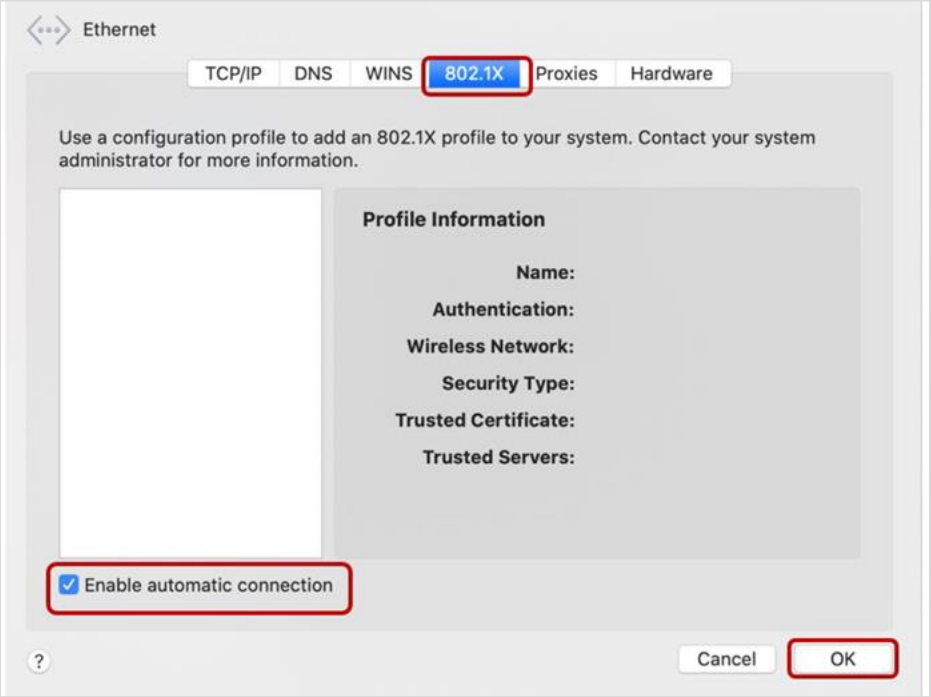
8. In your **Ethernet settings** window, you will now see the ad.umanitoba.ca domain listed as *Connected, signed in*.



macOS 12 or later

How to configure the 802.1x client on your macOS 12 or later computer.

1. Go to **Apple menu** > **System Settings**, then select the **Network icon** in the sidebar (You may need to scroll down.).
2. Select the network service you want to use, then click **Details...**.
3. Select **802.1X**.
4. Select the profile you want to view or connect to.
5. If you want to connect to the 802.1x network automatically every time, turn on **Enable automatic connection** and click **OK**.

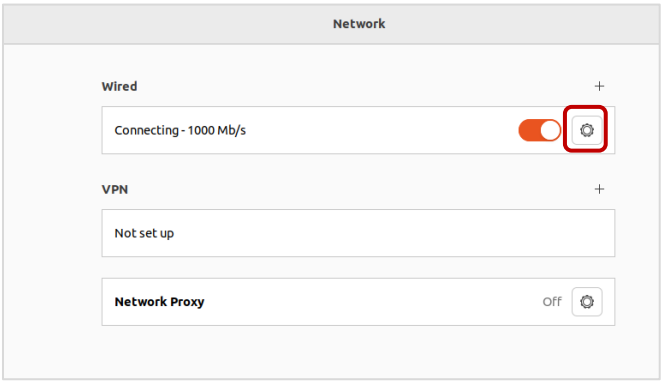


Linux Ubuntu and Fedora

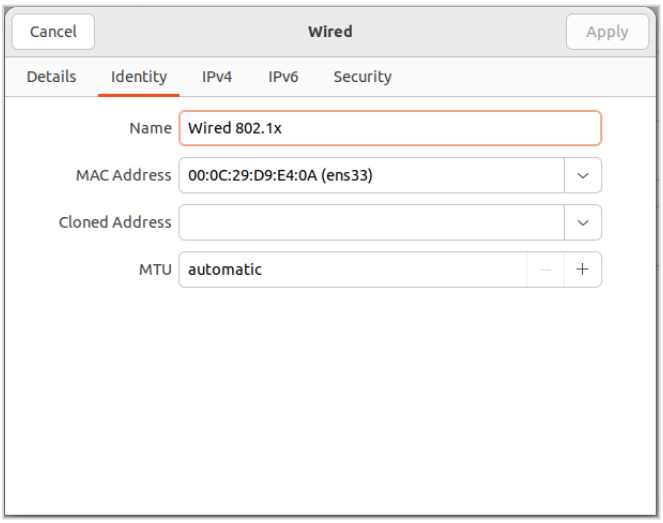
How to configure the 802.1x client on your Linux workstation.

802.1x client setup using the graphical user interface (GUI)

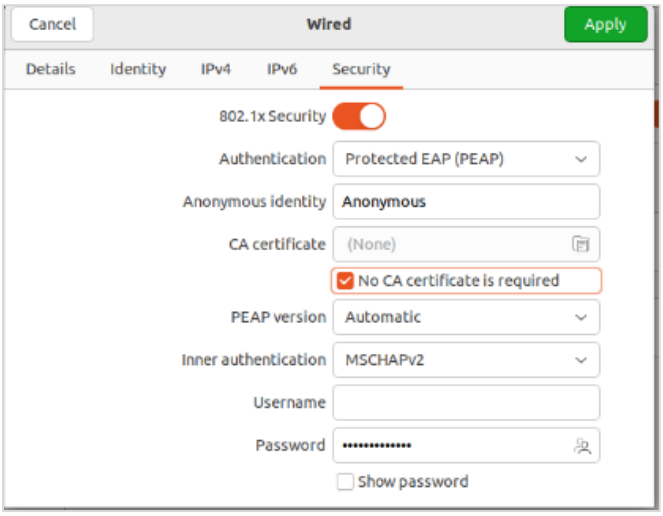
1. Open **Network Settings** and click the gear icon.



2. In the **Identity** tab, name your profile. For example, “Wired 802.1x.”



3. Under the **Security** tab:
   a. Enable 802.1x Security.
   b. Check **No CA certificate is required** and enter your *UMNetID (staff)* or *myumanitoba.ca email address (students)* and *password*.



4. Click **Apply**.

802.1x client setup using the command line interface (CLI)

Set up a connection profile (client) under: /etc/NetworkManager/system-connections.

1. With your CLI text editor, create a new file:

   a. sudo nano Profile.nmconnection (Ubuntu) or sudo vi Profile.nmconnection (Fedora)
   b. Copy/adjust the required fields. See *Table 1* below.

Table 1

Ubuntu	Fedora
[connection] id=Profile uuid=bb6fce4a-1539-4c98-849f-82786846af47 type=ethernet timestamp=1677787427 [ethernet] [802-1x] eap=peap; identity=UMNETID@myumanitoba.ca password=PASSWORD phase2-auth=mschapv2 [ipv4] method=auto [ipv6] addr-gen-mode=stable-privacy method=auto [proxy]	[connection] id=Profile 1 uuid=7e756735-1aaa-47f4-87a8-024dd7bdf421 type=ethernet interface-name=ens33 timestamp=1677789571 [ethernet] [802-1x] eap=peap; identity=UMNETID@myumanitoba.ca password=PASSWORD phase2-auth=mschapv2 [ipv4] method=auto [ipv6] addr-gen-mode=default method=auto [proxy]

2. After you have configured the client, restart the NetworkManager service:
    a. sudo service NetworkManager restart
3. If configured correctly, you should acquire a valid IP address from the DHCP server:
    a. Verify with: **ip addr**

2. Connecting to an 802.1x network port

Windows 10

Scenario 1: Using an IST domain-joined[1] computer with 802.1x enabled for the first time

Follow the instructions below if you log in to your Windows 10 computer (desktop or laptop) with your UMNetID and password.

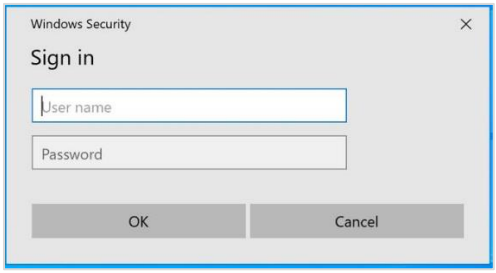
1. Plug your computer into the network outlet on the wall.
2. Turn on the computer (if it is not already on).
3. Log in to Windows with your *UMNetID* and *password*.
4. Select **Connect** to accept the certificate if/when prompted.

Note to IT administrators: When a user logs out of Windows, their workstation will be authenticated via Mac Address By-pass (MAB) or 802.1x using your workstation's MAC address and will stay in the Staff virtual network (VN).

Scenario 2: Using a computer with 802.1x enabled

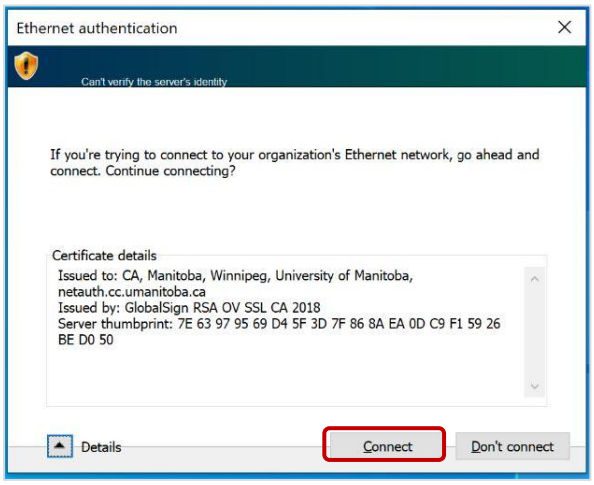
Follow the instructions below if you log in to your Windows 10 computer (desktop or laptop) with a personal account (not a UM account).

1. Plug your computer into the network outlet on the wall.
2. Turn on the computer (if it is not already on).
3. Log in to Windows with your personal *username* and *password*.
4. If the 802.1x client is enabled, you will get an authentication pop-up window.



5. Enter your *UMNetID (staff) or myumanitoba.ca email address (students)* and *password* and select **OK**.
6. Select **Connect** to accept the certificate if/when prompted.

[1] Please contact the IST Service Desk at 204-474-8600 or your IT Administrator if you do not know if you are using an IST domain-joined computer.



macOS 12 or later

Scenario 1: Using a computer with 802.1x enabled

Follow the instructions below if you log in to your macOS computer (desktop or laptop) with a personal account (not a UM account) .

1. Plug your computer into the network outlet on the wall.
2. Tun on the computer.
3. Log in to macOS with your personal *username* and *password*.
4. You will get an authentication pop-up if the 802.1x client is configured and automatic connections are enabled.
5. Enter your *UMNetID (staff)* or *myumanitoba.ca email address (students)* and *password* and select **OK**.

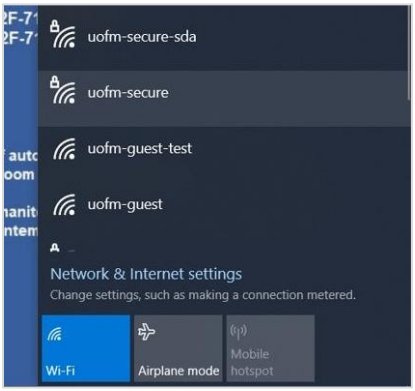
6. Select **Continue** to accept the certificate if/when prompted.

3. Connecting to uofm-secure Wi-Fi

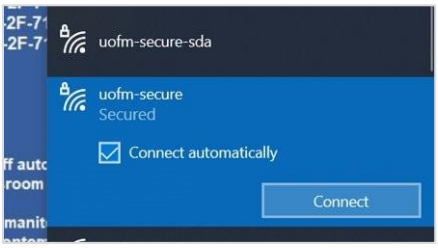
Windows 10 and 11

Connecting to uofm-secure through the wireless SDA network is the same as connecting through the legacy/traditional network.

1. From the available Wi-Fi connections, select **uofm-secure**.



2. Select **Connect**.

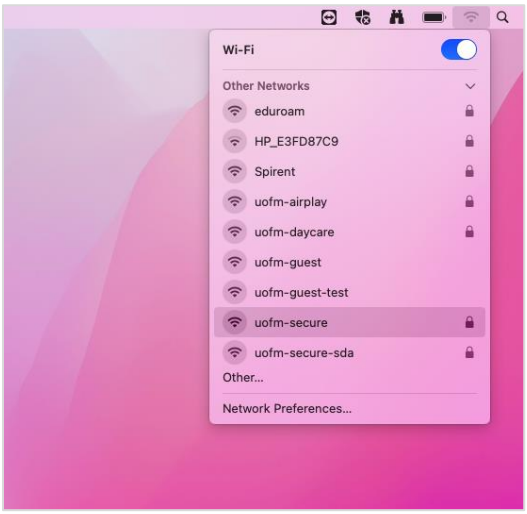


3. Enter your *UMNetID (staff)* or *myumanitoba.ca email address (students)* and *password*.

4. Select **Connect** to accept the certificate if/when prompted.

macOS 12 or later

1. From the available Wi-Fi connections, select **uofm-secure**.



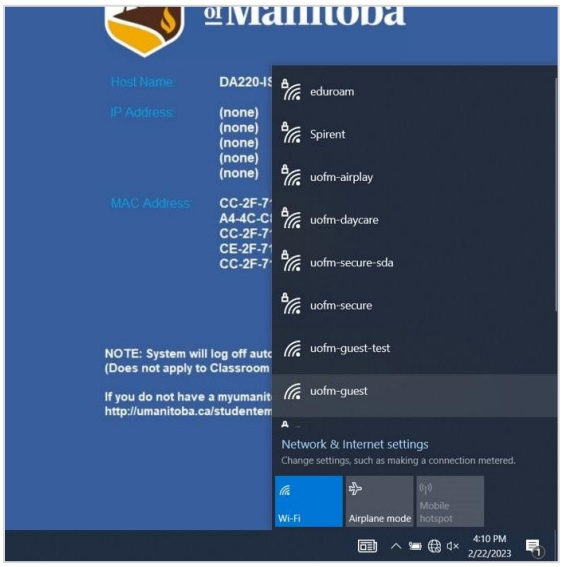
2. Enter your *UMNetID (staff)* or *myumanitoba.ca email address (students)* and password and select **OK**.

3. In the Verify Certificate window, select **Continue** to accept the certificate if/when prompted.

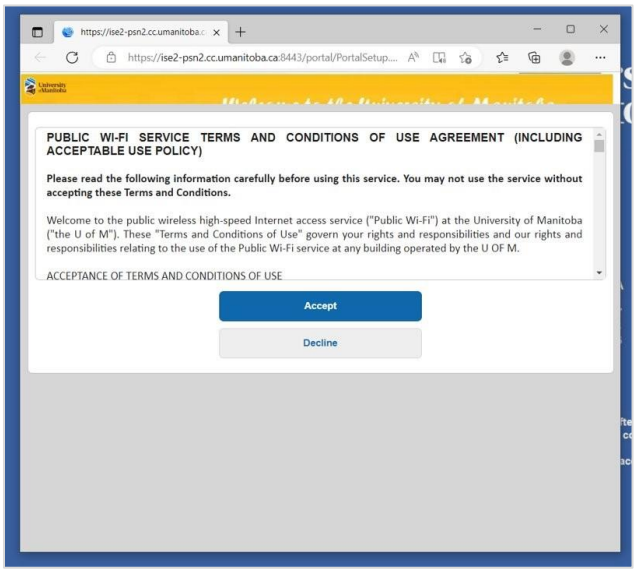
4. Connecting to uofm-guest Wi-Fi

Windows 10 and 11

1. From the available Wi-Fi connections, select **uofm-guest**. A terms and conditions page will pop up in your default web browser.



2. Select **Accept**. Your browser will be redirected to https://umanitoba.ca.

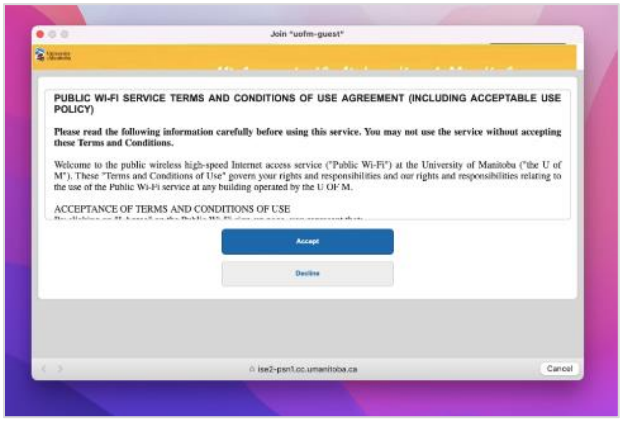

https://ise2-psn2.cc.umanitoba.ca:8443/portal/PortalSetup....
PUBLIC WI-FI SERVICE TERMS AND CONDITIONS OF USE AGREEMENT (INCLUDING ACCEPTABLE USE POLICY)
Please read the following information carefully before using this service. You may not use the service without accepting these Terms and Conditions.
Welcome to the public wireless high-speed Internet access service ("Public Wi-Fi") at the University of Manitoba ("the U of M"). These "Terms and Conditions of Use" govern your rights and responsibilities and our rights and responsibilities relating to the use of the Public Wi-Fi service at any building operated by the U OF M.
ACCEPTANCE OF TERMS AND CONDITIONS OF USE
Accept
Decline

macOS

1. Select the **Wi-Fi icon** in your menu bar and enable Wi-Fi if it is not already on.

2. From the available Wi-Fi connections, select **uofm-guest**. A terms and conditions page will pop up in your default browser.

3. Select **Accept**. Your browser will be redirected to https://umanitoba.ca.



4. Double-check your connection status by clicking on the Wi-Fi icon in the menu bar.