Wireless Setup for macOS (eduroam)

> ⚠️ **Note**
>
> Joining the **eduroam** wireless network requires you to meet either one of the two conditions below...
>
> - You have a UCCS username and password (because you are are a student, faculty or staff)
>   .... or ....
> - You have an account through your institution, which is a participating institution with eduroam
>
> If neither of the above apply to you, please visit the UCCS-Guest information page for information regarding guest wireless access.

Step 1: Opening Network Connections

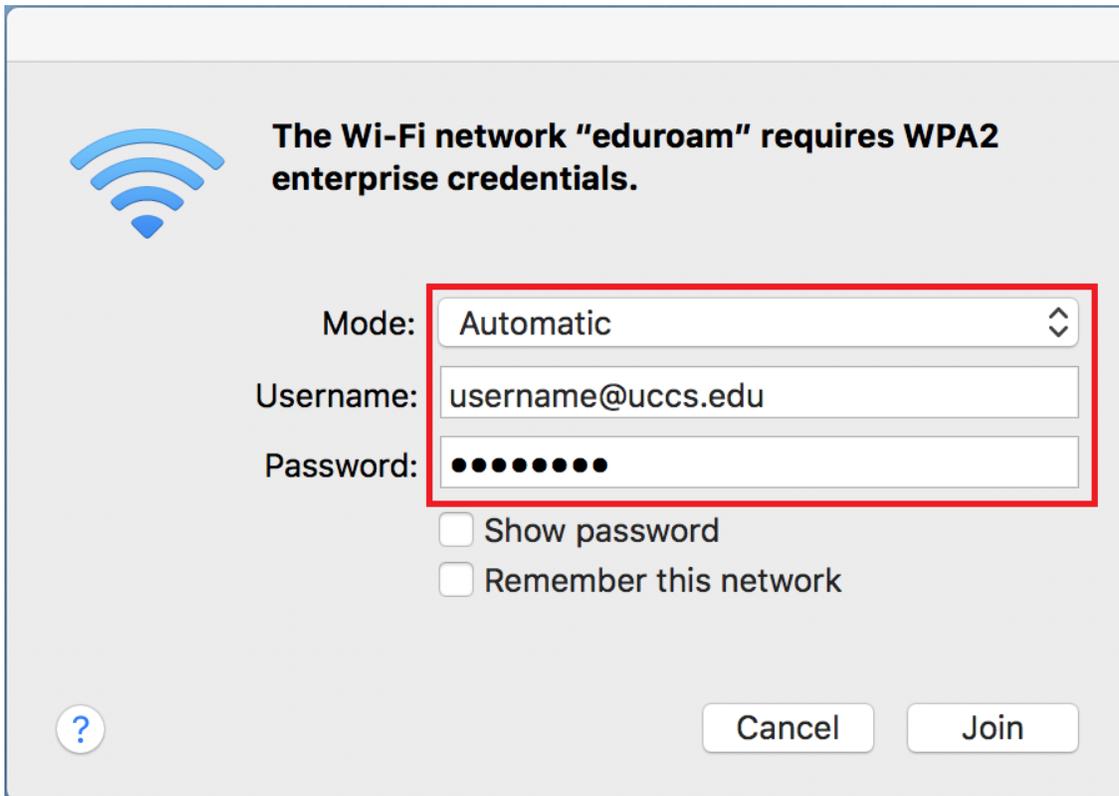Click the **wireless networking** icon, then make sure that it says **Turn Wifi Off**.

Step 2: Select eduroam
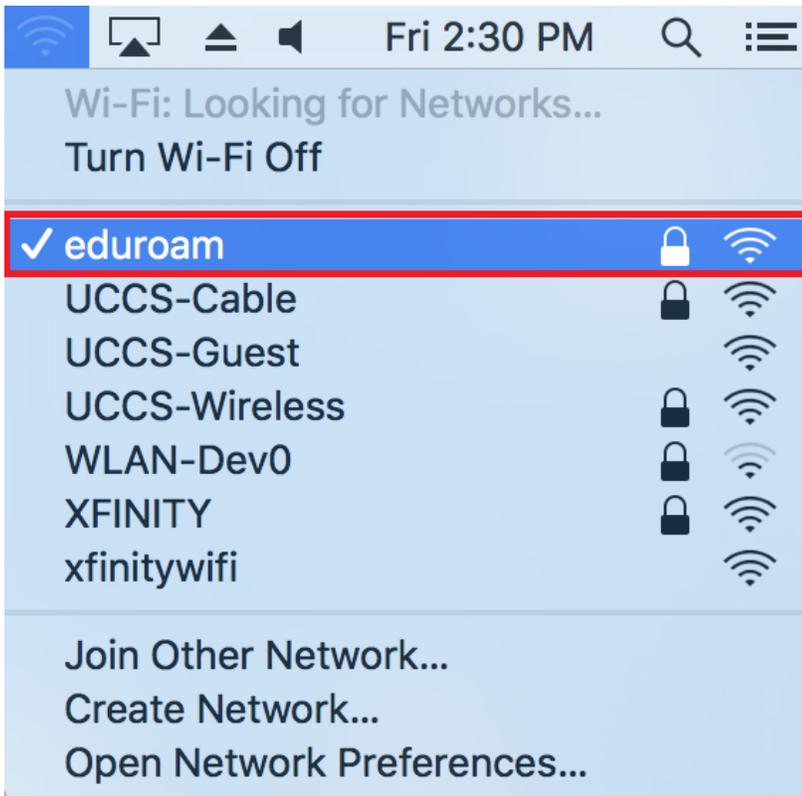
Step 3: Entering credentials

Enter your full domain UCCS username and password, then click **Join**.

Your username must be in the form **username@uccs.edu** (it must have "@uccs.edu" on the end)

Step 4: Review security certificate

You should see a screen similar to the following asking you to verify and accept the server's security certificate. The server "cppm.uccs.edu" is the server you are authenticated against.

To be safe you should always validate the certificate you are about to trust. To validate and see more information about the certificate, click **Show Certificate**.

Our certificate is issued by Comodo RSA Certificate Authority.
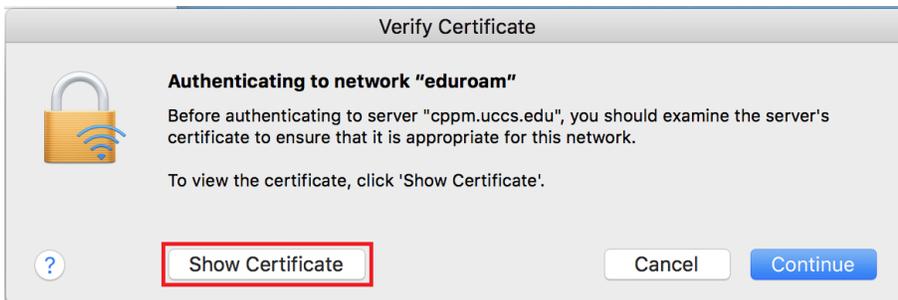
Expand the Details by clicking the **small triangle**, and you should see more details about the certificate as seen below.

Verify Certificate

Authenticating to network "eduroam"

Before authenticating to server "cppm.uccs.edu", you should examine the server's certificate to ensure that it is appropriate for this network.

To view the certificate, click 'Show Certificate'.

☑ Always trust "cppm.uccs.edu"

📁 COMODO RSA Certification Authority
  ↳ 📄 COMODO RSA Organization Validation Secure Server CA
    ↳ 📁 cppm.uccs.edu

Critical	NO
URI	http://crl.comodoca.com/COMODORSAOrganizationValidationSecureServerCA.crl
Extension	Embedded Signed Certificate Timestamp List (1.3.6.1.4.1.11129.2.4.2)
Critical	NO
Data	04 82 01 67 01 65 00 75 ...
Extension	Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical	NO
Method #1	CA Issuers (1.3.6.1.5.5.7.48.2)
URI	http://crt.comodoca.com/COMODORSAOrganizationValidationSecureServerCA.crt
Method #2	Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
URI	http://ocsp.comodoca.com

Fingerprints
SHA-256 0A 1E 26 F8 15 59 C8 68 6A 40 0A 00 18 EF 41 F1 D1 75 67 EC 18 03 22 1A 3A 35 2B 8E 94 00 2C F3
SHA-1 A7 D6 D8 4D FB 1F AC E7 B6 1F CD 59 A8 9A D7 03 77 A9 F8 09

? [Hide Certificate]   [Cancel] [Continue]

Scroll down until you see the Fingerprint section. Your certificate fingerprints should match the fingerprints outlined below:

ⓘ **CPPM Certificate Fingerprints (SHA-256 and SHA-1)**

SHA-256: 24 96 3E 77 CA 8C 98 AA 36 4B 07 C0 D6 63 16 7B 40 3A 68 BC 72 C2 7F 57 0C A1 E2 85 BB 8F E1 F3

SHA-1: 7F EF D3 17 14 12 50 59 1B B9 C0 CA D7 D6 C6 CC FB D6 03 45

If the fingerprints do not match, DO NOT trust the certificate! Click CANCEL and contact the OIT Helpdesk.

Step 6: Accept the security certificate

If your certificate fingerprints match those listed above, you can trust the certificate is valid. Click **Continue**.

Your computer may then prompt you for your username and password to allow your computer to store the newly trusted certificate.
If prompted, enter your credentials and click "Update Settings."
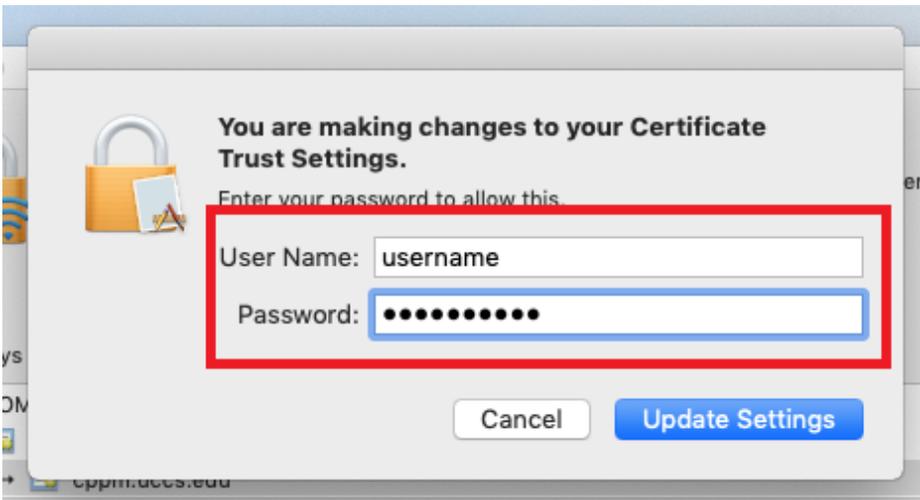
Step 7: Finished - Your device should now be connected to **eduroam.**