eduroam Service

Overview
eduroam (education roaming) is the secure worldwide-federated network access service developed for the international research and education community.

Tufts University is now subscribed to the eduroam service. While travelling and visiting at a participating institution, Tufts colleagues may now get access to the local institutions network and internet by simply entering their Tufts Username and Tufts Password.

eduroam provides per-user, per-session encrypted network access for visitors from participating institutions, without the need to gain guest credentials on arrival to an eduroam enabled location. The connectivity is instantaneous and the infrastructure is authenticated by the user. Study abroad students, faculty and staff can join thousands of eduroam hotspots without any hassle or additional data charges. Depending on local policies at the visited institutions, eduroam participants may also have additional resources (for example printers) at their disposal.

Availability
eduroam is available at many participating institutions around the world.

There is an International service locator at https://www.eduroam.org/?p=where

There is a U.S.A service locator at https://www.eduroam.us/eduroam_us_institutions

How to Connect
To connect to eduroam:

1. While on campus at the participating institution, select “eduroam” from the list of available networks.

2. Sign in by entering your Tufts Username in the form of tufts-username@tufts.edu (e.g. jsmith01@tufts.edu).

   It is important to note the format of the eduroam login user name is different than your usual Tufts email address (e.g. john.smith@tufts.edu). The format requires the input of the Tufts Username followed by @tufts.edu (e.g. jsmith01@tufts.edu). This is not the same format used as the Tufts user’s email address.

3. Enter your Tufts Password to complete login.

Additional Connectivity Information
In order to connect to eduroam, the network adapter must support WPA2 and MSCHAPv2. The user will also need to enter their Tufts Username and Tufts Password when prompted for a user name and password.
Connectivity information:

In order to connect to eduroam, your network adapter must support, WPA2 and MSCHAPv2. The user will also need to enter their Tufts Username and Tufts Password when prompted for a user name and password.

<table>
<thead>
<tr>
<th>Client Configuration Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Name (SSID)</td>
</tr>
<tr>
<td>Security Type</td>
</tr>
<tr>
<td>Encryption Type</td>
</tr>
<tr>
<td>Authentication Method</td>
</tr>
<tr>
<td>Inner Authentication Method</td>
</tr>
<tr>
<td>802.1x Setting - Authentication Mode</td>
</tr>
</tbody>
</table>

Further Information about device requirements:

https://confluence.terena.org/display/H2eduroam/endusers

How it works:
eduroam infrastructure:

• eduroam technology is based on 802.1X standard and a hierarchy of RADIUS proxy servers.

• The role of the RADIUS hierarchy is to forward the users' credentials to the users' home institution, where they can be verified and validated.

• When a user requests authentication, the user's realm determines where the request is routed to. The realm is the suffix of the user-name, delimited with '@', and is derived from the organization's DNS domain name.

• Every institution (i.e. university or equivalent) that wants to participate in eduroam connects its institutional RADIUS-server to the national top-level RADIUS (NTLR) server of the country where the institution is located.

• The NTLR is normally operated by the National Research and Education Network (NREN) of that country. These country-level servers have a complete list of the participating eduroam institutions in that country. This is sufficient to guarantee national roaming.

• For international roaming, a regional top-level RADIUS server is needed in order to roam the users request to the right country. Currently there are two main regions where eduroam is deployed: Europe and Asia-Pacific.

• In the case of Europe the top-level RADIUS server (ETLR) are operated by the Dutch NREN (SURFnet) and the Danish NREN (UNI-C).

• In the case of Asia-Pacific, the top-level RADIUS server (APTLR) is operated by the Australian NREN (AARNet) and by the University of Hong Kong
Logical Depiction

Support

- TechConnect
- it@tufts.edu
- TTS Service Desk: 617-627-3376

Related Links

https://it.tufts.edu/eduroam
https://www.eduroam.org/ (main service page)
https://www.eduroam.us/faq
http://www.eduroamus.org/introduction
http://www.internet2.edu/products-services/cloud-services-applications/eduroam/
Sample Client Setup

Getting connected to eduroam in Windows

• Right click on the wireless icon in the bottom right hand corner of your screen and select "View wireless networks". The Wireless Network Connection window will show which wireless networks are available.

• Click "Change the order of preferred networks" to display the Wireless Network Connection Properties window.
If the wireless network "eduroam" already exists in the "Preferred Networks" box, select it and click "Properties." If it does not appear click "Add."

- Set Network name (SSID) to "eduroam".
- Set Network Authentication to "WPA2".
- Set Data encryption to "AES".
- DO NOT click OK, but now select the "Authentication" tab.

- The option to "Enable IEEE 802.1x authentication" will be ticked but greyed out.
- Select "ProtectedEAP (PEAP)" from the list of EAP types.
- Deselect BOTH "Authenticate as computer" and "Authenticate as guest".
- Click "Properties".
• Ensure "Validate server certificate" is selected.
• Scroll down the list of Trusted Root Certificate Authorities and select "Thawte Premium Server CA" and "thawte Primary Root CA".
• Select "Secured password (EAP-MSCHAP v2)" from the list of Authentication methods.
• Ensure that "Enable Fast Reconnect" is NOT selected.
• Click "Configure".

• Ensure "Automatically use my Windows logon name" is NOT selected.
• Click "OK" to close the "EAP MSCHAPv2 Properties" window.
• Click "OK" to close the "Protected EAP Properties" window.
• Click "OK" to close the "Wireless Network Connection Properties" window.
• User name: Enter your username as your Tufts Username ID plus "@tufts.edu", e.g. "jsmith01@tufts.edu".
• Password: Enter the password that you specified when you registered for your Tufts Username (same as email password).
• Logon domain: Leave the "Logon domain" field blank.
• Click "OK".

Your device should now authenticate and, if successful, connect to the eduroam secure wireless network.

If you see the following box, click "ok" to continue and you should be able to continue to the eduroam network:

The first time you attempt to connect to the eduroam secure wireless network, a balloon-tip will appear in the Windows system tray prompting you to "Select a certificate or other credentials". Click in this balloon to display the "Enter Credentials" login window.
Additional eduroam FAQ


What is eduroam?

- eduroam (education roaming) allows users (researchers, teachers, students, staff) from participating institutions to securely access the Internet from any eduroam-enabled institution. The eduroam principle is based on the fact that the user's authentication is done by the user's home institution, whereas the authorisation decision allowing access to the network resources is done by the visited network.

I am a student / researcher / professor, can I use eduroam?

- As end-user you will only be able to use eduroam if your offers eduroam service. You will need to have a valid Tufts UTLN and password in order to user this service at the remote site.

What does eduroam cost?

- eduroam is free for its users, there is no charge for eduroam use world-wide. The providers of eduroam hotspots make the service available to benefit all members of the research and education community.

Can a public WiFi provider offer eduroam?

- eduroam separates the concepts of authentication (identity providers) and hotspots (service providers) allowing public, commercial or city wifi initiatives to offer eduroam in addition to research and education institutions.

    What commercial entities cannot do is become identity providers and offer a service to their customers that will work with eduroam. so any partnership with a commercial wifi service needs to respect that users of this hotspot cannot be charged for accessing the network.

How does the institution connect to and offer eduroam service?

- Your institution must be part of an eduroam service, which is provided by your National Roaming Operator (in most cases your National Research and Education Network (NREN)).

    The NREN in your country must participate in eduroam. To find out more about the NREN in your country please refer to the eduroam map. Your NREN representative will be able to inform you about the formal rules for participation.
**How does eduroam work?**

- When a user tries to log on to the wireless network of a visited eduroam-enabled institution, the user's authentication request is sent to the user's home institution. This is done via a hierarchical system of RADIUS servers. The user's home institution verifies the user's credentials and sends to the visited institution (via the RADIUS servers) the result of such a verification.

**What technology does eduroam use?**

- In eduroam, communication between the access point and the user's home institution is based on IEEE 802.1X standard; 802.1X encompasses the use of EAP, the Extensible Authentication Protocol, which allows for different authentication methods. Depending on the type of EAP method used, either a secure tunnel will be established from the user’s computer to his home institution through which the actual authentication information (username/password etc.) will be carried (EAP-TTLS or PEAP), or mutual authentication by public X.509 certificates, which is not vulnerable to eavesdropping, will be used (EAP-TLS).

**Is eduroam safe to use?**

- eduroam is based on the most secure encryption and authentication standards in existence today. Its security far exceeds typical commercial hotspots. Be aware though that when using the general Internet at an eduroam hotspot, the local site security measures at that hotspot will apply to you as well. For example, the firewall settings at the visited place may be different from those you are used to at home, and as a guest you may have access to fewer services on the Internet than you have at home.

**Does eduroam use a captive portal for authentication?**

- No. Web Portal, Captive Portal or Splash-Screen based authentication mechanisms are not a secure way of accepting eduroam credentials, even if the website is protected by an HTTPS secure connection. The distributed nature of eduroam would mean that many different pages, languages and layouts would be presented to eduroam users making it impossible to distinguish between legitimate and bogus sites (even a consistent layout can be mimicked by an adversary).

eduroam requires the use of 802.1X which provides end-to-end encryption to ensure that your private user credentials are only available to your home institution. The certificate of your home institution is the only point you need to trust regardless of who operates any intermediate infrastructure. Web portals require you to trust their infrastructure as they receive your password in clear text, this breaks the end-to-end encryption tenets of eduroam.
Does eduroam work on different platforms?

- eduroam uses open standards to enable cross platform uniform access. This means that eduroam works on Windows, Linux, MAC OS, and even Windows CE and many mobile devices.