# The Wireless Networks at MIT

## The Wireless Networks at MIT

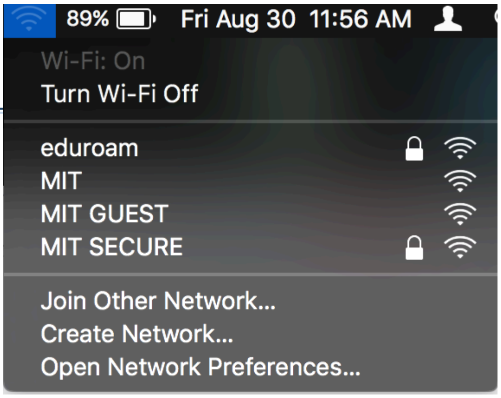
On this page:

- Overview
- Tips
- MIT Community
  - What you need to know:
- Guests, Visitors, and older hardware
  - What you need to know:
- eduroam
  - What you need to know:
- MIT
- SECURE vs. non-SECURE networks
- FAQ
  - How do I know the RADIUS server used by the wireless network to authenticate my password is legitimate?
  - Can I move from place to place while keeping my wireless connection?
  - Can I connect other wireless devices to the network, such as wireless printers or game consoles?
  - Can I use my own wireless access point?
  - How do I know if my wireless devices has a WiFi-certified adapter?
- Troubleshooting wireless connections
  - Poor Signal Areas
  - Short term vs. Long term problems
- See Also:

## Overview

MIT has an ubiquitous wireless network installation in all academic, administrative, and residential buildings including FSILG housing.

## Tips



- Make sure your device has the latest wireless device drivers and software installed. Many bugs have been fixed recently including the security vulnerability KRACK. The infrastructure is now running the latest software, so client devices should be as well for optimal performance.
- Delete/Forget the other MIT wireless networks a device knows about. i.e. Don't have both "MIT SECURE" and "MIT" (and/or "MIT GUEST") configured on a device. Only have one of those networks configured.
- If you are having difficulties connecting in an area where others are connected, try temporarily disabling (and then re-enabling) WiFi on your device. A reboot may also help.

## MIT Community

**MIT SECURE**
This is the preferred wireless network for members of the MIT community (students, faculty, staff, and affiliates). It provides an unrestricted, fast, reliable, and encrypted connection to the MIT network, the Internet, and internal resources. Use your MIT Kerberos username and password to login.

### What you need to know:

- Security method is WPA2-Enterprise (802.1x) with PEAP (MSCHAPv2) authentication and TLS encryption.
- Devices must support WPA2-Enterprise level encryption to connect. (See the list.)
- Network supports devices using 802.11 wireless specifications 802.11a/b/g/n/ac.

- Requires an active MIT Kerberos account - Use your kerberos username and password to authenticate (i.e. login).
- How do I connect to MIT SECURE wireless?
- **IMPORTANT:** We strongly recommend using a password that is less than one year old.
  Reset your kerberos password here.

## Guests, Visitors, and older hardware

**MIT GUEST**
Wireless connections for guests and visitors of MIT. Visitors connecting this network will be required to provide an e-mail address or mobile phone number to access the network. Guest users that do not have access to SMS/text messaging or e-mail (e.g. international travelers without data roaming) can use the "Request Access from Sponsor" option and enter their sponsor's MIT e-mail address.

This network is not encrypted, has limited access to the Internet, and is not intended for access to MIT internal resources. Learn more about the MIT GUEST wireless network.

### What you need to know:

- Available for guests and visitors of MIT
- Use for devices that do not support WPA2 encryption (See the list.)
- Use for operating systems that do not have WPA supplicants
- Use for older 802.11b hardware
- Not intended for long-term use
- Limited access to the Internet.

The MIT GUEST network is separated from the rest of the MIT network with a firewall and network address translation (NAT). This limits the services that will work over this wireless network. For instance, printing to printers over TCP port 631 (CUPS) will not work.

## eduroam

**eduroam**
This is an alternative wireless network for both members of the MIT community (students, faculty, staff, and affiliates) as well as visiting students, faculty, and staff from other higher education schools. After authenticating, MIT community members will simply be placed onto the same underlying encrypted network used by MIT SECURE while visitors will be connected to the underlying network used by MIT GUEST (however, unlike MIT GUEST, authenticated visitors will have an encrypted connection).

### What you need to know:

- Available to both MIT community members and visitors from other higher education schools participating in the global eduroam network.
- Login using your username and your school's domain name
  - MIT community members: "username@mit.edu"
  - Visitors: "username@harvard.edu", "username@yale.edu"

NOTE: MIT community members can use the same login convention while visiting other schools to connect to their "eduroam" wireless networks.

## MIT

**MIT**

The preferred network for user devices is "MIT SECURE". However, the "MIT" wireless network is available for devices that do not support WPA2-Enterise (802.1X) and can only authenticate using a PSK (Wi-Fi password). MIT (and Alumni) users can obtain a *personal* PSK for their personal devices via the Wi-Fi Onboarding Portal.

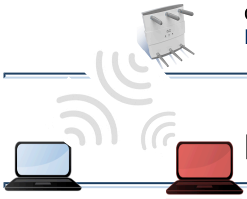
Note: Shared devices, **NOT** owned by or assigned to an individual user, may authenticate via a *generic* PSK - obtained by request via this form (Touchstone login required) by the DLC that owns the device. Examples of devices eligible for a generic PSK include: public kiosks, signage, lounge/classroom wall clocks, shared smart appliances, etc. (NOT personal devices)

## SECURE vs. non-SECURE networks

IS&T recommends MIT community members always use MIT SECURE. Use of the MIT or MIT GUEST networks will leave you vulnerable to **session hijacking**.

> **Session Hijacking:** Open wireless networks, including the MIT, MIT GUEST, and public wireless networks found in cafes and other shops, that do not require WPA or better encryption are susceptible to session hijacking attacks. If

connecting to an encrypted wireless network (such as "MIT SECURE") is not possible, IS&T recommends using the MIT Remote Access VPN to ensure your data remains secure and private.



## FAQ

### How do I know the RADIUS server used by the wireless network to authenticate my password is legitimate?

The RADIUS server will present a certificate (i.e. an ID). It is important to verify that the server name, as well as the certificate signing authority, match the expected value *before* entering your password.

If they do not match, do not continue to connect, and contact the IS&T Service Desk. Cyber criminals may attempt "man-in-the-middle" attacks by creating fraudulent wireless networks made to look like "MIT SECURE" or "eduroam". However, fraudulent networks won't present the correct certificate(s). You can verify the correct certificates by looking at the certificate's fingerprints.

### Can I move from place to place while keeping my wireless connection?

You should be able to move from place to place around campus without losing your wireless connection. You will lose your network connection when you move out of range of wireless, such as if you exit a building. When you arrive at another building with wireless access, your computer should try to reconnect to MIT SECURE. You may need to restart your network applications.

### Can I connect other wireless devices to the network, such as wireless printers or game consoles?

These devices must be connected via the MIT GUEST network. See which popular devices can and can't connect to MIT SECURE.

### Can I use my own wireless access point?

Use of switches, hubs, and routers (typically integrated into private access points) as well as creating a back-end network are not allowed under MITnet's policies. Although broadcasting a wireless network signal is not explicitly forbidden, personal access points can interfere and will be removed from the MIT network.

All MIT buildings should have ubiquitous wireless coverage and IS&T prohibits connecting personal or private access points to the MIT network. 802.11 wireless traffic is sent on a relatively small range of radio frequencies. Adding additional APs that are not connected, configured, and optimized to integrate with the MIT wireless installation can and will interfere with the current setup, causing signal degradation, loss of throughput, and connectivity issues for those users nearby.

### How do I know if my wireless devices has a WiFi-certified adapter?

Check the WiFi Alliance list of certified devices and adapters or refer to your device's documentation or specification

## Troubleshooting wireless connections

Please see the article on Troubleshooting your Wireless connection . If the steps do not prove useful, please contact the IS&T Service Desk.

### Poor Signal Areas

There are over 7,000 wireless access points that MIT has installed around campus. Because of the scale of this deployment, there are bound to be areas on campus that are in need of fine tuning, AP adjustment, and additional hardware. If you are in an area with poor or no wireless coverage, please read the troubleshooting tips in the article above and fill out a help request with the IS&T Service Desk.

### Short term vs. Long term problems

Often, wireless access points can be affected by the environment around them. Heat and overuse can cause them to operate incorrectly or incompletely. This type of outage is different from an interference or signal coverage issue and has a different procedure for resolution. It is important to indicate how long you've been noticing problems and how the current behavior differs from the expected behavior.

## See Also:

The Wireless Networks at MIT
How to connect to the MIT SECURE wireless network
Eduroam Landing Page
The MIT GUEST wireless network
Wireless RADIUS Server Certificate Fingerprints
Troubleshooting and reporting problems on the MIT wireless network
List of devices that can or can't connect to MIT SECURE