The Wireless Networks at MIT

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 also should be for optimal performance.

- Delete/Forget the other wireless networks a device knows about. i.e. Don’t have both "MIT" and "MIT SECURE" configured on a device or "MIT GUEST" when either of the others is configured. Only have one of those networks configured.

Recommended

**MIT SECURE**
This is the preferred wireless network for members of the MIT community, including 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.

**EDUROAM**
This is a recommended alternative wireless network (to MIT SECURE) for members of the MIT community, including 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 with "@MIT.EDU" and password to login. For visitors from other Eduroam participants, authentication is using the username and password for the user's home network, e.g. joeuser@yale.edu as the username.

What you need to know:

- The security method is WPA2 Enterprise with PEAP (MSCHAPv2) authentication and TLS encryption.
- Use for devices that support WPA2 Enterprise level encryption. (See the list.)
- Requires devices with 802.11g specification or better (802.11a/b/g/n/ac)
- Requires an active Kerberos account
- **IMPORTANT:** Requires an MIT kerberos username and password. We strongly recommend using a password that is less than one year old.
  Reset your kerberos password here.

Connect to and Log On

The MIT SECURE wireless network requires an MIT Kerberos username and password to log on. For instructions or help with connecting to the Secure wireless networks, please see: How do I connect to MIT SECURE wireless?

For MIT Guests, Visitors and older hardware

**MIT GUEST**
Wireless Connections for guests and visitors of MIT are also available through the MIT GUEST wireless network. This network does not require authentication, 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:
Use for guests or visitors of MIT
Use for devices that do not support WPA2 Enterprise 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 and has limited access to the MIT network and 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 the MIT GUEST network. For instance: printing to Athena cluster printers over TCP/IP port 631 (CUPS) will not work.

Retirement of MIT

The open wireless network MIT will eventually be phased out. The reason for this is that connections to these networks are unencrypted, putting data at risk. Although these networks are currently still available, IS&T does not recommend connecting to these networks. If you have one of these networks set up as your primary wireless network, please follow the instructions to connect to MIT SECURE.

What you need to know:

- Retiring on date to be determined
- Not encrypted and does not require authentication

SECURE vs. non-SECURE networks

IS&T recommends to 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 is not possible, IS&T recommends using the MIT VPN to ensure your data remains secure and private.

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

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

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.
Troubleshooting my wireless connection

Please see the article on Troubleshooting your Wireless connection. If these steps do not prove useful, please contact the IS&T Helpdesk for main campus buildings, or file a help request with the Residential Computing Consultants for dorms.

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 Helpdesk.

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
Troubleshooting and reporting problems on the MIT wireless network
List of devices that can or can't connect to MIT SECURE