The MIT GUEST Wireless Network

Intended Audience and Use

This network does not require authentication and is not encrypted. The network is provided for visitors and short-term guests and has limited access to the Internet and MIT resources. The MIT GUEST network is not intended for long-term use. For example, MIT GUEST should be used by summer program or conference attendees as well as non-student or non-faculty residents.

Limited Access

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 network. For instance: printing to Athena cluster printers over TCP/IP port 631 (CUPS) will not work. See the list of blocked and allowed ports on MIT GUEST.

Wireless Non-Computers

While MIT GUEST can be used for wireless devices, such as gaming consoles, that do not support the security protocols required to connect to the MIT SECURE wireless network, wired connections are usually better, if available, for your device. See which popular devices can and can’t connect to MIT SECURE.

How to Connect

It is easy to connect to the MIT GUEST wireless network with a wireless device. Since there are no restrictions to connecting, your device should be able to “see” the network as one of the open wireless options and connect instantly. If your device can not see the network, contact the IS&T Service Desk for assistance.

Wired Connection for Guests

If the wireless network is not available in your area of campus, you will need a wired network connection. Learn more.

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