

Guest Wireless Network Frequently Asked Questions

What is the guest wireless network?

The guest wireless network provides laboratory guests and visitors access to the wireless network while on campus for limited use for things such as web browsing, email and basic communications needs.

How do I access the guest wireless network?

To use the guest wireless network, select the “guest” SSID from a wireless device. Once connected to the guest network open up a web browser. You will then be redirected to the guest registration form. Fill out your contact information and agree to the terms of service.

How long does guest access last?

You will be redirected to the guest registration page after registration expires at midnight each day. On subsequent days, complete the registration form again and confirm your agreement to the terms of service. You will then be granted network access again until midnight. There is no limit to the number of days that you can use the guest wireless network.

Is there a limit to the number of devices I can use on the guest wireless network?

No. There is no limit to the number of devices you can use on the guest wireless network.

Does the guest wireless network require pre-authorization, a user account or an encryption key?

No preauthorization, user account or encryption keys are required to use the guest wireless network. Upon connecting to the guest wireless network, SSID “guest”, you will be prompted to enter your contact information and agree to the terms of service.

Why are some web sites blocked on the guest wireless network?

Access to web sites that meet certain criteria are blocked to help prevent virus infections and to assist users in following the Fermilab Policy on Computing.

Why are some applications (such as peer-to-peer file sharing) blocked on the guest wireless network?

The network is intended for limited use to provide web browsing, email and basic communications needs for guests and visitors while they are on campus. It is not intended to provide other Internet-based services such as transfers of audio files, video files and large datasets.

There is a web site or an application that is blocked on the guest wireless network that I believe should be allowed. Who should I contact?

First, please remember that the network is intended for limited use by campus guests and visitors only. If you are unable to perform your work using the network, you should consider using the main “fgz” wireless network from a registered machine. Otherwise, you can direct concerns regarding the security policy of the guest wireless network to the service desk at <https://servicedesk.fnal.gov>, 630-840-2345.

I work at Fermilab. Should I use the guest wireless network for any of my devices?

No. Please register all devices, including personal property, and use the main “fgz” wireless network. To permanently register your device, visit http://appora.fnal.gov/pls/default/node_registration.html

Can I use the Fermilab Virtual Private Network Service from the guest wireless network to access internal Fermilab resources?

Yes, but you do not need to. Since you have a Fermilab VPN account, you do not need to use the guest network. Instead please register your device and use the main “fgz” wireless network. To permanently register your device, visit http://appora.fnal.gov/pls/default/node_registration.html

What is the IP address range of the guest wireless network?

The IP address range is outside of the normal Fermilab IP block. This address range is subject to change, so please do not attempt to hard code it into any device or application.

What are the risks with using the guest wireless network?

Clients who use the guest wireless network run similar risks as when using other wireless networks such as those at restaurants, hotels, and airports. This network is segmented from the other Fermilab networks. As such, lab-wide security protections, such as managed anti-virus services, are not provided. We encourage guests using this network to ensure that their anti-virus protection, operating systems and other software are up to date. Guests who utilize this network do so at their own risk.