

Computer Security

Anyone conducting work at the Laboratory or using the Laboratory's computing resources that require Internet access must register his or her system's hardware or MAC address. To find such, go to URL: <http://www-dcn.fnal.gov/DCG-Docs/mac/> selecting the appropriate O/S.

Visitor computers brought on site may apply for a temporary DHCP address by connecting to the Fermilab network (SSID=fgz) using either a wired (Ethernet) or wireless) connection. Note the system will automatically detect fgz if configured to do so.

After filling out and submitting the Temporary DHCP Address web form, the system will be scanned and must demonstrate the same level of computer security required for all Lab machines. The easiest way to ensure a machine is secure, is to run an O/S update and/or Software update containing current security patches and virus signatures.

There are available Network 'Pix' lines (outside fnal.gov domain) located in the Email Center and in the Service Desk office allowing individuals to connect to the network and download and install critically deemed patches from a vendor or university. This connection will not have internal access to the Fermilab network but will have access to the Internet.

Note that only those critical vulnerabilities identified on the following web page will cause a system to be denied a temporary address:

<http://security.fnal.gov/CriticalVuln/index.html>

Machines with non-critical vulnerabilities (anything not on the above list) will be granted a temporary address and you will receive e-mail notification with instructions describing how to remediate the problem.

DHCP Registration

Temporary Registration

Users of unregistered computers will need to open a web browser and visit any URL to bring up the DHCP registration form. The form asks for some basic contact information and should take only about a minute to fill out. The registration process is described at:

http://computing.fnal.gov/security/registration_dhcp.html

If the system will be at Fermilab for longer than a few days, it must also be registered in the MISCOMP database, as temporary registration will only be allowed for a few days per visit. Permanent registration is accomplished as described below, and should become effective within one to two business days.

Permanent Registration

To apply for permanent registration, complete the form at:

http://appora.fnal.gov/pls/default/node_registration.html

The system name, its IP address (if a permanent assignment has already been made), its built-in hardware address (the so-called “MAC Address”), its location, and the name, e-mail address, and phone number of the individual responsible for this machine are all required. (Computers with multiple network interfaces must register all of the built-in addresses. See <http://www-dcn.fnal.gov/DCG-Docs/mac/> for more information about determining a computer’s built-in MAC address).

To see if your system is already registered, go to:

<http://appora.fnal.gov/misnet/systemName.html>

and enter its node name into the “Any System(s) by Name” query box.

To change information on an already registered machine, go to

http://appora.fnal.gov/pls/default/node_registration.html .

If you need help determining whether the systems you use are registered, contact your General Computer Security Coordinator (GCSC). There is a list of GCSCs at:

<http://computing.fnal.gov/security/#contacts>

Wireless Network

Wireless (802.11b/g) network connectivity is possible in most of Wilson Hall and in the Village User’s Center. Your computer will need to obtain an IP address via the Laboratory’s DHCP service. Please be aware, however, of the restrictions for obtaining IP addresses via DHCP. Although all computers must be registered in order to use the Fermilab network, visitors to the Lab may obtain temporary network access.

This temporary registration expires at midnight each day. The maximum number of days one may login using the temporary registration web page is (9) nine days.

To access the temporary registration form, simply start your web browser and request any web address. Fill in the required identification information. Your computer will then be scanned briefly for vulnerabilities, and an IP address assigned.

You will either need to reboot your computer, or restart your computer’s networking, in order to use the assigned IP address.

If your wireless driver does not successfully connect to the Fermilab 802.11b/g network, try the following configuration settings:

SSID, also known as “Network Name”, “Service Area”, “ESSID”, “WLAN Service Name”:

- Try leaving it blank for auto-detect
- Try the keywords “ANY” or “any” for auto-detect
- Use the keyword “fgz” (*not* “FGZ”)

Network type: Use “Infrastructure Mode” (not “Ad-hoc”)

Preamble mode: Long Tx preamble

Tx mode: 11 MB (“Automatic” will work on some cards, else hardcode to 11 Mb)

DHCP: Enabled

WEP / Encryption: Disabled

WEP Key: WEP is disabled

Radio Channel: Leave blank or set to “auto”

Most common reasons for being blocked

Unix/Linux/MAC users typically get blocked because of an unauthenticated ssh connection. Native ssh and telnet connections are not allowed. One must use ‘kerberized’ ssh or telnet to connect to a Fermilab system.

Also, systems must not allow unauthenticated ssh connections to their systems. Typically, MACs come configured with “Remote Access” checked under the Sharing folder. Other services such as ftp, etc. should also not be selected.

For those systems that have installed ssh, there may be a ssh_config file or an sshd_config file. Contained therein, is a line commented out containing PasswordAuthentication yes. The word “yes” needs to be changed to “no” (minus the quotes).

At startup, to prevent ssh processes from executing, enter the command -

```
/chkconfig --level 0123456 sshd off
```

To stop ssh from running, enter the command –

```
/etc/init.d/sshd stop
```

Note, to enter the above commands, one must be logged in as root.

If you’re running a Windows system and get blocked, either your system’s O/S and/or MS Office does not have the latest critically deemed patches, or attempts were made to connect to another system using a non-kerberized connection. Your local system Administrator or Helpdesk Staff member can assist you with how to establish a secure connection to another system complying with Fermilab’s Computer Security Policy.

What to do if you have been blocked

If it’s been determined that you have been blocked because of a computer security violation indicated from being assigned a 169.xx.xx.xx address or receive email indicating such, you will have to remediate the event by following the web link contained in the email sent you. You may also seek assistance from a member of the Helpdesk Staff.

The Service Desk Office is located on the ground floor of Wilson Hall in the Email Center. You may also call (630) 840-2345 or send email to servicedesk@fnal.gov for assistance. Office hours are Monday – Friday 8 am until 4:30 pm.