OSU Secure

What is OSU_Secure?

OSU_Secure is an option for **Students and Employees** on campus who require data encryption while accessing the internet. It is generally recommended to use OSU_Secure over OSU_Access whenever possible

Accessing OSU_Secure

You can either connect automatically or manually to the OSU_Secure. Connecting automatically should prompt for your onid username and password. If it doesn't, use the general settings for the OSU_Secure network to set it up manually:

» SSID: OSU_Secure
» Security: WPA2 Enterprise
» EAP Method: PEAP (PEAPv0/EAP-MSCHAPv2)
» Key Type: AES (or automatic)
» Phase2 Type: MSCHAPv2
» Username: *ONID Username*
» Password: *ONID Password*

More detailed instructions with pictures are available by clicking on your device below!

Windows XP ▸
Windows Vista, 7 ▸
Windows 8/8.1 ▸
Mac OS X 10.5 and Older ▸
Mac OS X 10.6 and Younger ▸
Linux (Unix) ▸

PLEASE NOTE:

The OSU Computer Helpdesk does not officially support Linux devices on the secure wireless network. Most should work fine if configured properly, but if any questions arise, they should be directed to the Linux community (there is a Linux Users Group on campus as well). The details on this page are only suggestions that have been reported to work in the past.

The general settings for the OSU Secure network are as follows:

» SSID: OSU_Secure
» Security: WPA2 Enterprise
» EAP Method: PEAP (PEAPv0/EAP-MSCHAPv2)
» Key Type: AES (or automatic)
» Phase2 Type: MSCHAPv2
» Domain (If required): ONID
» Username: *ONID Username*
» Password: *ONID Password*

If you are unable to get the default wireless manager to work, users have had success switching to WICD as their wireless manager.

For help installing WICD for your flavor of Linux, see the WICD Downloads Page. The top of this page also provides some basic troubleshooting steps to start using it.

NOTE: Once you install WICD, you will have to uninstall or stop your other wireless manager to use it.

Mobile Settings ▸

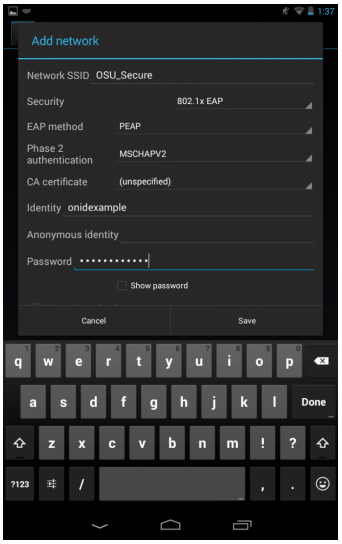
These are the general settings that a mobile device will have to have in order to connect to OSU_Secure.

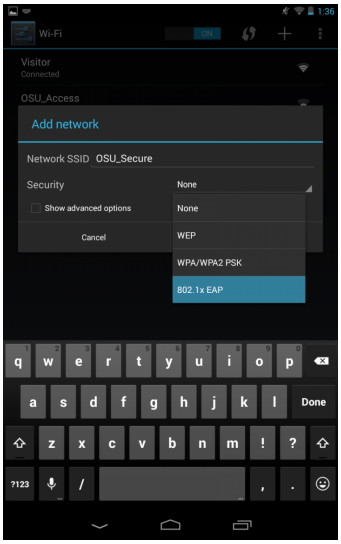
» SSID: OSU_Secure
» Security: WPA2 Enterprise (Or 802.1x EAP)
» EAP Method: PEAP (PEAPv0 / EAP-MSCHAPv2)
» Key Type: AES (or automatic)
» Phase2 Type: MSCHAPv2
» Username: *ONID Username*
» Password: *ONID Password*
» Note: Under **Show advanced options** make sure **Proxy settings** is set to none, otherwise you will be unable to save.

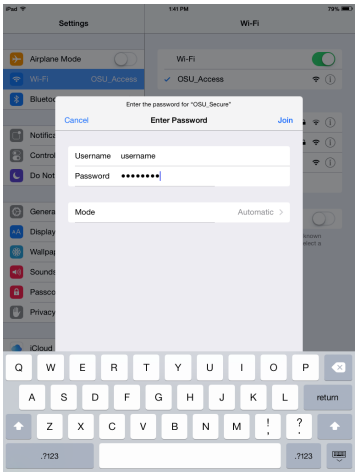
Note: These pictures only reflect one version of Android. If you cannot set up your phone on the network, please call us at: 541-737-3474

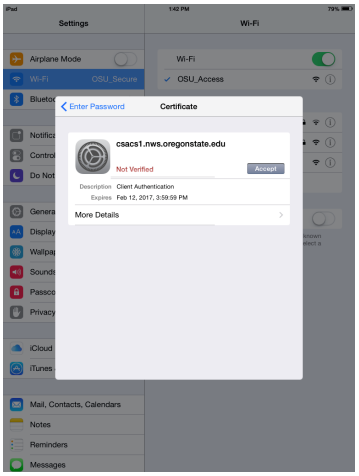
In general, please find OSU_Secure in your Wi-Fi settings. Once you click OSU_Secure, it's going to request that you put in a username, and a password. Proceed to put your ONID username, and your ONID password in the appropriate fields.

If it asks you to accept a network certificate after you've successfully entered your ONID username and ONID password in the appropriate login fields - please accept this certificate. Once you've fully accepted - you should have access to the wireless network.









If your device is not listed, feel free the click the Feedback Button below to request information!

"Fun Facts:" ▸

Why OSU_Secure?

Secure networks ensure the safety of sensitive information transmitted over the web, such as banking transactions and emails. Wireless clients using the OSU_Access network will be limited to what they can access. You can use the VPN service on the OSU_Access network to have similar to secure access capabilities that OSU_Secure provides.

What does the "Secure" part of OSU Secure mean?

The secure part means that any data you send over the wireless connection is encrypted. Browsers and websites can encrypt the data transmissions themselves, which happens on most or all sites that transfer any sensitive information. You can determine if a website is encrypting information when the URL indicates an HTTPS connection, as opposed to an unencrypted HTTP connection (S stands for secure). The encryption done by the wireless network is another layer of security that helps protect your sensitive information on all websites. The following is more technical information which is unnecessary for the use of the wireless networks.

Examples:

Unsecured Wireless (OSU_Access):

Data sent through an HTTP connection will be transmitted over the wireless network completely unencrypted. If you are submitting a comment to an unsecured forum the data would be transmitted in clear text which could be read by anybody with the correct software. For poorly designed websites they may also be able to see the username, password, and what website you were trying to log in to.

Data sent through an HTTPS connection will be encrypted on your computer and sent through the network. Anybody with the correct software would be able to see where you were sending the information to but not the actual information being sent. (more technically the header information will not be encrypted but the data will be).

Secured Wireless (OSU_Secure):

Data sent through either type of connection will still result in everything being encrypted. Anybody with the correct software will be able to see that you are sending and receiving data but they will not be able to tell where you are sending it or what information you are sending (including usernames and passwords).

‹ Eduroam Wireless up OSU_Access ›

» Printer-friendly version

We want your feedback!

Helpdocs are made just for you, so please tell us how we can make this information more clear and accessible. The more feedback that you can provide, the more we can improve our services to you!