



Connecting to SU-secure – Windows 8

Updated 10/10/18

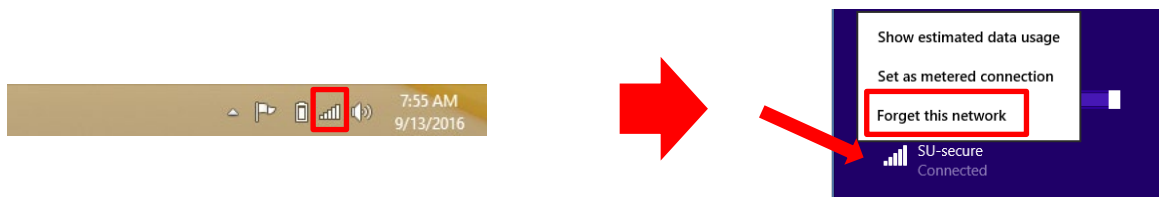
Content provided by ITS Data Network Operations

Overview

This document provides step-by-step instructions for both automatically and manually configuring your Windows 8 computer to connect to SU-secure. Attempt automatic configuration first. Only attempt manual configuration if automatic configuration is unsuccessful. SU-secure is only available for use by Seattle University students, faculty, staff, and Jesuits. For information about guest wireless access, please visit the guest account page at: <https://www.seattleu.edu/support/guides/guest-accounts/>

Remove Existing SU-secure Profile

1. Click on the wifi icon in the system tray
2. Right click on SU-secure and select 'Forget this network'



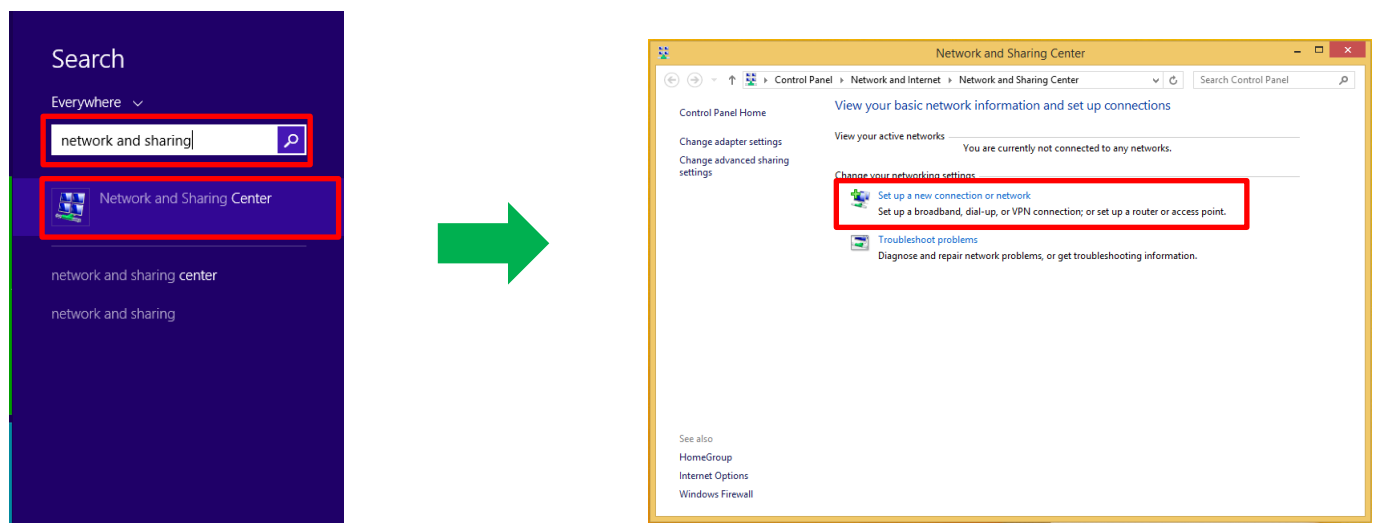
Automatic Configuration

1. Per the instructions above, ensure you have removed any existing SU-secure profiles from your device.
2. Visit the ITS downloads page at <https://www.seattleu.edu/support/downloads/>. You may be prompted to enter your SeattleU credentials to access this page.
3. Locate the 'Autoconfigure SU-secure' heading and download the Windows Devices configuration package.
4. Locate the 'AutoConfigureWindows-SU-secure.zip' file in your downloads folder
5. Right-click the folder, select 'Extract All' and then click on the 'Extract' button
6. The extracted contents of 'Autoconfigure SU-secure.zip' will appear
7. Double click the 'RUNME – Auto configure SU-secure' file to automatically configure your SU-secure connection
8. Select SU-secure from the list of available networks, click connect, and enter your SeattleU credentials in the authentication prompt that appears

Manual Configuration

1. Add SU-secure to your wifi network list

- a. Click on the start button, type 'network and sharing center' in the search bar, and click on the Network and Sharing Center button. The Network and Sharing Center will appear.
- b. Click on the 'Set up a new connection or network' button to add a new wireless network.



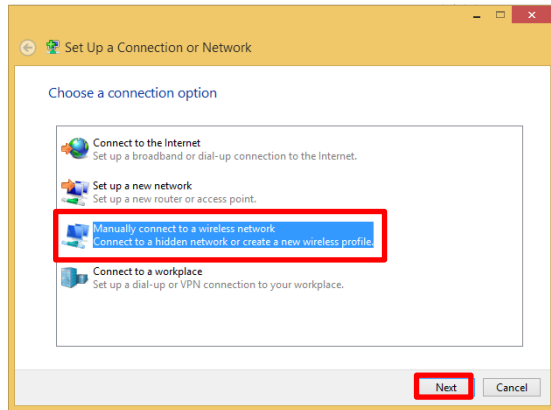


Connecting to SU-secure – Windows 8

Updated 10/10/18

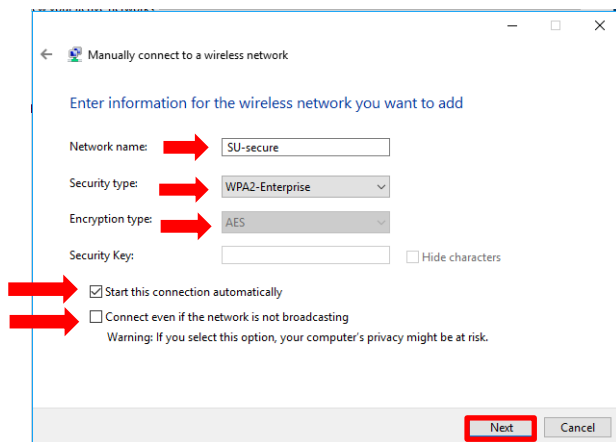
Content provided by ITS Data Network Operations

- c. The Set Up a Connection or Network menu will appear. Select 'Manually connect to a wireless network' and press 'Next' to continue.



- d. The initial connection set up menu will appear. Enter the following information and then click 'Next' to add SU-secure to your list of wireless networks

- i. Network name: **SU-secure**
- ii. Security type: **WPA2-Enterprise**
- iii. Encryption type: **AES**
- iv. Security key: **Leave blank**
- v. Start this connection automatically: **Checked**
- vi. Connect even if the network is not broadcasting: **Unchecked**





Connecting to SU-secure – Windows 8

Updated 10/10/18

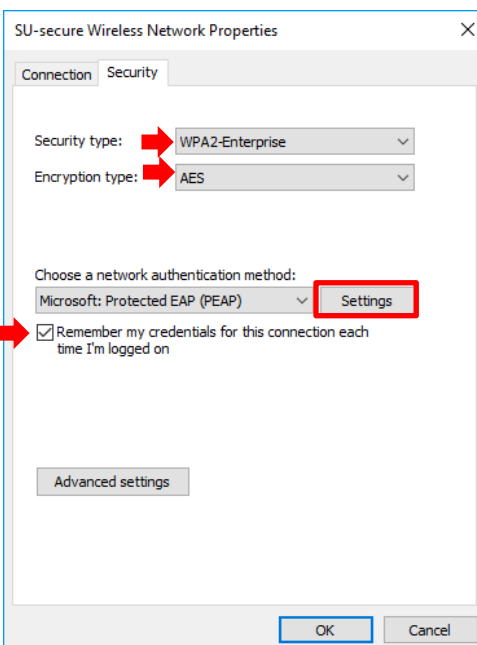
Content provided by ITS Data Network Operations

2. Configure your connection

- A window will appear that confirms SU-secure was successfully added. Select 'Change connection settings' to continue to the wireless properties menu.
- Click on the 'Security' tab at the top of the wireless properties menu.



- Once on the Security tab, ensure the following settings are configured:
 - Network authentication method: **Microsoft: Protected EAP (PEAP)**
 - Remember my credentials for this connection each time I'm logged on: **Checked**
- Then click the 'Settings' button next to the network authentication method drop down bar.





Connecting to SU-secure – Windows 8

Updated 10/10/18

Content provided by ITS Data Network Operations

- e. The Protected EAP properties menu will appear. Make the following changes and click 'OK':
 - i. Validate server certificate: **Checked**
 - ii. Connect to these servers: **Checked**
 - iii. Server list: **oitias2.seattleu.edu;**
 - iv. Trusted Root Certification Authorities: **Check 'AddTrust External CA Root' and then scroll down in the list to check 'USERTrust RSA Certification Authority'**
 - v. Do not prompt user to authorize new servers or trusted certification authorities: **Unchecked**
 - vi. Select Authentication Method: **Secured password (EAP-MSCHAP v2)**
 - vii. Click on 'Configure...' next to the Authentication method dropdown bar and **uncheck 'Automatically use my windows logon name and password' in the popup box that appears, then click 'OK'**
 - viii. Enable Fast Reconnect: **Checked**

Protected EAP Properties

When connecting:

- Verify the server's identity by validating the certificate
- Connect to these servers (examples: srv1; srv2; *, srv3, com):
oitias2.seattleu.edu;

Trusted Root Certification Authorities:

- AddTrust External CA Root
- Baltimore CyberTrust Root
- Certification Authority of WoSign
- Class 3 Public Primary Certification Authority
- COMODO RSA Certification Authority
- DigiCert Assured ID Root CA
- DigiCert Global Root CA

Notifications before connecting:

Tell user if the server's identity can't be verified

Select Authentication Method:

Secured password (EAP-MSCHAP v2) Configure...

- Enable Fast Reconnect
- Disconnect if server does not present cryptobinding TLV
- Enable Identity Privacy

Trusted Root Certification Authorities:

- Symantec Enterprise Mobile Root for Microsoft
- Thawte Premium Server CA
- thawte Primary Root CA
- thawte Primary Root CA - G3
- Thawte Timestamping CA
- USERTrust RSA Certification Authority
- UTN-USERFirst-Object

EAP MSCHAPv2 Properties

When connecting:

- Automatically use my Windows logon name and password (and domain if any).

OK Cancel

- f. Click 'OK' on the Protected EAP properties menu
- g. Click 'OK' on the Wireless Network Properties menu
- h. Click 'Close' on the Manually Connect to a Wireless Network menu.

Protected EAP Properties

When connecting:

- Verify the server's identity by validating the certificate
- Connect to these servers (examples: srv1; srv2; *, srv3, com):
oitias2.seattleu.edu;

Trusted Root Certification Authorities:

- AddTrust External CA Root
- Baltimore CyberTrust Root
- Certification Authority of WoSign
- Class 3 Public Primary Certification Authority
- COMODO RSA Certification Authority
- DigiCert Assured ID Root CA
- DigiCert Global Root CA

Notifications before connecting:

Tell user if the server's identity can't be verified

Select Authentication Method:

Secured password (EAP-MSCHAP v2) Configure...

- Enable Fast Reconnect
- Disconnect if server does not present cryptobinding TLV
- Enable Identity Privacy

OK Cancel

SU-secure Wireless Network Properties

Connection Security

Security type: WPA2-Enterprise

Encryption type: AES

Choose a network authentication method:

Microsoft: Protected EAP (PEAP) Settings

- Remember my credentials for this connection each time I'm logged on

Advanced settings

OK Cancel

Manually connect to a wireless network

Successfully added SU-secure

Change connection settings
Open the connection properties so that I can change the settings.

Close

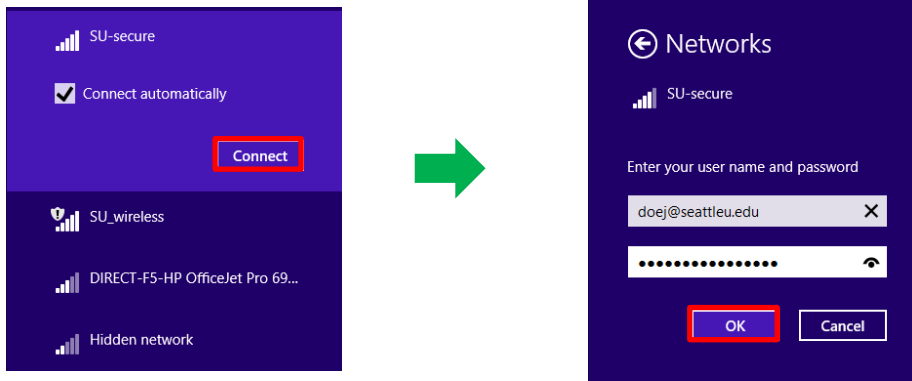


Connecting to SU-secure – Windows 8

Updated 10/10/18

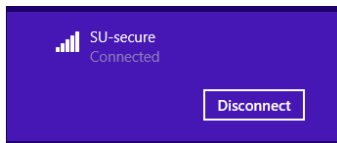
Content provided by ITS Data Network Operations

- i. Click on the wifi icon in the system tray to bring up the list of available wireless networks. Select SU-secure from the list and click 'Connect'.
- j. You will be prompted to enter your credentials. Enter your SU credentials and click 'OK' to connect.



3. Verify that you are connected

- a. Upon successful connection, your system tray menu will show that you are connected to SU-secure:



4. If you are unable to connect your device to SU-secure after following the above steps:

- a. Visit <https://www.seattleu.edu/its/support/support-articles/wireless-network-connect-to-su-secure.html> and locate the troubleshooting guide for your device.

If you need assistance

If you are still unable to connect to SU-secure after configuring your device according to the steps in this document, you can contact the Help Desk for assistance. For time-sensitive issues, the ITS Help Desk is available Monday-Friday 7:00am-7:00pm via phone at 206-296-5571. For non-time sensitive issues, or issues occurring outside Help Desk hours, you can contact the Help Desk via email at helpdesk@seattleu.edu.

When opening a support ticket with the Help Desk, please provide the following information:

- Your account username (i.e. 'doej').
- The brand and model of the device you are attempting to connect to SU-secure.
- The operating system version of the device you are attempting to connect to SU-secure.
- What location (building, room) you are attempting to connect in.
- A description of the error message or problem you are seeing.