

St. Clair College Wireless Overview

St. Clair College hosts several wireless networks to support students, faculty and staff.

These services are based on a secure reliable platform using WPA/2 enterprise encryption with 802.1X authentication.

Please be aware devices that use WPA personal encryption will not work on this network, including some wireless printers, gaming consoles, etc.

STUDENT WIRELESS NETWORKS

SCCSTUDENT5G (Student wireless network 5GHz network)

- If faster speeds and a more reliable connection are most important to you, 5GHz is usually a better choice than 2.4 GHz.
- The 5GHz band is less likely to be congested, and offer much higher data transfer speeds.
- For Wi-Fi dense areas like the residences we recommend the use of this network.
- We recommend that Apple devices connect to this network.

SCCSTUDENT (Student wireless network 2.4GHz/5GHz network)

Most devices have the capability of using 2.4GHz & 5GHz and might default to 5GHz using this network, unless you have the ability to change the settings.

- If wireless range is more important to you, 2.4 GHz is usually a better choice than 5 GHz.
- If you have a lot of devices nearby that use 2.4 GHz and you are experiencing intermittent connectivity issues or dropped wireless connection then 5 GHz is probably a better option.
- If you have an older device that doesn't support 5GHz then 2.4GHz is to be used.

STAFF WIRELESS NETWORKS

StaffBYOD (Staff wireless network 2.4GHz/5GHz for personal devices)

- Use this network if you're a current staff member requiring Internet access for your personal devices, such as
 phones and tablets.
- This network does not connect to any internal resources and only connects to the Internet.

SccSTAFF (Staff wireless network 2.4GHz/5GHz for College owned devices)

- Only for use with College owned Equipment.
- Cell Phones should not use this SSID

Device Specific Connection Details for Common Devices

Android Devices

Each version of Android has a different interface. You should find all the information required to connect in the following list.

Select the appropriate Wi-Fi network (SCCSTUDENT/SCCSTUDENT5G/StaffBYOD) based on your needs.

Use the following settings;

EAP Method = PEAP

Phase 2 Authentication = None

CA Certificate = DON'T VALIDATE

Identity = St.Clair ONE username

Anonymous Identity = empty, leave blank

Password = St.Clair ONE password

iOSs (Apple Devices)

Select the appropriate Wi-Fi network (SCCSTUDENT/SCCSTUDENT5G/StaffBYOD) based on your needs.

Enter your St. Clair ONE username and password into the Username and Password fields.

Tap JOIN

TAP Trust the SSL certificate - wifisponsor1.stclaircollege.ca

Windows (8 and 10)

Select the appropriate Wi-Fi network (SCCSTUDENT/SCCSTUDENT5G/StaffBYOD) based on your needs. (*If you want to connect automatically within range of the selected network make sure Connect automatically is checked*)

Enter your St. Clair ONE username and password into the User name and Password fields and proceed.

You may be prompted to CONTINUE CONNECTING

Click CONNECT

(k	SCCSTUDENT5G Secured	
	Continue connecting? If you expect to find SC location, go ahead and may be a different netw name. Show certificate details	connect. Otherwise, it vork with the same
	Connect	Cancel

ChromeBook

Select the appropriate Wi-Fi SSID (SCCSTUDENT/SCCSTUDENT5G/StaffBYOD) based on your needs. Use the following settings; Security = EAP EAP Method = PEAP EAP Phase 2 authentication = Automatic Server CA Certificate = DO NOT CHECK Identity = St.Clair ONE username Password = St.Clair ONE username Password = St.Clair ONE password Anonymous Identity = empty, leave blank Save Identity and Password = Turn ON Allow other users of this device to use this network = Turn Off Click CONNECT

PIXEL Cell Phones (Not all Pixel models work with these settings.)

Select the appropriate Wi-Fi SSID (SCCSTUDENT/SCCSTUDENT5G/StaffBYOD) based on your needs. Use the Following settings

Security - EAP

EAP Method = PEAP

Phase 2 Authentication = MSCHAPV2

CA Certificate = Use system certificates

Domain = stclaircollege.ca

Identity = St.Clair ONE username

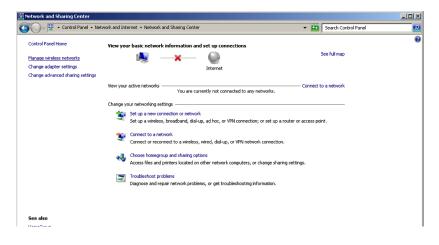
Anonymous Identity = empty, leave blank

Password = St.Clair ONE password

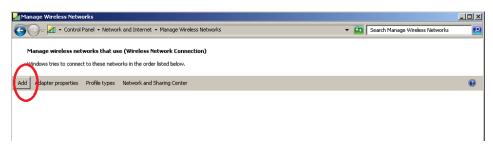
Windows 7

Click Start > Control Panel > Network and Sharing Center

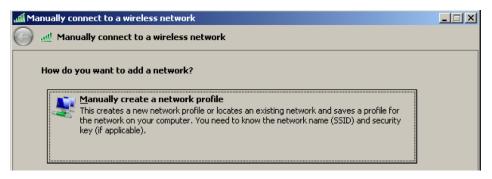
Click Manage wireless networks from the menu on the left



In the "Manage Wireless Networks" window click Add



Click Manually create a network profile



Complete the information in the form

Manually connect to a v	vireless network	
Enter information for	the wireless network you want to add	
Network name:	SCCSTUDENT	
Security type:	WPA2-Enterprise	
Encryption type:	AES 🔹	
Security Key:	Hide characters	
Start this connection	automatically	
Connect even if the	network is not broadcasting	
Warning: If you sele	ct this option, your computer's privacy might be at risk.	
	Next	t Cancel

The NETWORK NAME must be spelled exactly like the SSID you want to connect to.

(SCCSTUDENT or SCCSTUDENT5G or StaffBYOD)

Click Next

A new window will open informing you that you have successfully added the SSIDcure Access. Click Change connection settings



Click CLOSE

You will now see the Manage Wireless Networks window.

RIGHT Click on the Network you just created.

Click Properties

This opens the properties windows.

SCCSTUDENT Wireless	Network Properties
Connection Security	
Name:	SCCSTUDENT
SSID:	SCCSTUDENT
Network type:	Access point
Network availability:	All users
Connect automati	cally when this network is in range
Connect to a more	e preferred network if available
Connect even if t	he network is not broadcasting its name (SSID)
Enable WLAN con	nection settings
Configure	

Select the Security TAB

Ensure the window is filled in as shown.

-	SCCSTUDENT Wireless Network Properties	x
	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	
	ОК Са	ncel

Ensure the windows is filled in as shown below

Protected EAP Properties
When connecting:
Connect to these servers:
Trusted Root Certification Authorities:
AddTrust External CA Root Baltimore CyberTrust Root
Certum CA Class 3 Public Primary Certification Authority DigiCert Assured ID Root CA
DigiCert Global Root CA DigiCert Global Root G2
4 III +
Do not prompt user to authorize new servers or trusted certification authorities. Select Authentication Method:
Secured password (EAP-MSCHAP v2) Configure
Enable Fast Reconnect Enforce Network Access Protection Disconnect if server does not present cryptobinding TLV Enable Identity Privacy
OK Cancel

Click Configure button

Ensure the Automatic Logon is NOT checked



Click OK

Click OK

You should be back to the Properties Security TAB

Click ADVANCED SETTINGS

Click Specify Authentication Mode

Change the setting to USER Authentication

Do NOT click save credentials

Click OK

Click OK

You have now Created a Wireless Profile for the SSID you chose (This is only done once)

Close the Manage Wireless Networks window.

LEFT Click on the Wireless Icon in the taskbar and choose the SSID you just setup the profile for.

Enter your St.Clair ONE username and password.

Click OK

You will receive a warning that the connection could not be completed.



Click CONNECT

You should now have access to the Internet.