Different devices and operating systems have differing ways of referring to the same settings for connecting to a wireless network. This document covers common settings and their names for connecting to the wireless network at JMU.

Enable Wireless

You may need to toggle a switch on your device to enable wireless, go into the device’s settings, or use a particular wireless menu to make sure that the wireless network capability is turned on. This can vary greatly from device to device.

Find the Network

Your device will likely present a list of available wireless networks in settings or a wireless menu, though some older devices may require you enter the name of the network manually. Select or enter JMU-Official-Wireless.

If your device requires you to specify the Network Type or Operating Mode, select Infrastructure. Do not specify Ad-Hoc.

Security Settings

Your device may prompt you to specify security settings for the wireless network. Unfortunately, different ones may ask for different types of settings and refer to them by a variety of names. Not all of the following settings may apply to your device and your device may list them in a different order. Some devices may not prompt at all and determine the correct settings automatically.
Network Security Type

This configures the overall type of security used on the wireless network and may be automatically determined by your device. This setting is sometimes also called Wireless Security, Security Type, Security Mode, Security, or Network Authentication.

If your device does not determine this automatically, configure it for WPA2 Enterprise. This could also be called WPA2 EAP or WPA Enterprise if there is no WPA2-specific option. If there are no WPA Enterprise or EAP options, you may be able to use 802.1x EAP. Do not chose any option with PSK or WEP.

EAP Type

EAP specifies how your computer will send your username and password to the wireless network so that it can verify your identity securely. This setting is sometimes also called EAP Method, Authentication Type, 802.1x Authentication Type, Authentication, Security SubType, or Network Authentication Method.

If your device does not determine this automatically, configure it for Protected EAP (PEAP). This could also just be called PEAP. Do not chose any option for LEAP, Fast, or TLS.

PEAP Version

The PEAP version specifies particular details about how your computer sends your credentials to the wireless network. Most devices will not ask for this.

If your device does not determine this automatically, configure it for Version 0.

Authentication Type

The authentication method inside EAP specifies particular details about how your computer sends your credentials to the wireless network. This setting is sometimes also called Inner Authentication, Inner Link Security, Inner EAP Method, Phase 2 Authentication, Tunnel Authentication Type, or Authentication Protocol.

If your device does not determine this automatically, configure it for MSCHAPv2. This could also be called EAP-MSCHAP v2. Do not chose any option for EAP-GTC.
Certificate Authority

The wireless network uses a digital certificate to identify itself to your device so that your device will know that it's not connecting to a fraudulent network that's calling itself **JMU-Official-Wireless**.

Your device verifies the network's certificate by checking to see if a known, trusted organization issued (sometimes called "signed") the certificate. This setting is sometimes called **CA Certificate**, **Trusted CA**, **Trusted Root Certification Authority**, **Certificate Issuer**, or **Server Certificate**.

The certificate for **JMU-Official-Wireless** (wireless.jmu.edu) was issued by **InCommon RSA Server CA**, which was issued by **USERTrust RSA Certification Authority**, whose certificate was in turn issued by **AddTrust External CA Root**. Your device may show all of the issuers or only one. It's possible that your device may need you to specify the the issuer/CA's name or certificate file. For devices that need the file specified, the path may vary.

On some Linux distributions like Debian, Ubuntu, or Mint, you should specify:

```
/etc/ssl/certs/AddTrust_Experlal_Root.crt
```

On some Linux distributions like Red Hat, Fedora, CentOS, or Oracle, you should specify:

```
/etc/pki/tls/certs/ca-bundle.crt
```

Your device may instead offer to just verify the certificate, possibly using "System CA" certificates, and you do not need to specify any information about a particular issuer. Some devices may not perform this validation at all.

Encryption Type

This specifies the way in which your communications will be secured over the wireless network. This setting may also be called **Data Encryption**. Most devices will not ask for this.

If your device does not determine this automatically, configure it for **AES**.

Anonymous Identity

This is **not** your JMU eID. If your device asks for this leave it **blank**.
Network Settings

If your device asks how it should configure its IP address and/or related settings like DNS server, go with **Automatic**. Manually configuring the IP address and related settings will not work on the wireless network.