Connect to GreenRiverWireless

Connect to the GreenRiverWireless SSID

If the landing page does not show up, browse to neverssl.com to force a redirection

Click for GatorWIFI – Annual internet access

Select Student

Read and agree to the AUP

Enter your GRC student domain credentials (like logging into an open lab computer)
Android-Specific Configuration Instructions
The application detects the user agent for the Android operating system and provides the correct installation and configuration instructions.

The following screen is displayed for devices running the Android operating system 6.0 or newer.

Tap Install the Network to start the installation process.

The following screen is displayed for devices running the Android operating system 5.x or older.

Tap Step 1: First, Install the App to start the installation process
Download and Install Application
The application is available from Google Play Store, Amazon Market, and as a Direct Download from a local web server.

Select the installation method to continue.

Install from Google Play
The application can be installed from the Google Play Store.

Tap Install to continue.

Accept Access Request
To run the enrollment wizard and configure the device, the application requires access to location of the device.

Tap Allow to continue.

Next Step After Application is Installed on Device
If you are using the Google Play Store installation, your next step depends on your Android version.

Do one of the following, depending on your Android version:
• If you are running Android version 6.0 or later, you can click the Open button on the app
• If you are running a version earlier than Android 6.0, do not tap the Open button. Instead, use the Back arrow to return to the Installation and Configuration screen. Next, click the “Install the Network” button. (This option works for any version of android that has the cloud path app installed.)
The device should be connected to GatorWIFI for the academic year once the installer runs.

**Android 4.2 and earlier experience** - Most android phones are much newer than this, this experience is becoming very rare.

**Passcode PIN or Pattern Lock**

The Android OS requires the user to enter your passcode PIN or pattern to unlock the keystore and install the certificates on the device.

The application provides instructions for responding to these prompts. Read each screen carefully and respond as directed to the screens that follow.

**FIGURE 22 Prompt to Respond to Passcode Lock**
Tap OK to continue.
If requested, confirm the screen lock passcode to allow the application to install the certificate into the keystore.

**NOTE**
Certain Android devices do not allow a pattern to secure the keystore. This is a function of the Android OS and not the Cloudpath application. In these cases, the user is prompted to enter a PIN passcode for the screen lock before they can continue.

**How to Respond to Certificate Installation Prompts**
Before each certificate prompt, the application displays a message that tells the user how to respond on the following credential extraction and installation screens.
Read each screen carefully and respond as directed to the screens that follow.

**FIGURE 23 How to Respond to Certificate Prompts**

**Extract Certificate**
The device requires access to the keystore to extract the certificate.
Tap OK to extract the certificate, as instructed on the previous screen.

**Name the Certificate**

The application pre-populates the certificate name based on the network configuration.

If the previous screen indicated that you must enter a certificate name, enter it on this screen. Otherwise, tap OK to keep the default name.

**NOTE**

If the network has been configured for additional credentials, you might be required to repeat the previous 3 steps (Message, Extract, Name Certificate)
Troubleshooting

Common Android Issues
This chapter describes issues with using Cloudpath on the Android operating system that might prompt you to contact the network help desk.

Fully Connect to the Internet
Connect to GreenRiverWireless, and choose the alternate single session internet login, and connect to the internet. Then browse to wifireg.greenriver.edu to enroll in GatorWIFI. Occasionally this is necessary if the device insists on verifying a public certificate or scanning downloaded files before properly installing the network.

Remove Certificates
If there are old certificates on the device that were installed previously by the Wizard, they can be removed. Go to Settings > Security and select Clear Credentials (or Clear Storage).

Remove SSID
Sometimes a previous connection has corrupted or old settings and the user needs to remove the SSID from the device. Go to Settings > Wi-Fi, locate the SSID for the network, and tap Forget.

Android .netconfig File
If you tap the link to Continue with configuration of the network and receive a message that says it downloaded a file called android.netconfig, you need to check the device for the following issues:
1. You do not have the Cloudpath Wizard installed, so the server cannot instruct the device to start the application and use the file.
2. You were prompted to Play Online or Download when tapping the link, and selected Download. The user must select Play Online for the wizard to start up.

Passwords and Lock Screen PINs
The Android operating system stores portions of the data needed to authenticate in an encrypted key store. On Android versions prior to version 4.0, a password is needed to access the key store. From versions 4.0 through 6.0, the lock screen pin is the password that is used to access the key store, which is why the operating system requires that the lock screen to be enabled. To clear the key store, Go to the Settings screen, select Security, and scroll to the bottom of the screen and select Clear Credentials.

Blank Certificate Field
Android does not have a supported method for getting certificate chains in to the key store for use in authentication. Because of this, Cloudpath uses workarounds to make the authentication system use certificate chains. However, some workarounds do not show up in the settings screen. In addition, if Android claims the certificate was installed in the key store and then the authentication fails, the application falls back to our workaround methods. This is done because some devices claim to have installed the certificate, but actually don't.

Certificate Passwords
Android APIs do not allow Cloudpath to specify the password when the application inserts the certificate into the key store. The workaround is to use a password prompt to install the certificate. You simply enter the password that is displayed in the password prompt and Cloudpath installs the certificate.

Memory Card
In some cases, the Cloudpath Wizard stores data on the memory card in the device. If you remove or change the memory card, authentication fails, and you must redeploy the wizard with the new memory card in the device to get it working properly.

Uninstalling the Application
It is sometimes necessary to remove the 802.1X configuration and certificates provided by the wizard before you can uninstall the application. This is enforced by the device OS, and not by the Cloudpath Wizard. If you encounter issues while attempting to uninstall the Cloudpath application from your Android device, check the following settings.

Remove Device Administrator
If the device has any settings configured that use Android's device administration capabilities (such as mobile device management), the Cloudpath Wizard creates an administrative user during installation and this user must be removed before Cloudpath can be uninstalled. Go to Settings > Security, select Device Administrator and uncheck the Cloudpath administrative user.

Remove Certificates
If there are certificates on the device that were installed by the Wizard, they should be removed. Go to Settings > Security and select Clear...
Credentials (or Clear Storage).

**Remove SSID**

The user might be required to remove the SSID from the device. Go to Settings > Wi-Fi, locate the SSID for the network, and tap Forget.