SecureCanes Instructions

What is SecureCanes?

SecureCanes is a wireless network that provides encryption for your wireless communications from your device to the wireless access point. Users must use their CaneID and password to access the SecureCanes network.

Why?

SecureCanes uses an IEEE industry standard 802.1X which provides enhanced security to wireless networks. The 802.1X standard offers an effective framework for authenticating and controlling user traffic to a protected network.

CanesGuest vs SecureCanes

CanesGuest is an open, unsecure network that offers no encryption to the wireless network. It provides guests of the University with limited Wi-Fi access.

SecureCanes is an encrypted Wi-Fi network that allows faculty, staff, and student employees to surf the Internet in a secure manner. Start using SecureCanes today for your security!

How?

This documentation serves as a how-to SecureCanes connection guide.

The examples in this guide include walk-throughs for the following operating systems:

- Windows 10
- Windows 8
- Windows 7
- Mac OSX Sierra (10.12) or higher
- Apple iOS
- Android
- Chrome OS

Requirements

Faculty, staff, and students can connect to SecureCanes using a wireless-capable device, such as a laptop, tablet, or smartphone.

Support

For additional assistance and support, please contact the UMIT Service Desk at: (305) 284-6565, help@miami.edu
SecureCanes

Section 1.1 Windows 10

1) Click on the wireless signal icon on the bottom right of your screen.

2) Select SecureCanes from the list of wireless network connections.
Section 1.1 Windows 10 cont’d

3) Click on Connect for SecureCanes and checkmark Connect automatically.

4) You will be prompted to input your CaneID username and password. Then click OK.
Section 1.1 Windows 10 cont’d

5) You will be prompted to “Continue connecting?” Click Connect.

6) You will then be connected to the SecureCanes network.
Section 2.1 Windows 8

1) Click on the wireless signal icon on the bottom right of your screen.

2) Select SecureCanes from the list of wireless network connections and click Connect.
Section 2.1 Windows 8 cont’d

3) You will be prompted to input your CaneID username and password. Then click OK.

4) Click on Connect to accept the 802.1x certificate.

5) You will then be connected to the SecureCanes network.
Section 3.1 Windows 7

1) Click on the wireless signal icon on the bottom right of your screen.

2) Select SecureCanes from the list of wireless network connections.
Section 3.1 Windows 7 cont’d

3) Click on Connect for SecureCanes and checkmark Connect automatically.

4) You will be prompted to input your CaneID username and password. Then click OK.
Section 3.1 Windows 7 cont’d

5) Click on Connect to accept the 802.1x certificate.

6) You will then be connected to the SecureCanes network.
Section 4.1 Mac OS X

1) Click on the wireless signal icon on the top right of your screen.

2) Select SecureCanes from the list of wireless networks.

3) You will be prompted to input your CaneID username and password. Checkmark Remember this network and then click OK.
Section 4.1 Mac OS X cont’d

4) Click on *Continue* to accept the 802.1x certificate.

5) If your Mac prompts you for a password, type in your local user password and then click *OK*.

6) You will then be connected to the *SecureCanes* network.
Section 5.1 Apple iOS Mobile Devices

1) Tap on the Settings icon on your home screen.

2) On the Settings screen, tap on Wi-Fi.

3) Tap on SecureCanes from the list of Wi-Fi networks.
Section 5.1 Apple iOS Mobile Devices cont’d

4) You will be prompted to input your CaneID username and password. Then tap Join.

5) Tap on Accept to accept the 802.1x certificate.

6) You will then be connected to the SecureCanes network.
Section 6.1 Android 8.0 and select versions of Android 9.0

1) Tap on the *Settings* icon located in your Apps.

2) Under Wireless and network, tap on *Wi-Fi*.

3) Tap on *SecureCanes* in Wi-Fi.
Section 6.1 Android 8.0 and select versions of Android 9.0 cont’d

4) From the Connect menu select “PEAP” as the EAP method and “MSCHAPV2” as the Phase 2 authentication. Select the CA certificate as “Use system certificates”.

5) Enter “miami.edu” as the Domain, and input your CaneID and Password as your identity and password. Then tap Connect.

6) You will then be connected to the SecureCanes network.
Section 6.2 Android 9.1 Mobile Devices

1) Tap on the Settings icon located in your Apps.

2) Under Connections, tap on Wi-Fi.

3) Tap on SecureCanes.
Section 6.2 Android 9.1 Mobile Devices cont’d

4) From the Connect menu select “PEAP” as the EAP method.

5) Input your CaneID and Password as your identity and password. Then tap Connect.

6) You will then be connected to the SecureCanes network.
Section 6.3 Android 10.0 Mobile Devices

1) Tap on the Settings icon located in your Apps.

2) Select Network & internet, and then tap on Wi-Fi.

3) Tap on SecureCanes in Wi-Fi.
Section 6.3 Android 10.0 Mobile Devices cont’d

4) From the Connect menu select “PEAP” as the EAP method and “MSCHAPV2” as the Phase 2 authentication. Select the CA certificate as “Use system certificates”.

5) Enter “miami.edu” as the Domain, and input your CaneID and Password as your identity and password. Then tap Connect.

6) You will then be connected to the SecureCanes network.
Section 7.1 Chrome OS

1) Select the wireless and clock icon at the bottom right hand corner of the screen.

1) Select the No network” option to see the list of available networks.

1) Select the SecureCanes network.
Section 7.1 Chrome OS cont’d

1) On the Join Wi-Fi network page, enter “EAP-TTLS” as the EAP method, and “MSCHAPV2” as the EAP Phase 2 authentication. Use “Default” for the Server CA certificate.

1) Input your CaneID and Password as the Identity and Password. Then select “Connect”.