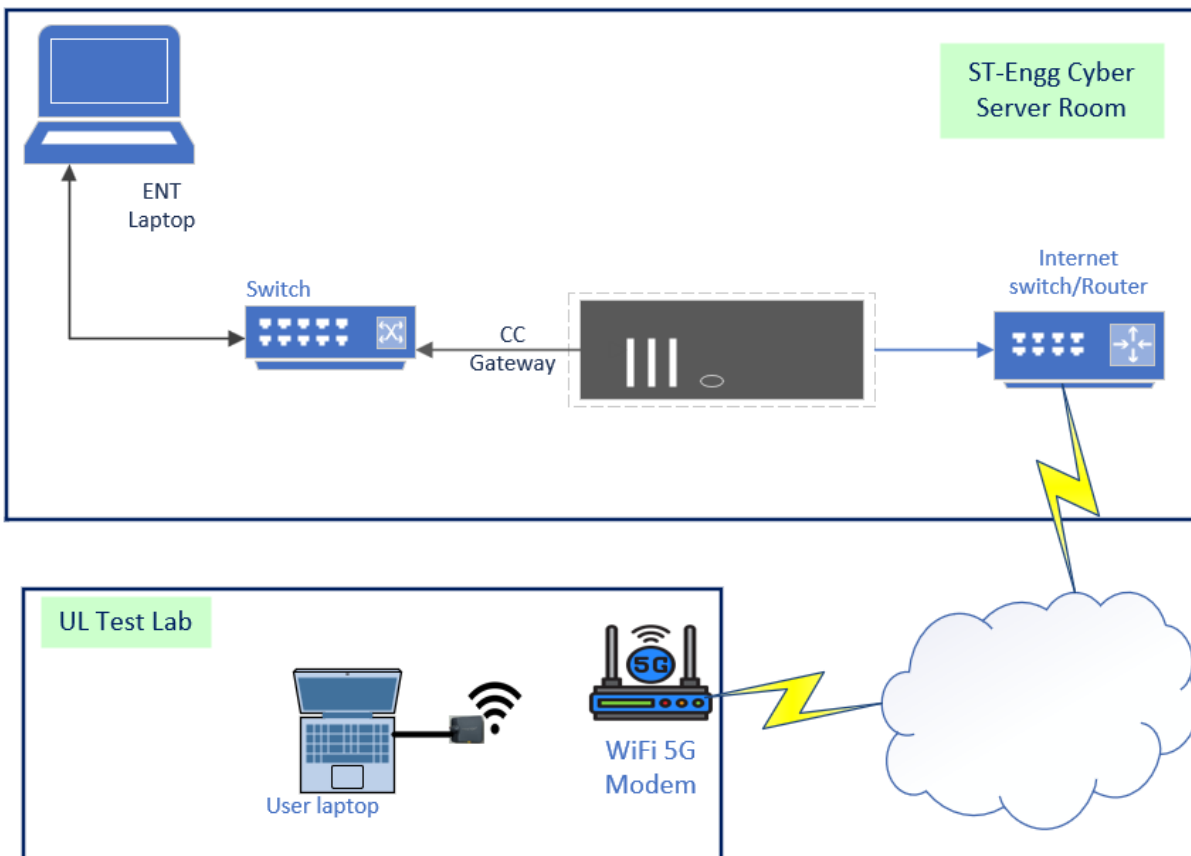


WiZ-Knight (on-prem) functional user manual

WiZ-Knight (on-prem) system includes an Enterprise gateway and portable encryptors to connect to the gateway. Portable encryptors are small handheld devices that will be used for secured access to the enterprise resources through the back-end gateway.

To validate the dongle, the backend gateway must be set up with the relevant configuration and must be available online. Dongle is to be provisioned with the appropriate keys and certificates for communicating with the gateway.

The test system consists of both the front-end and back-end components is shown below.



A user laptop, portable encryptor and 5G modem are only required. Portable encryptor is the DUT that is to be evaluated and certified.

WiZ-Knight Portable Encryptor



Model Number	WK
Serial Number format	WK-YYZZZZZ YY is the year of manufacture ZZZZZ is the serial number ranging from 00001 - 99999

The device has a USB interface and can be used to connect to the user laptop. The device also includes three LEDs to indicate the different states of the device. The device also has a wireless interface to connect to the 5G router over Wi-Fi.

Required Software & Configuration

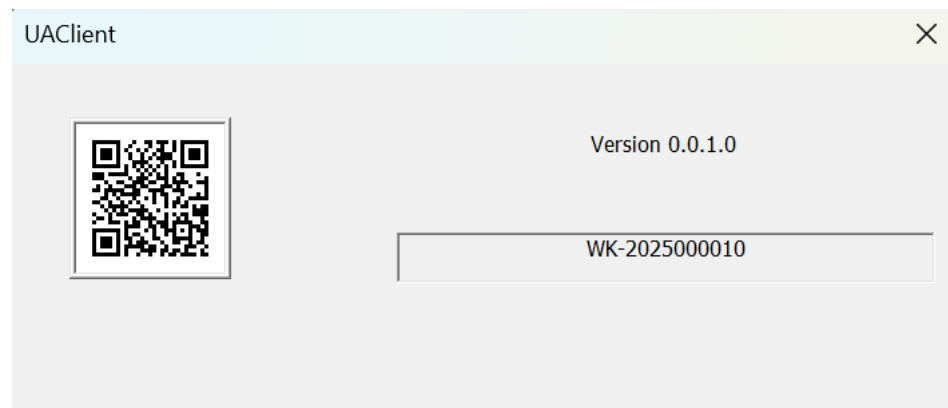
1. User Login Agent at Laptop
 - a. Install the user agent on your organization-issued laptop. This application will facilitate the initial connection between your mobile device and the dongle.
2. Mobile Application Installation
 - a. Install the mobile app on your mobile device.
 - i. For iOS devices please use the Apple App Store.
 - ii. For Android devices please use the Google Play Store or respective app store for your device.
3. User Laptop Installation of Certificates
 - a. Ensure that the user certificate has been installed on the organization-issued user laptop within the dedicated user certificate store. This certificate will authenticate the user, when using the dongle to connect to the gateway.
 - b. Ensure that the enterprise RCA/ICA certificate has also been installed into the trusted root certification authorities certificate store.

Dongle Test flow

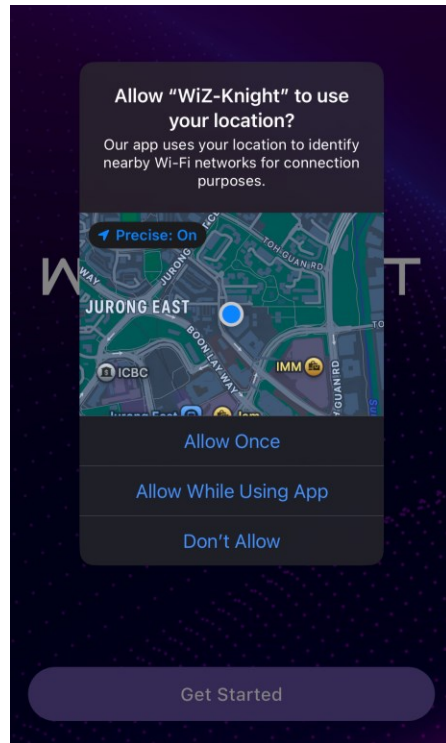
1. Connect the dongle to the user laptop via a USB-C cable.
2. The dongle will begin to boot up and all three LEDs will briefly light up. The VPN LED will switch to AMBER with greater intensity briefly. Then all three LEDs will switch OFF after booting up is complete.



3. On the user laptop, launch the user login agent application.
 - a. The application will display a QR code on the laptop screen.



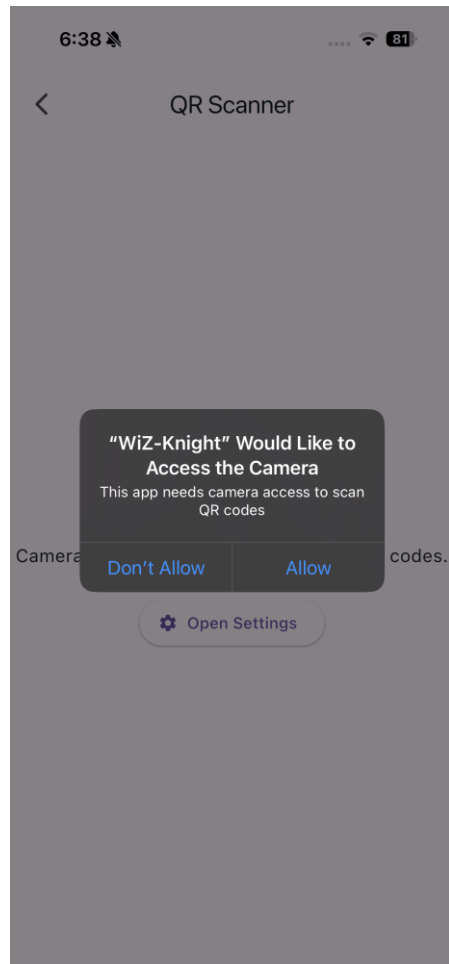
4. Connect the mobile application to the dongle to configure its wireless connectivity.
 - a. Launch the mobile application and accept any location permissions which appear.



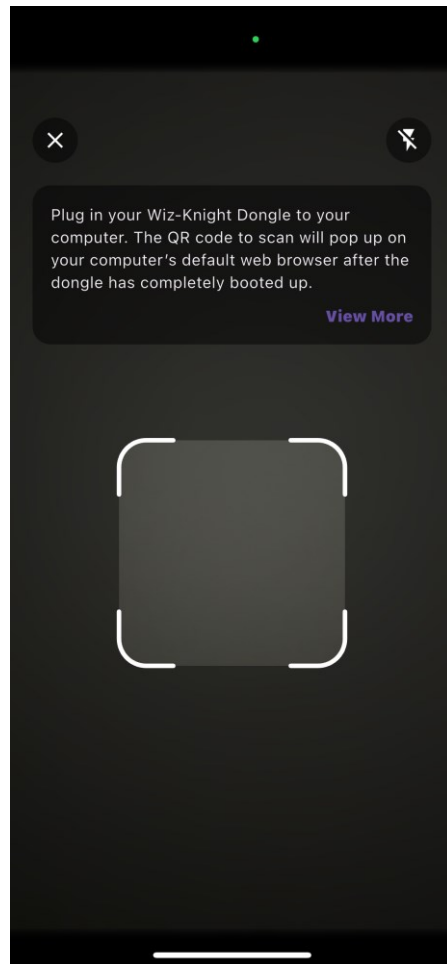
- b. After accepting location permissions, the main home screen of the app will be displayed.



- c. Tap on the "Get Started" button to begin scanning the QR code to connect the mobile app to the dongle.
- d. Accept any camera permission if required.



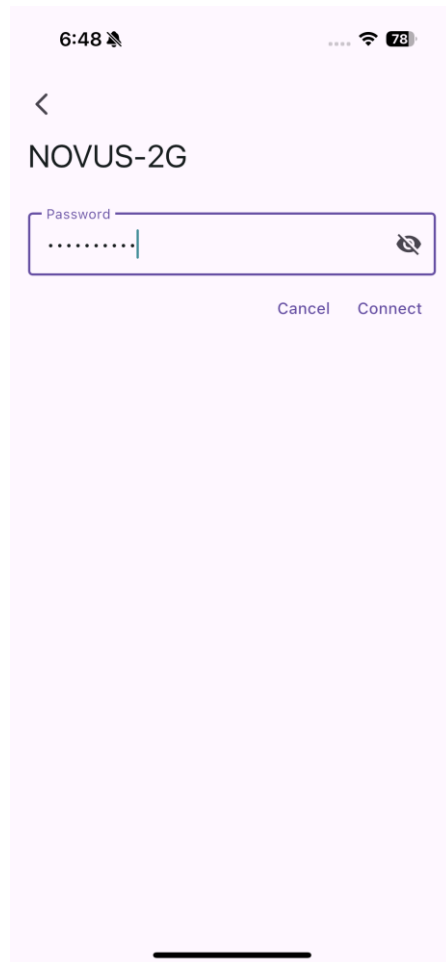
- e. Use the mobile device's camera to scan the QR code displayed on the user laptop screen.



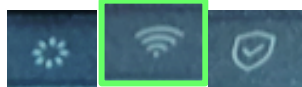
- f. The mobile application will attempt to connect to the dongle.
- g. Wait for the list of Wi-Fi networks to appear.



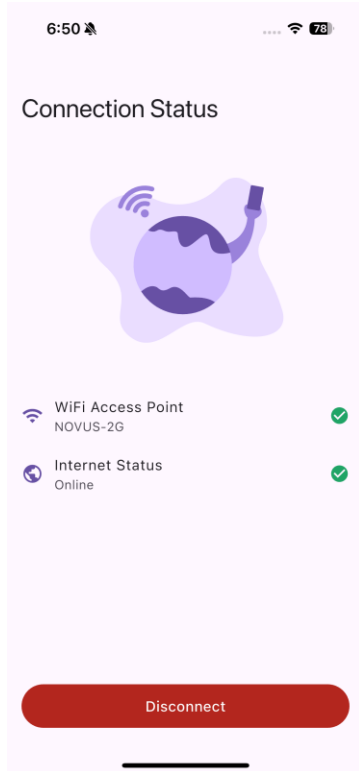
- h. On the mobile application, select the SSID of the wireless network you wish to connect to.
- i. Fill in the password and then click on the "Connect" button.



- j. The Wi-Fi LED on the must turn green on successful connection to the 5G router.



5. The mobile application will reflect the status of the connection.



6. Wait for the dongle to establish the secure tunnel automatically.
 - a. Wait and observe the state of the dongle's LEDs.
 - b. At the end of the process all three LEDs (status, Wi-Fi, VPN) will be lit GREEN.



7. You should now be able to access the enterprise network.
8. You should be able to ping a host on the enterprise network.

```
Ping statistics for 192.168.99.99:  
  Packets: Sent = 1427, Received = 1245, Lost = 182 (12% loss),  
Approximate round trip times in milli-seconds:  
  Minimum = 3ms, Maximum = 29ms, Average = 9ms  
Control-C
```



The device firmware is being improved for stability and self-recovery. Hence, during a connection drop, the test can be continued by power cycling the device.

FCC Compliance

Contains FCC ID: 2BTY5WKPE5XV1YM

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

*If it is difficult to describe this statement on the host product due to the size, please describe in the User's manual.

FCC CAUTION

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Compliance with FCC requirement 15.407(c)

Data transmission is always initiated by software, which is then passed down through the MAC, through the digital and analog baseband, and finally to the RF chip. Several special packets are initiated by the MAC. These are the only ways the digital baseband portion will turn on the RF transmitter, which it then turns off at the end of the packet. Therefore, the transmitter will be on only while one of the aforementioned packets is being transmitted. In other words, this device automatically discontinues transmission in case of either absence of information to transmit or operational failure.

Frequency Tolerance: ± 20 ppm

This transmitter must not be co-located or operated in conjunction with any other antenna or transmitter.



The SAR limit set by the FCC/IC is 1.6W/kg-1g. For close to head operation conditions, this device has been tested and meets the FCC/IC RF exposure guidelines. When used with an accessory, the accessory should not contain any metal element and positioned minimum of 0 mm from the body. RF exposure compliance with any accessory that contains metal was not tested and certified, and use of such accessory should be avoided.