Installation Instructions

1.1 Provided Hardware Items

Ethernet Cable

Guardian Module

USB A-B Cable

1.2 Claiming the Guardian Device to an Azure Sphere Tenant

The purpose of this document is to provide guidance to field personnel, on a simplified method to **configure the Wi-Fi settings** when installing a new Guardian device, without any requirement to open the Guardian enclosure or install Azure Sphere SDK on the laptop computer that is used.

This assumes however that the Guardian has already been "claimed" to an Azure Sphere tenant (previously setup for your organization). That one-time process must be completed from a computer:

a) on which Azure Sphere SDK has been installed, and
b) on which the user has logged-into the Azure Sphere tenant to which the device will be claimed (the Microsoft Azure Sphere documentation provides details of this process here)

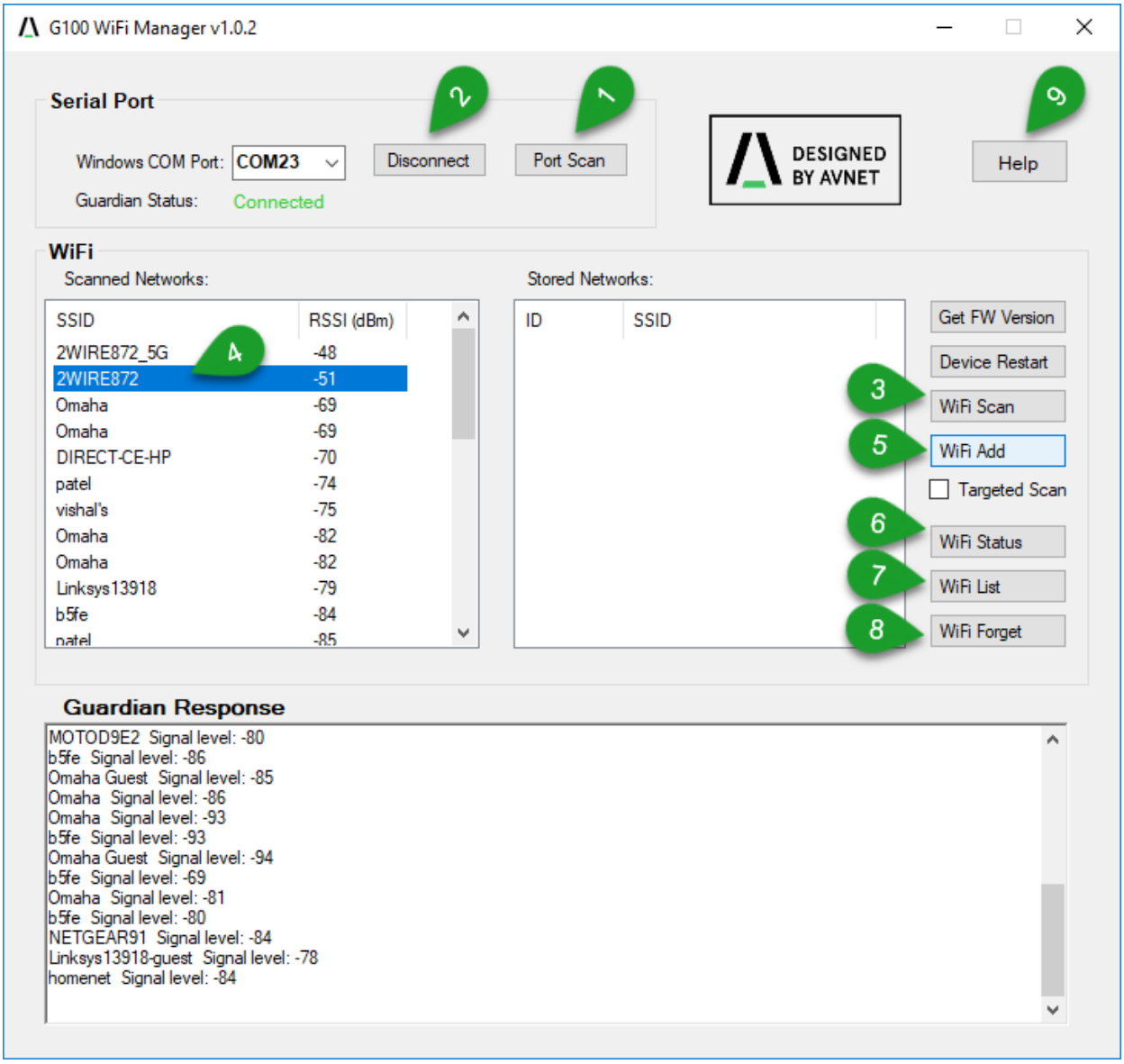
Note! Claiming a Guardian device to a tenant requires resources and actions not typically expected of a field installation person. It is recommended that all Guardian units be "claimed" at a central facility, prior to distribution to their end-destinations.

1.3 Wi-Fi Setup (using WiFi Manager Windows Application)

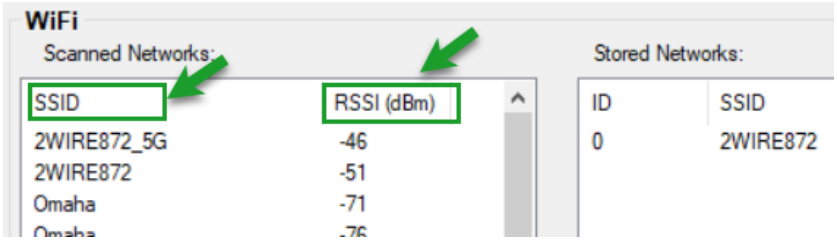
From April 2020, Guardian 100 ships with **WiFi Manager** embedded utility application programmed into flash memory. This facilitates a simplified field-setup of Guardian's non-volatile Wi-Fi settings, using just the supplied **USB-A to USB-B cable**, connected from Guardian's external USB-B connector, to a laptop computer where the only requirement is that it runs the provided **WiFi Manager Windows application**. (Note: Azure Sphere SDK installation is ***not*** required on this computer)

Check the Serial Number (SER) on Guardian's barcode label (located on the enclosure lid).
The last 4-digits represent a date code in YYWW format. Date codes of 2014 or later, confirm that the Guardian has been factory-programmed to auto-run the WiFi Manager application on power-up.

Names of Wi-Fi access points are selected and their passwords entered within the user-friendly Windows WiFi Manager application, ***without*** need for Azure Sphere SDK or access to Guardian's Debug USB port.



1) Connect the provided USB-A to USB-B cable from Guardian to the computer, then click on the "**Port Scan**" button to auto-populate the relevant Windows COM port in the drop-down list (The Ethernet cable does not need to be attached at this time)
2) Click the "**Connect**" button. The reported Guardian Status should change to **Connected**.
3) Click the "**WiFi Scan**" button. After a couple of seconds, a listing of Access Points will be reported in the Scanned Networks panel. Click on the RSSI column label to sort the reported results by signal strength (or click on the SSID column label, to sort this alphabetically)



4) Highlight the name of the Wi-Fi network for which password credentials will be entered

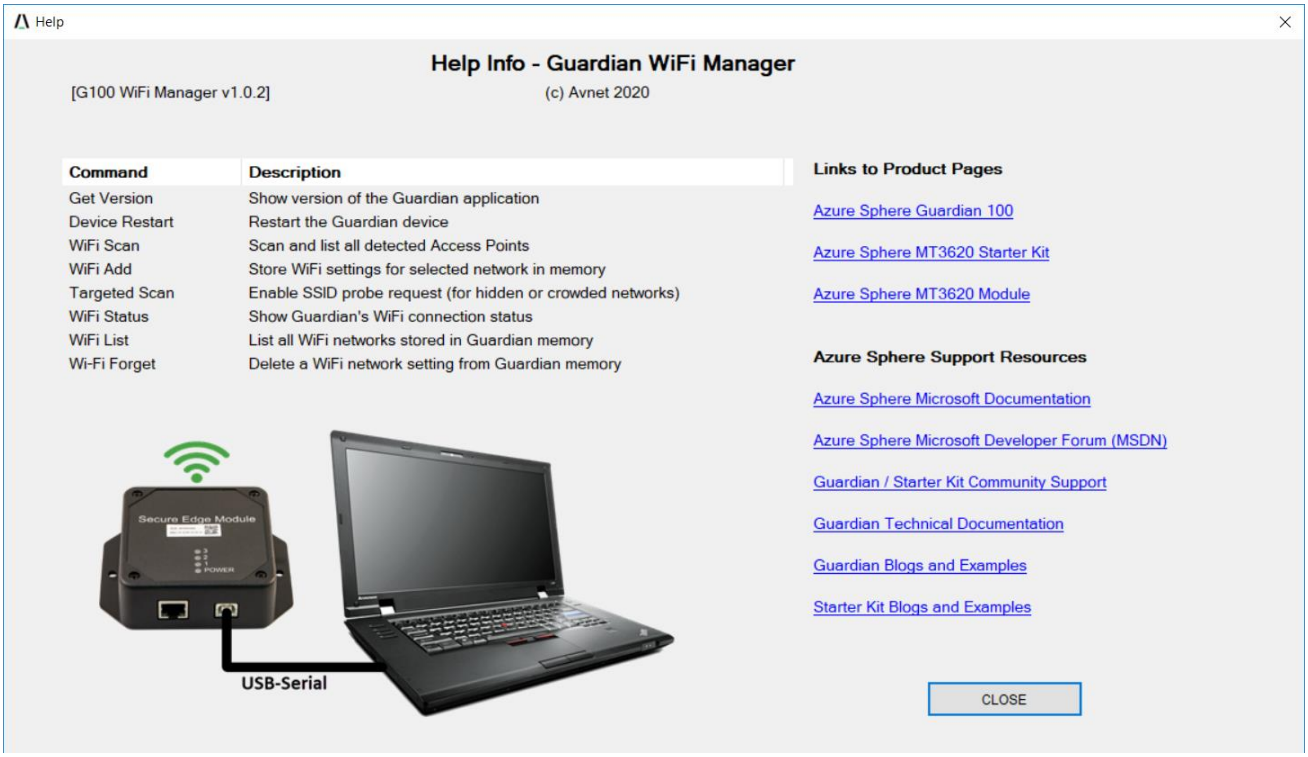
5) Click the "**WiFi Add**" button. A dialog window will open, prompting you to enter a password for this Wi-Fi network. The "**Targeted Scan**" checkbox is provided to provide a way to connect to networks whose name is not reported (due to hidden SSID, or where there is a lot of competing Wi-Fi activity). If this box is checked, you will be prompted to enter the SSID name in addition to the password)

6) Click the "**WiFi Status**" button (Pause 5 seconds before clicking, after Wi-Fi Add or WiFi Forget). This reports the name of the connected network as well as it's RSSI signal strength (in dB). Installation Tip: You can repeatedly press this **WiFi Status** button while positioning the Guardian for best signal strength (Note: Numerically lower -dB values indicate higher signal strengths)

7) Click the "**WiFi List**" button (Pause 5 seconds before clicking, after Wi-Fi Add or WiFi Forget) to get a listing of all currently stored networks

8) If a stored Wi-Fi network needs to be deleted or have it's Wi-Fi password credentials re-entered, highlight this network name in the Stored Networks panel, then click "**WiFi Forget**"

9) Click on the "Help" button to view additional setup and command information. Links to Avnet Azure Sphere product pages, documentation and technical support resources are also provided.



Notes:

- Click “**Get FW Version**” button to view version of WiFi Manager firmware installed on Guardian. An "*ERROR:timeout*” response implies that the utility has been deleted or overwritten. (This occurs when new applications are programmed into Guardian, via Debug USB connector, or via OTA from the Microsoft server. The stored Wi-Fi settings however remain persistent)

- A log file (G100_WiFi_Error_Log.txt) records locally any issues encountered during the session

1.4 Re-installing the WiFi Manager Embedded Application

The factory installed WiFi Manager application makes the Wi-Fi setup task for field installation personnel very much simpler. In a small percentage of cases the embedded application may need to be reinstalled (eg. if relocating equipment to a different location, or if needing to deploy Guardian units that were manufactured prior to April 2020)

Instructions on how to reinstall the WiFi manager application requires use of a computer on which Azure Sphere SDK has been installed. The procedure for re-programming this application into Guardian’s flash memory, is currently available on request via a separate Application Note document.