Wireless Network Security Assessment

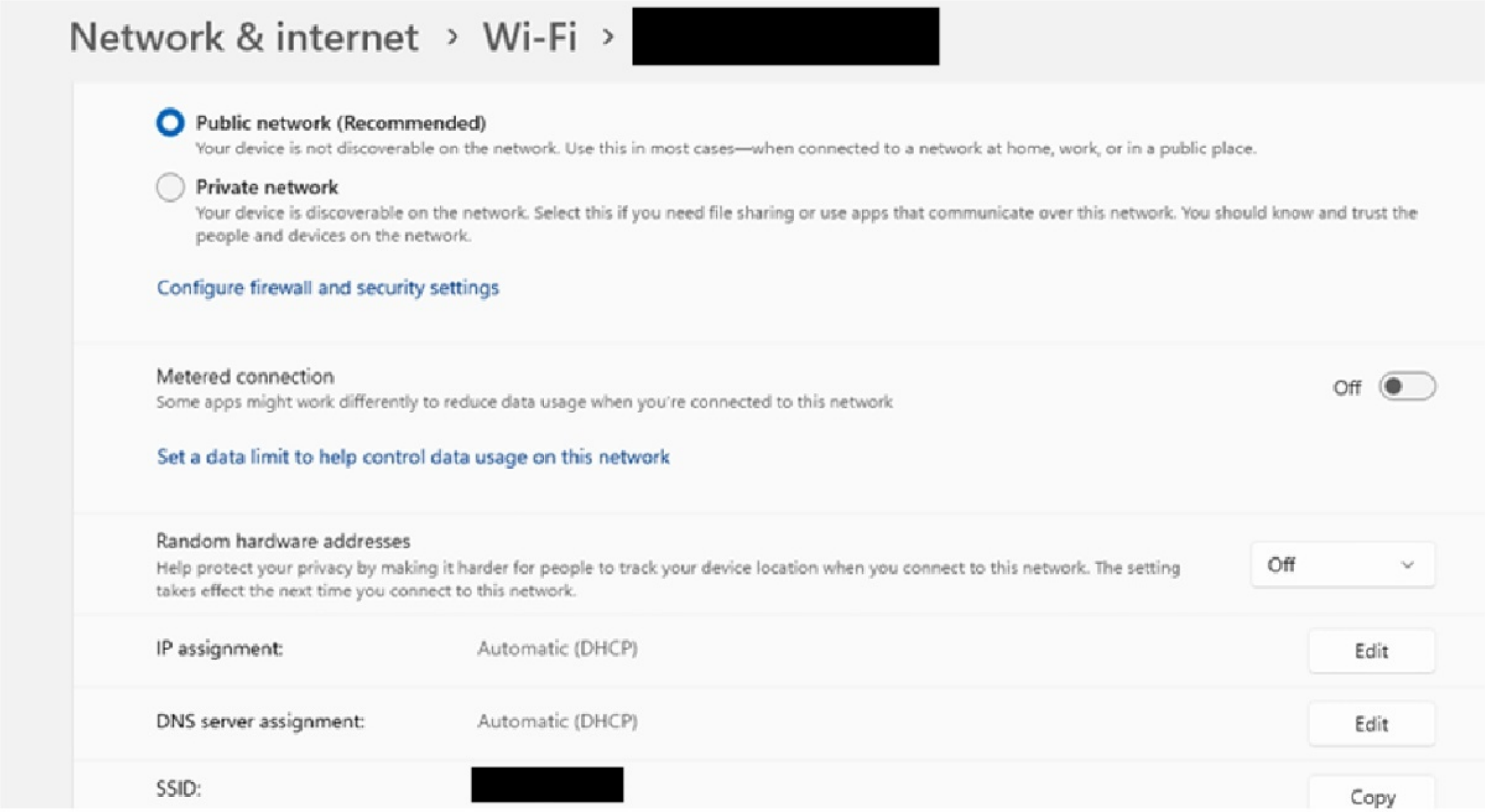
Created by: Lakpa Sherpa

Date: November 2025

Part 1: Network Discovery

Network Name (SSID)	Signal Strength	Security Type	Special Characteristics
1. [redacted] (Home Network)	Strong	WPA2	Personal Network

- The network name (SSID is [redacted], and it is a personal network.



Network & internet › Wi-Fi › [redacted]

● Public network (Recommended)
Your device is not discoverable on the network. Use this in most cases—when connected to a network at home, work, or in a public place.

○ Private network
Your device is discoverable on the network. Select this if you need file sharing or use apps that communicate over this network. You should know and trust the people and devices on the network.

Configure firewall and security settings

Metered connection
Some apps might work differently to reduce data usage when you're connected to this network
Off

Set a data limit to help control data usage on this network

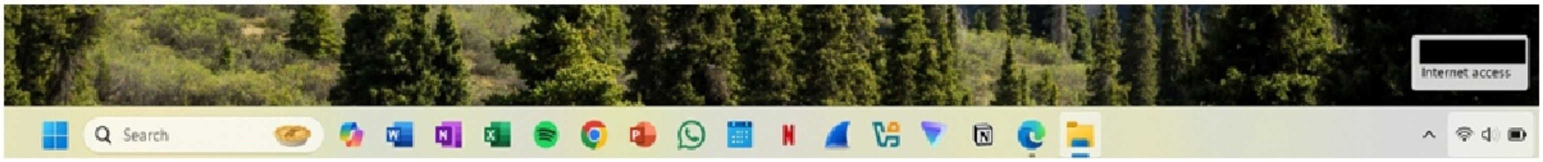
Random hardware addresses
Help protect your privacy by making it harder for people to track your device location when you connect to this network. The setting takes effect the next time you connect to this network.
Off

IP assignment: Automatic (DHCP) Edit

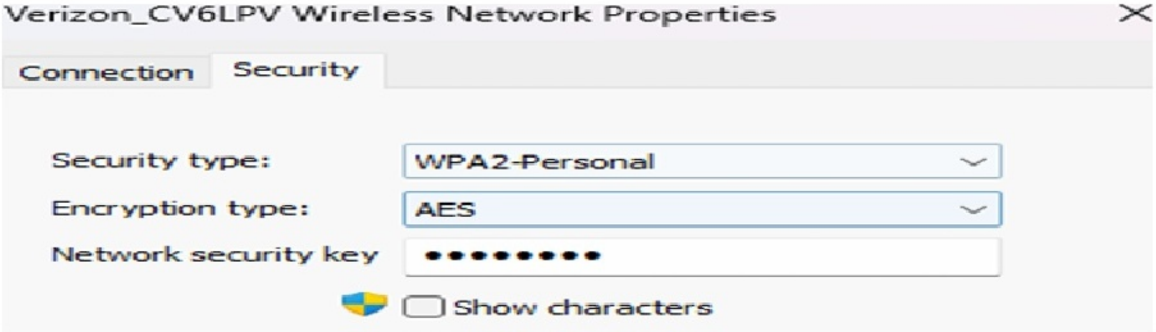
DNS server assignment: Automatic (DHCP) Edit

SSID: [redacted] Copy

- The signal strength is strong with a full tower.



- The Security type is WPA2.



Verizon_CV6LPV Wireless Network Properties

Connection | Security

Security type: WPA2-Personal

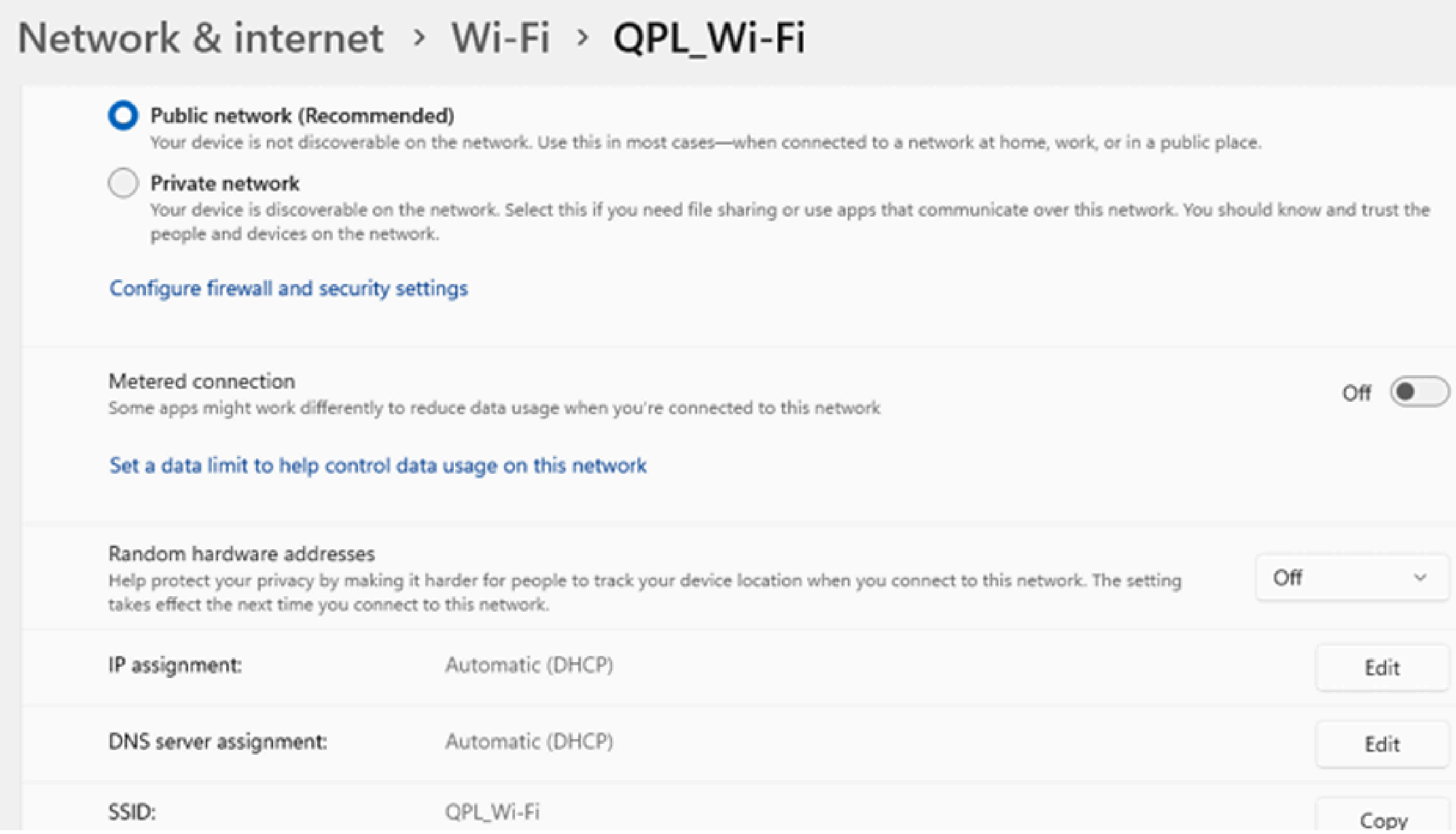
Encryption type: AES

Network security key ●●●●●●●●

□ Show characters

Network Name (SSID)	**Signal Strength**	**Security Type**	**Special Characteristics**
2. QPL_Wi-Fi (Queens Library)	Medium	Open	Public Wifi

- The Network name (SSID) is QPL_Wi-Fi, and it is a public network.



Network & internet › Wi-Fi › QPL_Wi-Fi

● Public network (Recommended)
Your device is not discoverable on the network. Use this in most cases—when connected to a network at home, work, or in a public place.

○ Private network
Your device is discoverable on the network. Select this if you need file sharing or use apps that communicate over this network. You should know and trust the people and devices on the network.

Configure firewall and security settings

Metered connection
Some apps might work differently to reduce data usage when you're connected to this network
Off

Set a data limit to help control data usage on this network

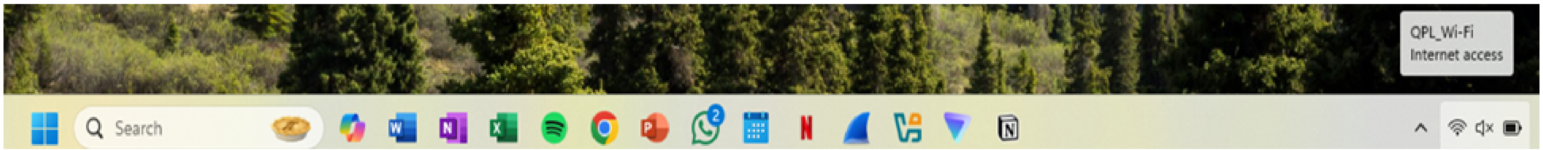
Random hardware addresses
Help protect your privacy by making it harder for people to track your device location when you connect to this network. The setting takes effect the next time you connect to this network.
Off

IP assignment: Automatic (DHCP) Edit

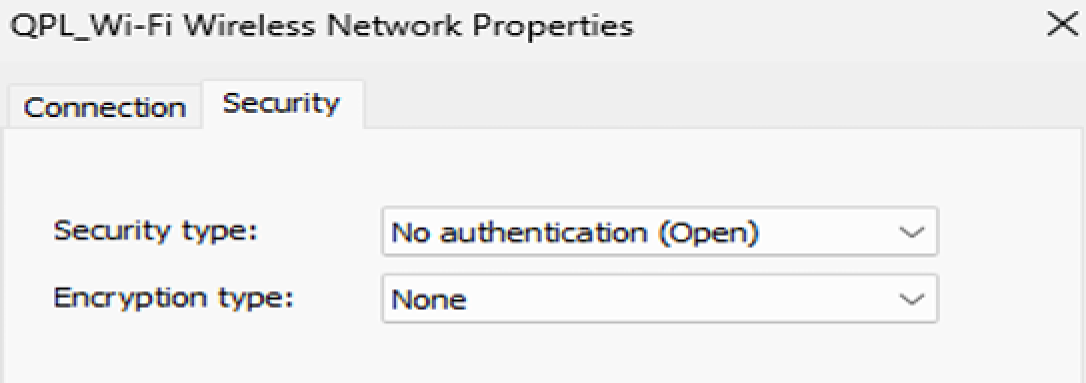
DNS server assignment: Automatic (DHCP) Edit

SSID: QPL_Wi-Fi Copy

- The Signal strength is strong with a full tower.



- The Security type is open, and it is not authenticated.



QPL_Wi-Fi Wireless Network Properties

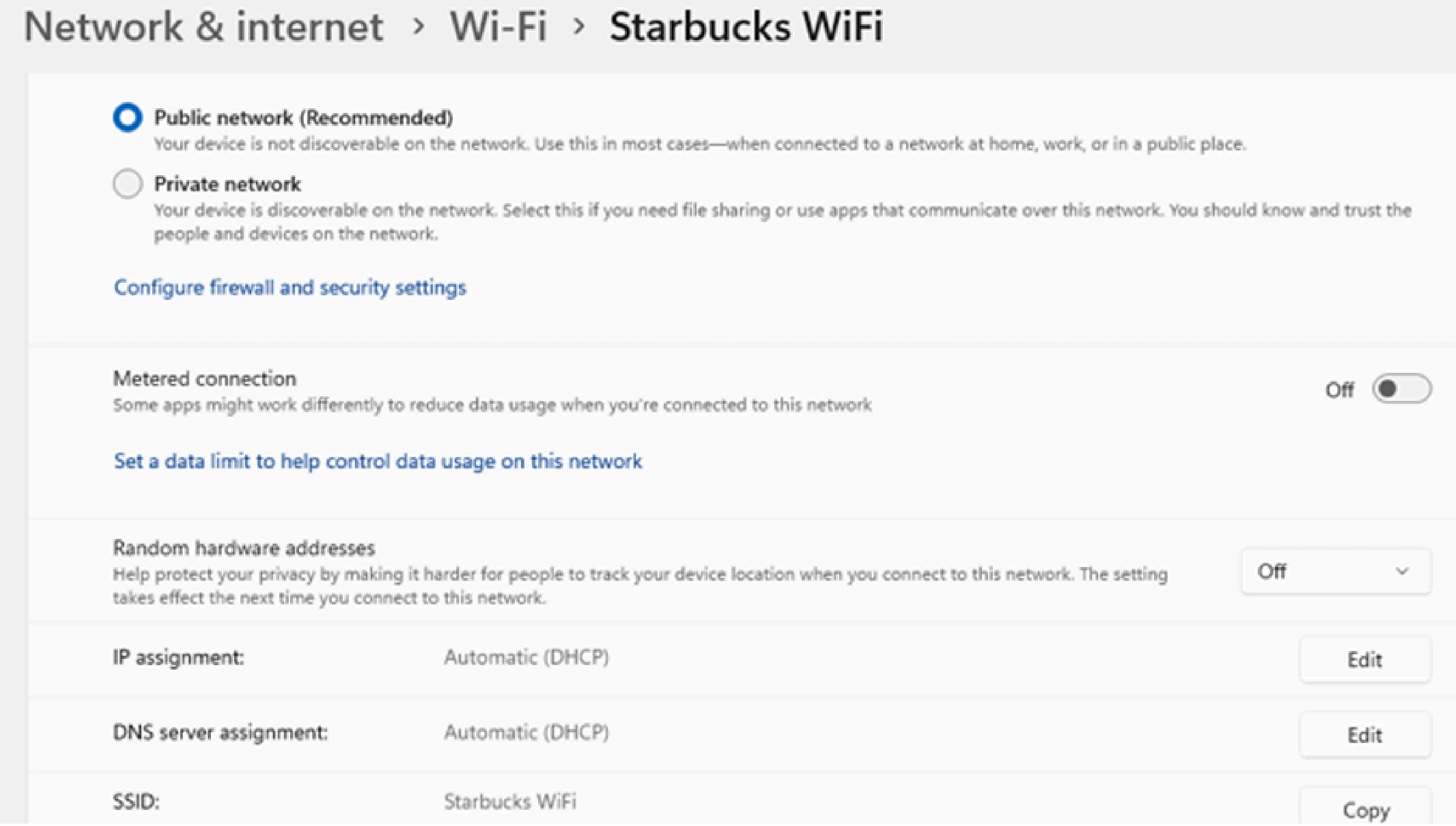
Connection | Security

Security type: No authentication (Open)

Encryption type: None

Network Name (SSID)	Signal Strength	Security Type	Special Characteristics
3. Starbucks WiFi (Cafe)	Medium	Open	Public Wifi

- The Network name (SSID) is Starbucks WiFi, and it is a public network.



Network & internet › Wi-Fi › Starbucks WiFi

● Public network (Recommended)
Your device is not discoverable on the network. Use this in most cases—when connected to a network at home, work, or in a public place.

○ Private network
Your device is discoverable on the network. Select this if you need file sharing or use apps that communicate over this network. You should know and trust the people and devices on the network.

Configure firewall and security settings

Metered connection
Some apps might work differently to reduce data usage when you're connected to this network
Off

Set a data limit to help control data usage on this network

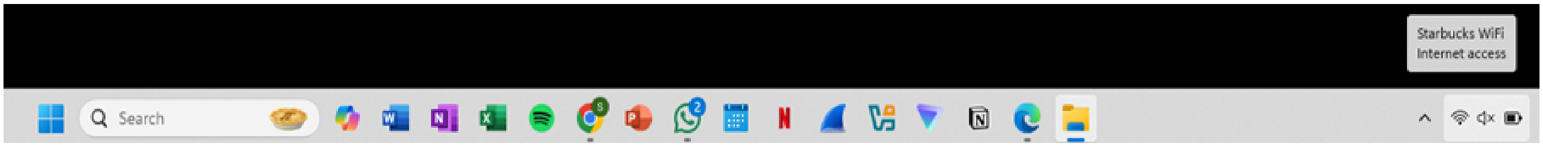
Random hardware addresses
Help protect your privacy by making it harder for people to track your device location when you connect to this network. The setting takes effect the next time you connect to this network.
Off

IP assignment: Automatic (DHCP) Edit

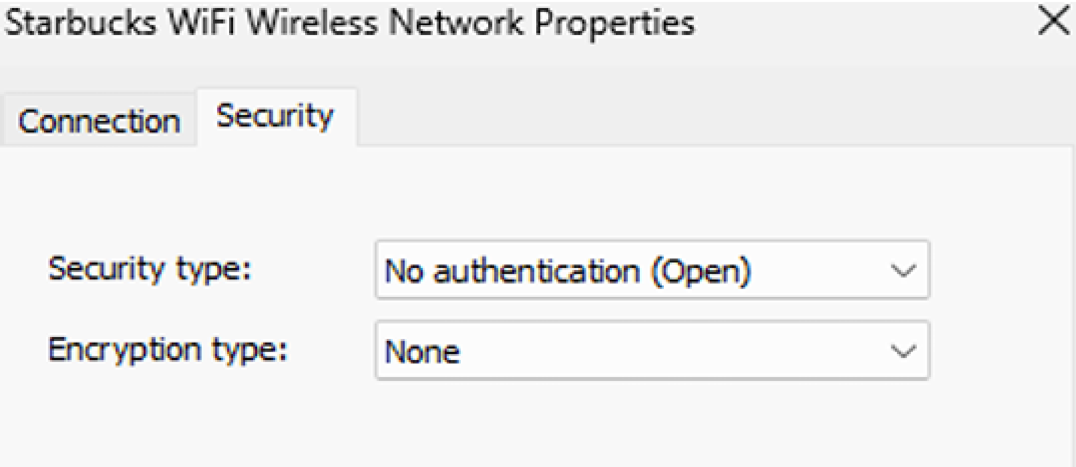
DNS server assignment: Automatic (DHCP) Edit

SSID: Starbucks WiFi Copy

- The Signal strength is strong with a full tower.



- The Security type is open, and it is not authenticated.



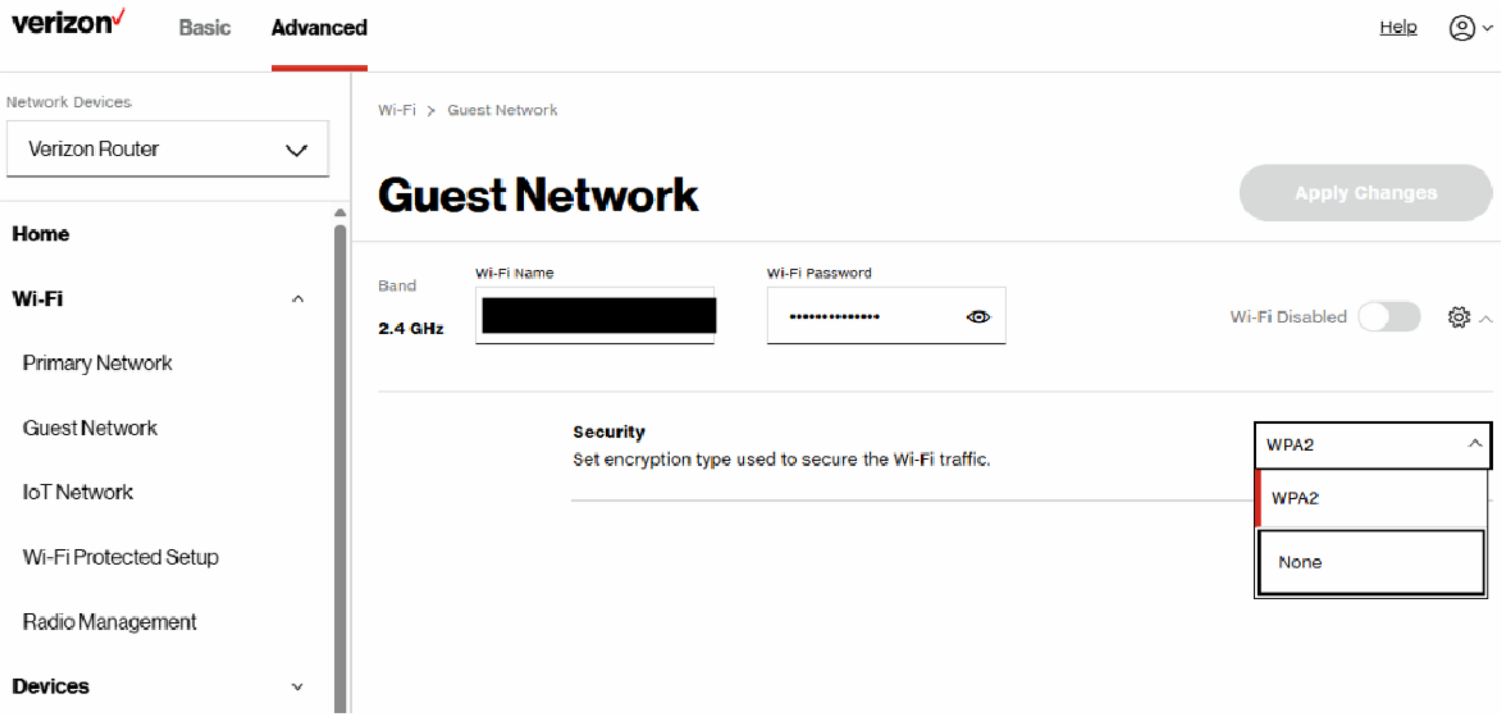
Starbucks WiFi Wireless Network Properties

Security type: No authentication (Open)

Encryption type: None

Part 2: Security Analysis for Home Network

- The network currently uses the WPA2 security protocol, which provides moderate protection but is less secure than WPA3.



Guest Network

Band: 2.4 GHz

Wi-Fi Name: [redacted]

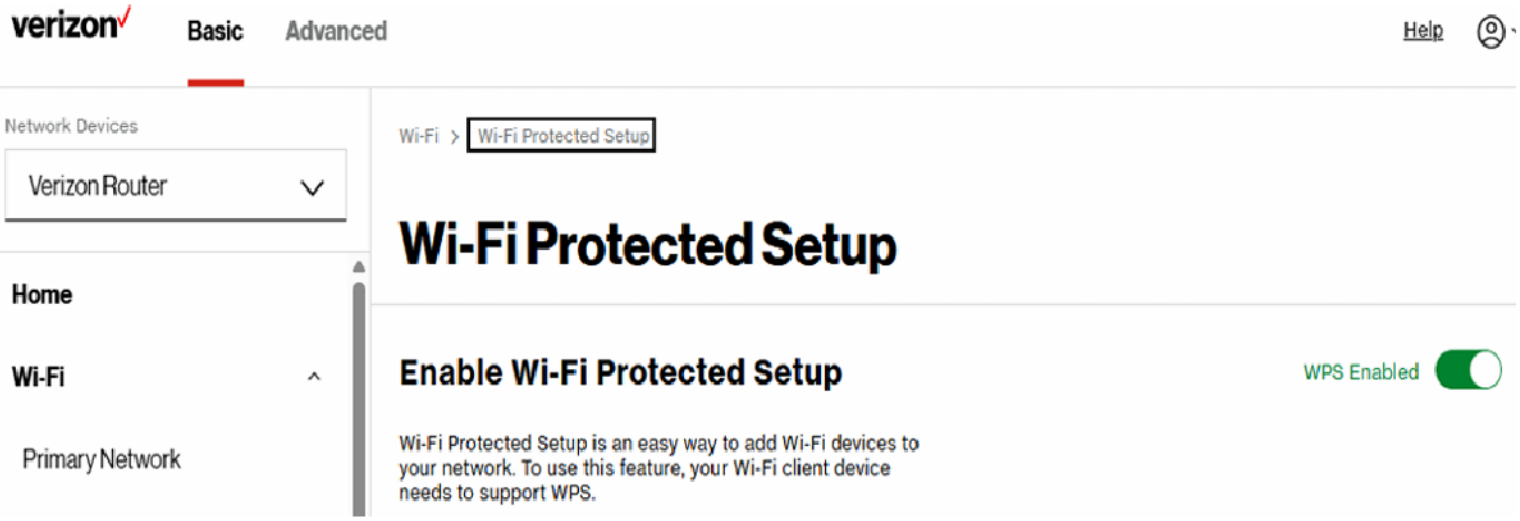
Wi-Fi Password: ••••••••••••••

Wi-Fi Disabled

Security
Set encryption type used to secure the Wi-Fi traffic.

WPA2
- WPA2
- None

- WPS (Wi-Fi Protected Setup) is currently enabled, which may expose the network to brute-force attacks.



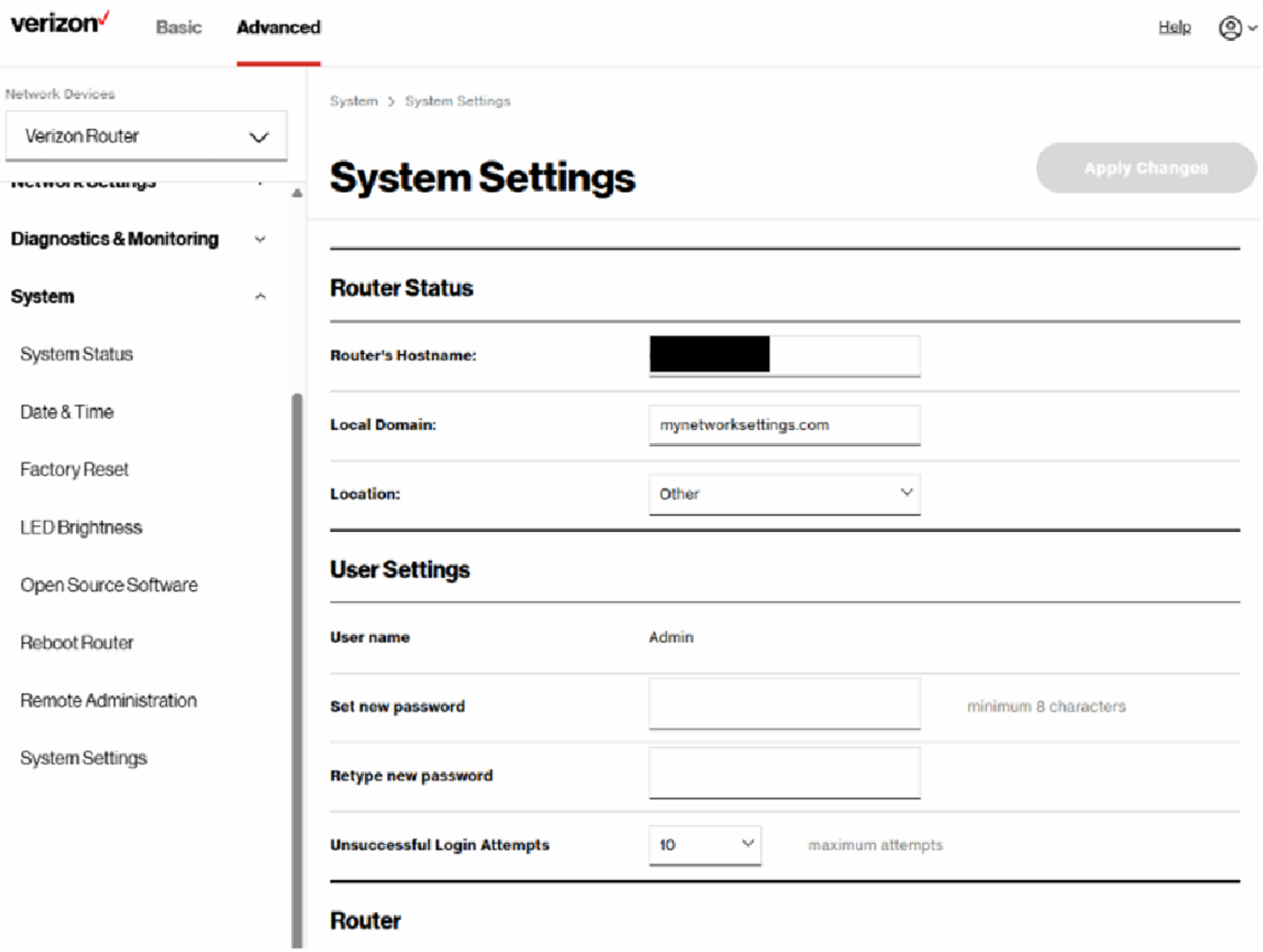
Wi-Fi Protected Setup

Enable Wi-Fi Protected Setup

WPS Enabled

Wi-Fi Protected Setup is an easy way to add Wi-Fi devices to your network. To use this feature, your Wi-Fi client device needs to support WPS.

- The default administrator password has not been changed, increasing the risk of unauthorized access.



System Settings

Router Status

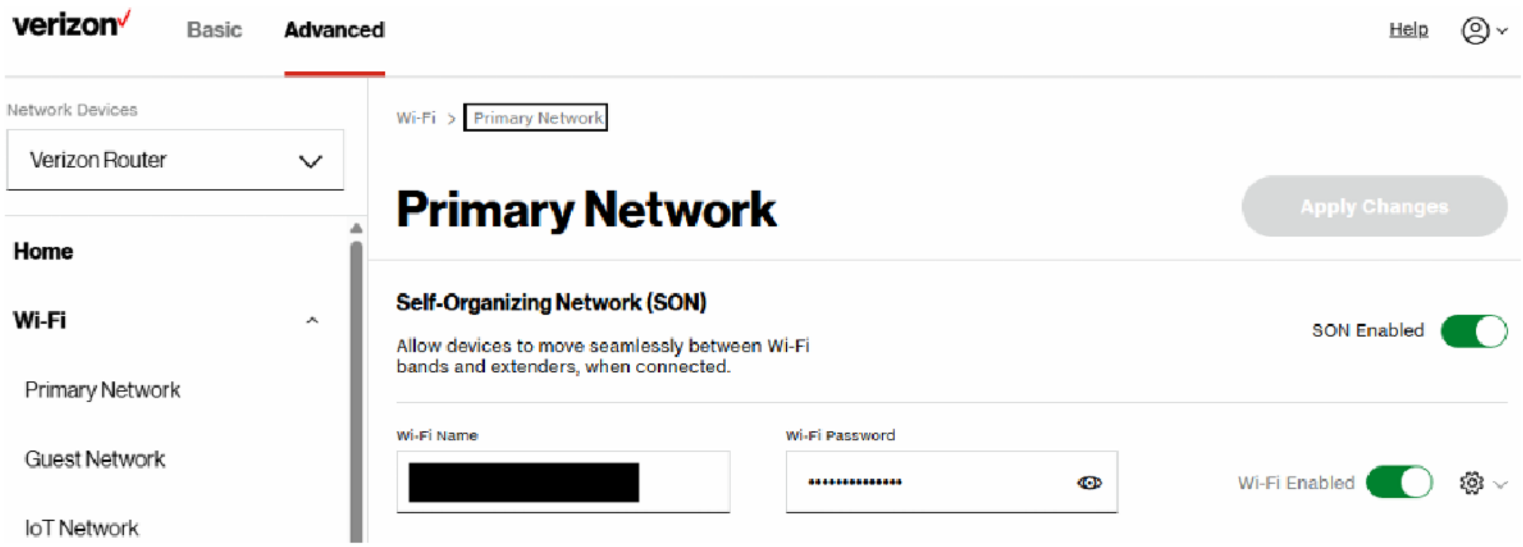
Router's Hostname:	[redacted]
Local Domain:	mynetworksettings.com
Location:	Other

User Settings

User name	Admin	
Set new password		minimum 8 characters
Retype new password		
Unsuccessful Login Attempts	10	maximum attempts

Router

- The network SSID is still using the default name, making it easily identifiable and less secure.



Primary Network

Self-Organizing Network (SON)

Allow devices to move seamlessly between Wi-Fi bands and extenders, when connected.

SON Enabled

Wi-Fi Name	Wi-Fi Password	
[redacted]	••••••••••••••	Wi-Fi Enabled

Part 3: Potential security issues

- The home router configuration contains several settings that may expose the network to risk.

- The network currently uses WPA2 encryption, which provides adequate protection but lacks the stronger security features of WPA3.

- WPS (Wi-Fi Protected Setup) is enabled, increasing the likelihood of brute-force or PIN-based attacks if exploited by an attacker.

- The default administrator password has not been changed, leaving the management interface vulnerable to unauthorized access.

Part 4: Improvement Plan

To strengthen my home network's security posture:

1. Change the default administrator password to a strong, unique passphrase stored securely in a password manager.

2. Disable WPS (Wi-Fi Protected Setup) to eliminate potential brute-force vulnerabilities. Although this will require manually entering the Wi-Fi password for new devices, it significantly reduces risk.

3. Upgrade to WPA3 encryption if supported by the router and connected devices, as it offers improved encryption and authentication mechanisms compared to WPA2.

4. Rename the SSID (Wi-Fi network name) to remove default identifiers and avoid revealing the router's make or model. Optionally, hide the SSID to reduce network visibility in public scans.

Implementing these steps will enhance the overall security of the wireless network and help prevent unauthorized access or compromise.

.