

WorryFree Wi-Fi Analyzer

For Version 3.4.x



ZEBRA

Administrator Guide
for Android™

Copyright

ZEBRA and the stylized Zebra head are trademarks of Zebra Technologies Corporation, registered in many jurisdictions worldwide. All other trademarks are the property of their respective owners. © 2019 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

COPYRIGHTS & TRADEMARKS: For complete copyright and trademark information, go to www.zebra.com/copyright.

WARRANTY: For complete warranty information, go to www.zebra.com/warranty.

END USER LICENSE AGREEMENT: For complete EULA information, go to www.zebra.com/eula.

Terms of Use

- **Proprietary Statement**

This manual contains proprietary information of Zebra Technologies Corporation and its subsidiaries (“Zebra Technologies”). It is intended solely for the information and use of parties operating and maintaining the equipment described herein. Such proprietary information may not be used, reproduced, or disclosed to any other parties for any other purpose without the express, written permission of Zebra Technologies.

- **Product Improvements**

Continuous improvement of products is a policy of Zebra Technologies. All specifications and designs are subject to change without notice.

- **Liability Disclaimer**

Zebra Technologies takes steps to ensure that its published Engineering specifications and manuals are correct; however, errors do occur. Zebra Technologies reserves the right to correct any such errors and disclaims liability resulting therefrom.

- **Limitation of Liability**

In no event shall Zebra Technologies or anyone else involved in the creation, production, or delivery of the accompanying product (including hardware and software) be liable for any damages whatsoever (including, without limitation, consequential damages including loss of business profits, business interruption, or loss of business information) arising out of the use of, the results of use of, or inability to use such product, even if Zebra Technologies has been advised of the possibility of such damages. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Revision History

Changes to the original guide are listed below:

Change	Date	Description
-01 Rev A	7/2019	Initial release.

Table of Contents

Copyright	2
Terms of Use	2
Revision History	2
About This Guide	5
Introduction	5
Product Support	5
Best Practices	5
Chapter Descriptions	6
WFW Analyzer Use Cases	7
Notational Conventions	8
Provide Documentation Feedback	8
Using WFW Analyzer	9
Introduction	9
Opening WFW Analyzer	10
Enabling Real-Time Analysis	10
Home Screen	11
Status	11
Connected IP Network	12
Device Information	13
Scan List	14
Filter Options	14
Detailed Capabilities for BSSID	15
Connection Analysis	17
Module Selections	18
Results	19
Setting Network Parameters	20
Networking Tools	22
Ping	22

Table of Contents

Ping Settings	22
TraceRoute	24
Device's Coverage View	26
Auto Reachability Test	27
Logging	28
Logging Management Packets	28
Logging All Packets	29
Fusion Advanced Configuration	30
About	31
Camera Preview	32
Configuration	33
Configuration Using Mobility Extensions	33
Configuration Using StageNow	33
Setting the Password	33
Packet Capture	37
Introduction	37
Features	37
Supported Packet Types	38
Supported Headers and Content	38

About This Guide

Introduction

This guide provides information for the WorryFree Wi-Fi Analyzer (WFW Analyzer) app (formerly SmartMU).



NOTE: It is not recommended to set the Font size and Display size on the device to larger than the default.

Product Support

WFW Analyzer version 3.4.x is available on the following devices running Android Oreo.

- TC52
- TC57
- TC72
- TC77
- PS20
- EC30
- TC83
- MC93
- VC83
- L10A
- CC6000

Best Practices

For the best experience while using WFW Analyzer:

- It is not recommended to change the Font size and Display size on the device from the default. Adjusting the Font size or Display size may cause the WFW Analyzer app to not display correctly.
- It is not recommended to use Multi-Window mode. Using Multi-Window mode may cause the WFW Analyzer app to not display correctly.
- Ensure the primary user is logged into the device. The Android multi-user feature is not supported by the WFW Analyzer app.

- Do not change the Wi-Fi settings on the device while actively using a WFW Analyzer feature. This applies to the WFW Analyzer app or WFW Analyzer configuration using a Mobile Device Manager (MDM).
- Packet capture and networking tools can run at the same time as another WFW Analyzer feature. This applies to the WFW Analyzer app or WFW Analyzer configuration using an MDM.
- Do not run Ping using a short time interval if also running other WFW Analyzer feature(s) at the same time. This applies to the WFW Analyzer app or WFW Analyzer configuration using an MDM.
- If the Connection Analysis feature is started using a staging tool or an MDM, do not start another feature from the WFW Analyzer app until the connection analysis is complete.
- Each time the Connection feature starts, the device disconnects and then reconnects to the network. When using this feature to analyze the Wi-Fi connection of a device and test the traffic of another app, it is highly recommended to start the analysis feature before starting the other app. This prevents interruption of the Wi-Fi connection during the test. Other WFW Analyzer features do not interrupt the Wi-Fi connection.
- It is not recommended to toggle the Analyzer Activated switch while using a WFW Analyzer feature. Toggling the switch resets the radio and interrupts the Wi-Fi connection.

Chapter Descriptions

Topics covered in this guide are:

- [Using WFW Analyzer](#) describes how to use the WFW Analyzer app.
- [Configuration](#) describes how to use the WFW Security app.
- [Packet Capture](#) provides detailed information about WFW Security packet captures.

WFW Analyzer Use Cases

Analysis data provided by WFW Analyzer saves time and cost by allowing administrators to quickly improve or mitigate performance issues. Actions may include reconfiguring the RF or WLAN system, reconfiguring the device, or locating an issue that requires further investigation.

The following table describes some of the common WFW Analyzer use cases.

Table 1 Use Cases

Summary	Detailed Description	WFW Analyzer Feature
Basic connectivity information.	View the status of the connected device, including the connected AP, RSSI, channel, and IP/DHCP/DNS.	Home screen
WiFi surveys and coverage from the mobile device view.	View multiple networks and access points (APs) from locations within radio frequency (RF) range of the device. View connectivity and roam events. Perform an auto reachability test from connected APs to the gateway. Verify the APs over-the-air advertised data, retrieved directly from the information elements of the AP packets.	Scan List Device Coverage View
WiFi connection analysis.	On demand troubleshooting of initial and full associations to the SSID and IP network, including reasons and sub-protocols triggering a connection failure.	Connection Analysis
Packet capture for off-line analysis using a computer.	Enabled packet capture to automatically save packets to pcap format. Content includes 802.11-header and radiotap.	Logging
Troubleshoot and compare Fusion configuration parameters.	View the band preference or power save parameters to compare configurations. Test configurations on-site without waiting for a configuration update from a software patch or central staging.	Fusion Advanced Config
Network reachability and performance testing.	Run one or two independent pings at the same time, each with a separate configuration of the packets and destination. Validate performance and simulate an app's required concurrency of network destinations. Use TraceRoute to display the route (path) and transit delays of packets across an IP network to a set destination.	Network Tools > Ping / TraceRoute

Notational Conventions

This document uses the following conventions:

- **Bold** text is used to highlight the following:
 - Dialog box, window and screen names
 - Drop-down list and list box names
 - Check box and radio button names
 - Icons on a screen
 - Key names on a keypad
 - Button names on a screen.
- Bullets (•) indicate:
 - Action items
 - Lists of alternatives
 - Lists of required steps that are not necessarily sequential.
- Sequential lists (e.g., those that describe step-by-step procedures) appear as numbered lists.

Provide Documentation Feedback

If you have comments, questions, or suggestions about this guide, send an email to EVM-Techdocs@zebra.com.

Using WFW Analyzer

Introduction

This chapter describes the following WFW Analyzer features:

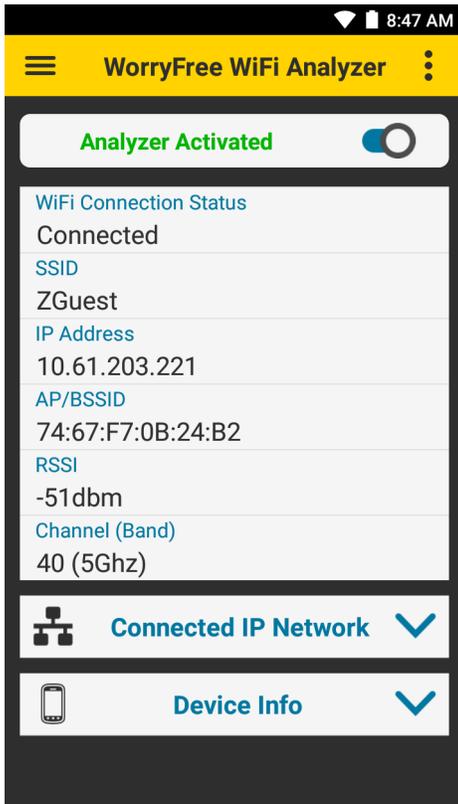
- [Opening WFW Analyzer on page 10](#)
- [Home Screen on page 11](#)
- [Scan List on page 14](#)
- [Connection Analysis on page 17](#)
- [Networking Tools on page 22](#)
- [Device's Coverage View on page 26](#)
- [Logging on page 28](#)
- [Fusion Advanced Configuration on page 30](#)
- [About on page 31](#)
- [Camera Preview on page 32](#)

Opening WFW Analyzer

Before using WFW Analyzer, ensure that Wi-Fi is enabled on the device. For information on how to enable Wi-Fi, refer to the user guide for your device.

To open the WFW Analyzer app, swipe up from the bottom of the Home screen and touch .

Figure 1 WFW Analyzer Screen



Enabling Real-Time Analysis

By default, analysis and data collection features are disabled. Only previously collected data is available for viewing.

To enable analysis and data collection features, from the Main Menu or Home screen, touch the **Analyzer Not Activated** switch. The Wi-Fi connection restarts and the analysis and data collection features are enabled.

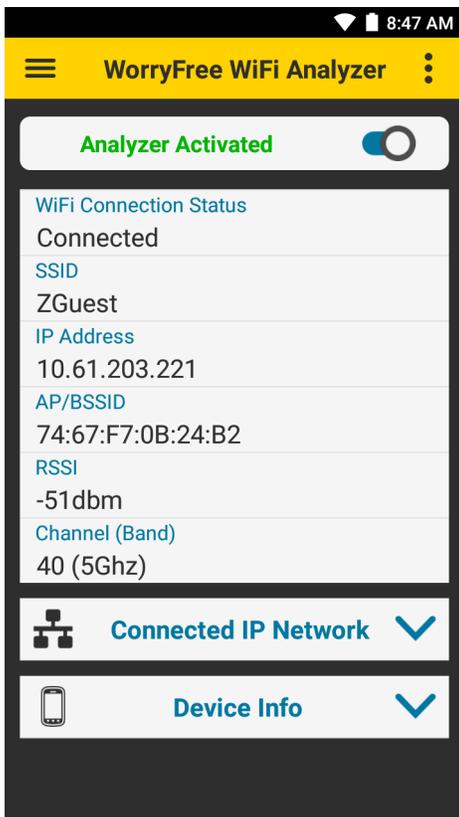
When not using analysis features, it is recommended to disable them. To disable the analysis and data collection features, from the Main Menu or Home screen, touch the **Analyzer Activated** switch. The Wi-Fi connection restarts and the analysis and data collection features are disabled.

Home Screen

The **Home** screen displays:

- Device status
- Connected IP Network
- Device Information.

Figure 2 Home Screen



Home screen information continues updating when analysis and data collection are disabled.

Status

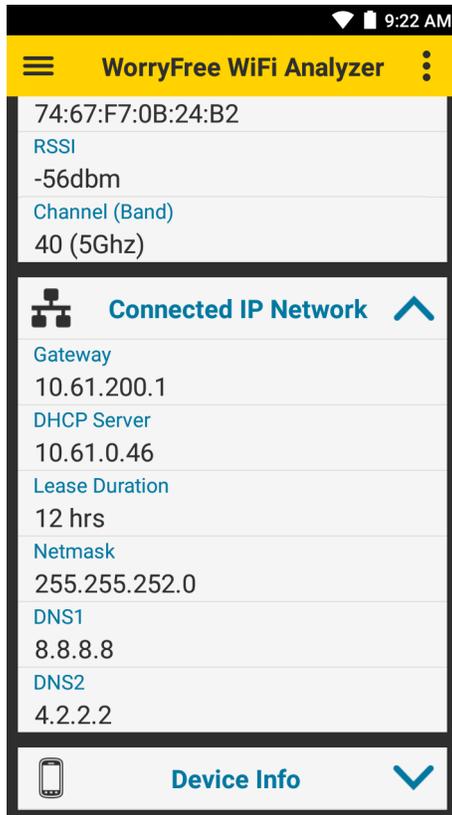
The Home screen displays the current device status.

- **WiFi Connection Status** - Current connection status
- **SSID** - Name of the connected WLAN network
- **IP Address** - IP address of the device
- **AP/BSSID** - Basic Service Set ID (BSSID) of the connected access point
- **RSSI** - RSSI of the connected access point
- **Channel (Band)** - Displays the channel.

Connected IP Network

To view the following details of the connected IP network, touch the down arrow next to **Connected IP Network**.

Figure 3 Connected IP Network

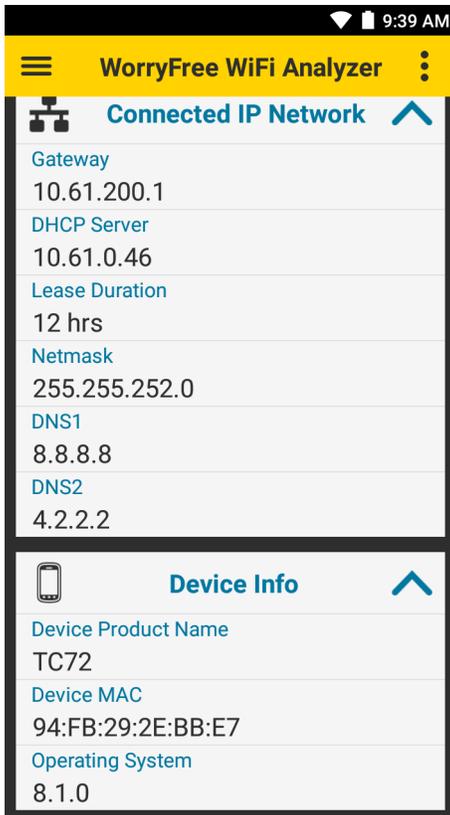


- **Gateway** - IP address of the network gateway
- **DHCP Server** - IP address of the DHCP server
- **Lease Duration** - Amount of time the IP address of the device is leased. The device renews the lease before the lease duration expires.
- **Netmask** - Server subnet mask address
- **DNS1** - Domain Name System 1 (DNS1) address
- **DNS2** - DNS2 address.

Device Information

To view the following device information, touch the down arrow next to **Device Info**.

Figure 4 Device Info



- **Device Product Name**
- **Device MAC**
- **Operating System.**

Scan List

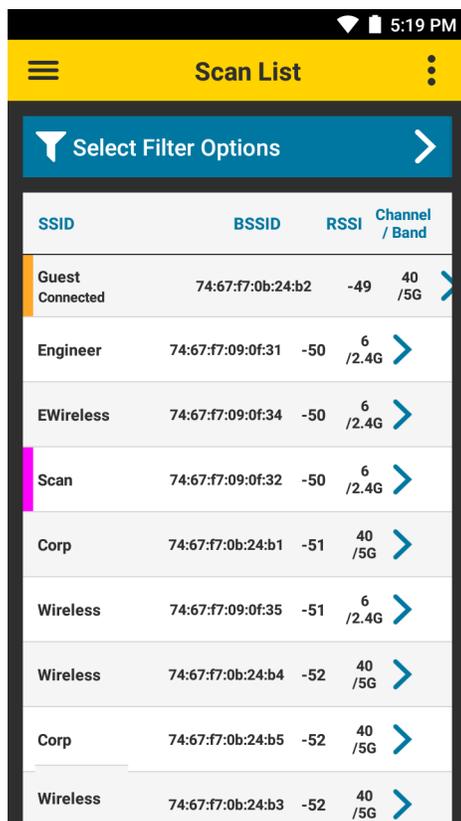
The **Scan List** main screen displays a list of BSSIDs and their corresponding SSIDs, RSSI, and channels. The first row displays the currently connected BSSID, unless the connected SSID is filtered out using **Select Filter Options**, or the device is not connected at all. All other rows are sorted and filtered according to the filter options. See [Filter Options on page 14](#).

When Wi-Fi is disabled, the **Scan List** can display results using Wi-Fi Scanning. Filter Options and Detailed Capabilities for BSSID are not supported when using Wi-Fi Scanning.

The **Scan List** includes all BSSIDs with the same country, band, configuration, and WLAN protocols as the current channel. Wi-Fi Direct SSIDs are not supported.

To view the **Scan List**, touch **☰ > Scan List**.

Figure 5 Scan List



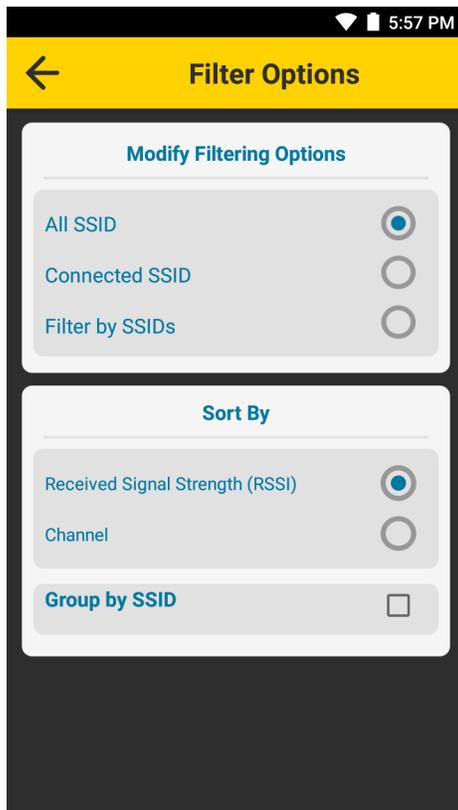
For each BSSID, the following displays:

- **BSSID** - MAC address of the access point BSSID
- **RSSI** - Received signal strength in dBm. The closer the dBm number is to zero, the stronger the signal.
- **SSID** - Name of an 802.11 wireless local area network (WLAN)
- **Channel/Band** - Channel and frequency band.

Filter Options

From the **Scan List** screen, touch **Select Filter Options** to filter networks.

Figure 6 Filter Options

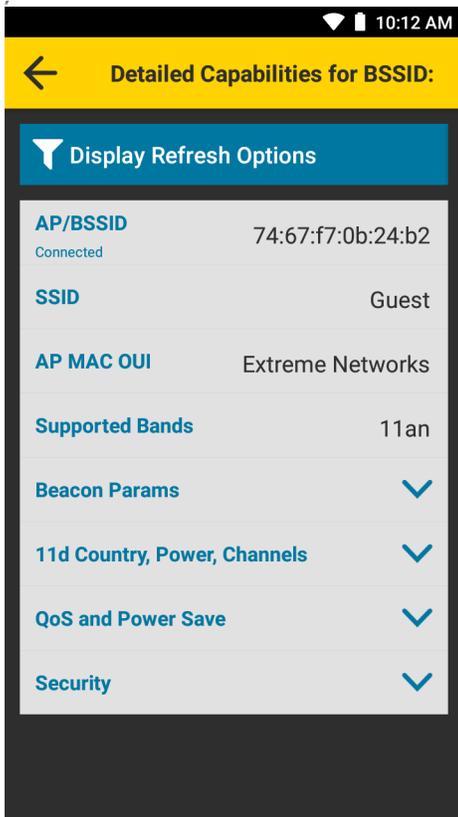


- **Modify Filtering Options** - Select to filter the Scan List using one of the following options:
 - **All SSID** - Display BSSIDs of all SSIDs (default)
 - **Connected SSID** - Display BSSIDs of only the connected SSID
 - **Filter by SSIDs** - Touch to display a list of SSIDs. Select an SSID to enable or disable view of its corresponding BSSIDs in the Scan List.
- **Sort By** - Select to sort the Scan List by **Received Signal Strength (RSSI)** (default), or **Channel**.
- **Group by SSID** - Select to group SSIDs with the same name together. SSIDs are listed in alphabetical order.

Detailed Capabilities for BSSID

From the **Scan List** screen, touch a BSSID to display detailed capabilities.

Figure 7 Detailed Capabilities for BSSID



- **AP/BSSID** - Displays the MAC address of the access point BSSID.
- **SSID** - Displays the WLAN network name corresponding to the BSSID.
- **AP MAC OUI** - Displays the Organizationally Unique Identifier (OUI). When an organization was not assigned an identifier, or an identifier was recently assigned by the IEEE Registration Authority, this value is empty.
- **Supported Bands** - Displays the notation of the supported 802.11 standard for the associated 2.4 GHz or 5 GHz band.

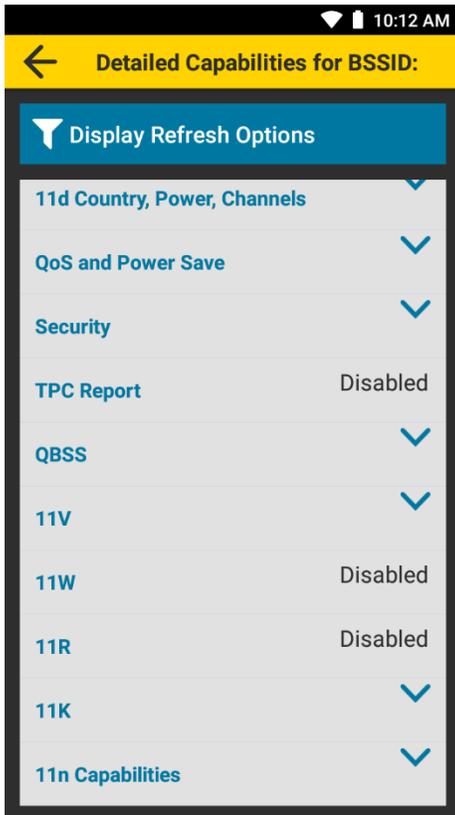
A physical AP is typically dual-band, where each band of the AP has a unique BSSID identifier, so each BSSID of the AP is listed as a unique item on the Scan List main screen.

- **Beacon Params** - Touch the down arrow next to **Beacon Params** to view the beacon interval.
- **11d Country, Power, Channels** - Touch the down arrow to view details.
- **QoS and Power Save** - Touch the down arrow next to **QoS and Power Save** to view QoS and Power Save information.

Some APs do not support **QoS and Power Save**. If **Not Supported** displays, it is recommended to check the AP's Wi-Fi Multimedia (WMM) settings in the AP packets using packet capture. See [Packet Capture on page 37](#).

- **Security** - Touch the down arrow next to **Security** to view security WLAN information.

Figure 8 Detailed Capabilities for BSSID - Continued



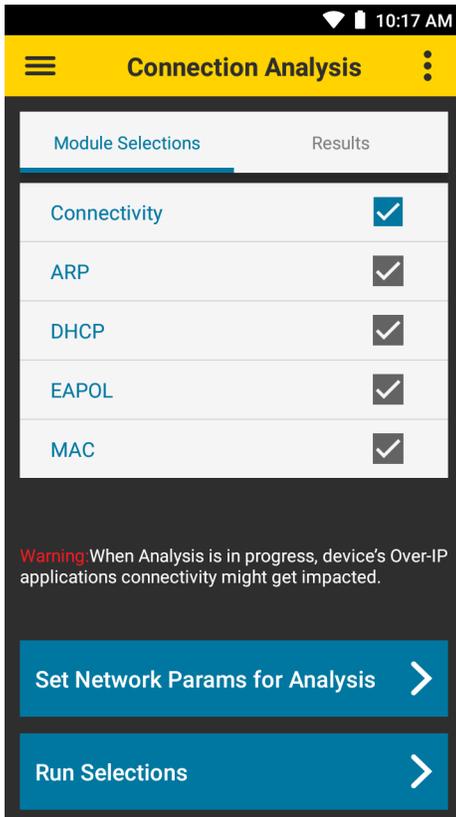
- **TPC Report** - Displays whether Transmit Power Control is enabled.
- **QBSS** - Touch the down arrow to view the QoS enhanced basic service set values such as station count, channel utilization.
- **11V** - Touch the down arrow to view if the BSS Transition is enabled.
- **11W** - Displays whether 11w is enabled.
- **11R** - Displays whether 11r is enabled.
- **11K** - Touch the down arrow to view if the neighbor report is enabled.
- **11n Capabilities** - Touch the down arrow to see all the 11n capabilities.

Connection Analysis

Use Connection Analysis to perform a one-time connection analysis on the selected SSID network. Selecting a network layer in the **Module Selections** tab automatically selects all of the dependent layers below it. The order that the connection analysis runs is based on standard WLAN networking dependency, from the bottom (**MAC**) to the top (**Connectivity**). If any of the dependent layers fail, all layers above it also fail.

By default, the analysis is run on the connected WLAN network, unless configured in settings. See [Setting Network Parameters on page 20](#).

Figure 9 Connection Analysis



- **Connectivity** - This test is initiated by the WFW Analyzer app, and analyzes the ICMP (ping) reachability test using the selected SSID network.
To run a full connection analysis on all layers, select the **Connectivity** layer.
- **Address Resolution Protocol (ARP)** - This test is initiated by the WFW Analyzer app, and analyzes the ARP process using resolved parameters from the DHCP layer.
- **Dynamic Host Configuration Protocol (DHCP)** - The DHCP is initiated automatically by Android, and analyzes the native Android DHCP process.
- **Extensible Authentication Protocol over LAN (EAPOL)** - This analyzes the EAPOL process of the WLAN network stack. If the EAPOL is not required, for example, with an open network, the analysis is skipped.
- **Media Access Control (MAC)** - This analyzes the MAC-based communications used for 802.11 authentication and association with an access point.

Module Selections

Use the **Module Selections** tab to choose a network layer to analyze.

1. Touch **≡ > Connection Analysis > Module Selections**.
2. Touch a network layer to select it. The box next to the selected layer is checked and turns blue.
The network layers below it are automatically checked and turn gray. To clear all selections, touch the blue check box.
3. Select **Run Selections**. The **Results** tab displays.

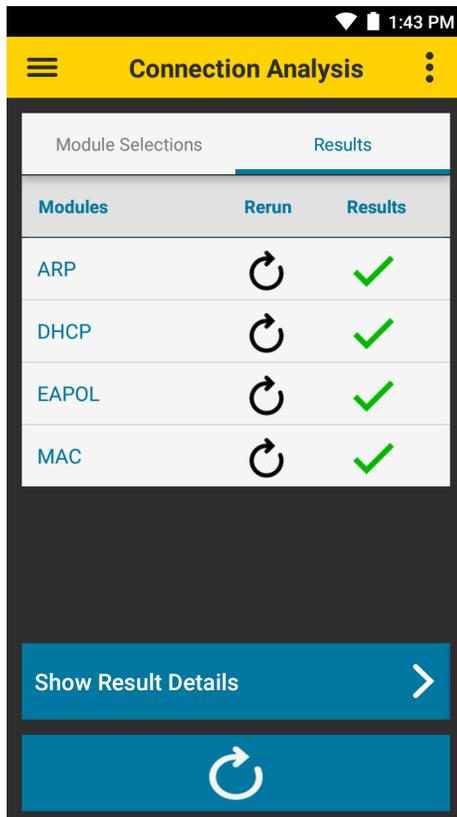
Results

When an analysis is complete, the results display in the **Results** tab.



NOTE: Results only display for the first connection attempt to the SSID. If the first connection attempt fails, subsequent attempts are not analyzed. This may cause the Connection Analysis screen to show a connection failure even if the device is connected.

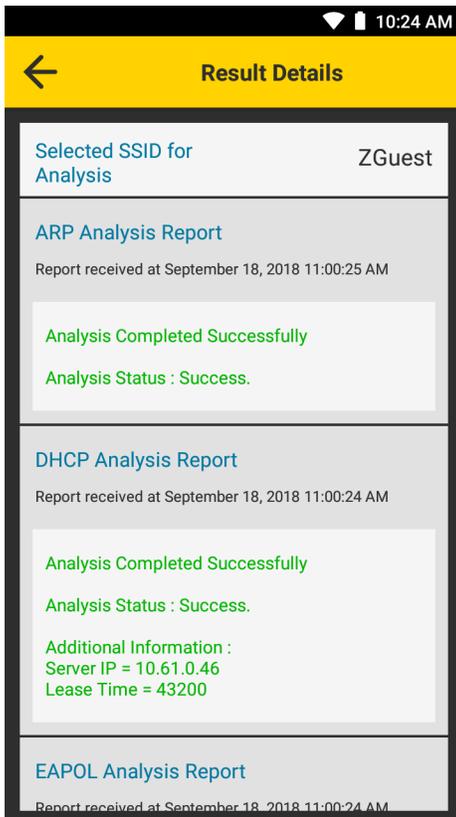
Figure 10 Connection Analysis Results



Select to rerun connection analysis for a selected layer, or all layers.

Touch **Show Result Details** to display detailed analysis reports for each network layer.

Figure 11 Connection Analysis Results

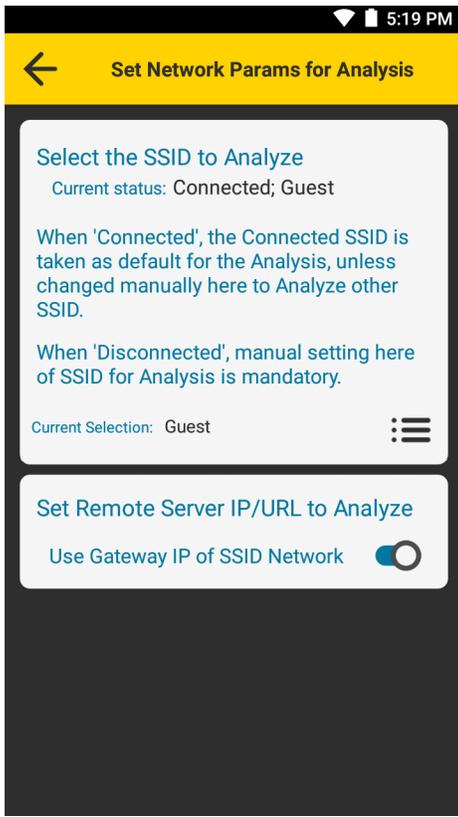


The **Results Details** screen displays the network layers in the same order as they appear on the **Results** tab.

Setting Network Parameters

By default, the analysis is run on the connected WLAN network.

Figure 12 Set Network Parameters



To select a different network:

1. Touch **☰** > **Connection Analysis** > **Module Selections** > **Set Network Params for Analysis**.
2. Touch **☰**. A list of previously saved networks displays.
3. Touch a network to select it.
4. Select **OK**.
5. Select **←**.

To set the server IP, URL, or Fully Qualified Domain Name (FQDN) for the connectivity reachability test:

1. Touch **☰** > **Connection Analysis** > **Module Selections** > **Set Network Params for Analysis** > **☰**.
2. Touch the switch next to **Use Gateway IP of SSID Network**.
3. Enter the server IP, URL, or FQDN.
4. Select **←**.

Networking Tools

To view available networking tools, touch ≡ > **Networking Tools**.

Ping

Ping is a self-contained utility that sends an ICMP ping with configurable input settings. Configure and run up to two separate pings at the same time, each with a different IP, URL, or FQDN address.

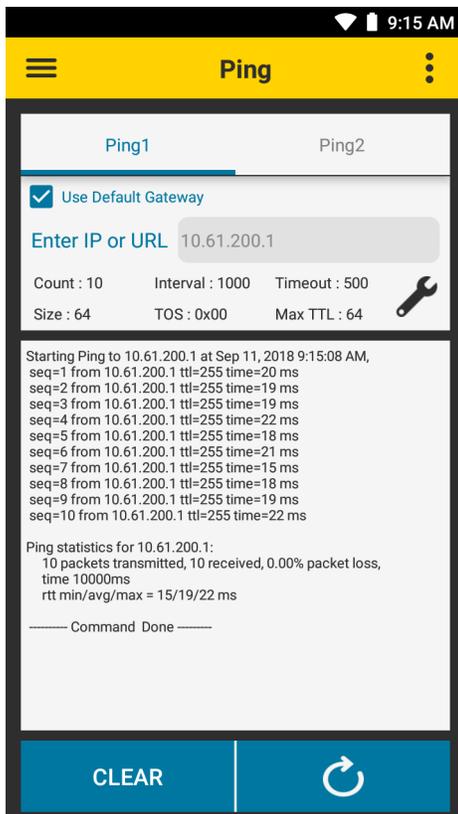
Use Ping to determine reachability and to perform a self-contained test of end to end traffic performance.

To use Ping, touch ≡ > **Networking Tools** > **Ping**.

To start the ping test:

1. Touch ≡ > **Networking Tools** > **Ping**.
2. If connected to a Virtual Private Network (VPN), check the **Use Default Gateway** check box.
3. To use a custom IP, URL, or FQDN, uncheck the **Use Default Gateway** check box and enter the IP, URL, or FQDN.
4. Touch ↻.

Figure 13 Ping Screen



Ping Settings

Ping Settings provides options for configuring ping input settings. To configure ping input settings, touch .

Figure 14 Ping Settings



- **Continuous ping** - Enable or disable continuous ping (default: disabled)
- **Count** - Number of ping requests to send (default: 10). This option is not available when using continuous ping.
- **Interval (ms)** - Amount of time in ms between ping requests (default: 1000)
- **Timeout (ms)** - Amount of time in ms before a ping times out (default: 500)
- **Max TTL** - Maximum time to live for a packet (default: 64)
- **Packet Size** - Size of each ping packet in bytes (default: 64)
- **TOS (Hex Value)** - Type of service as a hexadecimal value from 00 to FF. Recommended values are B8 Voice, A0 Video, 20 Background, and 00 Best Effort (default).

TraceRoute

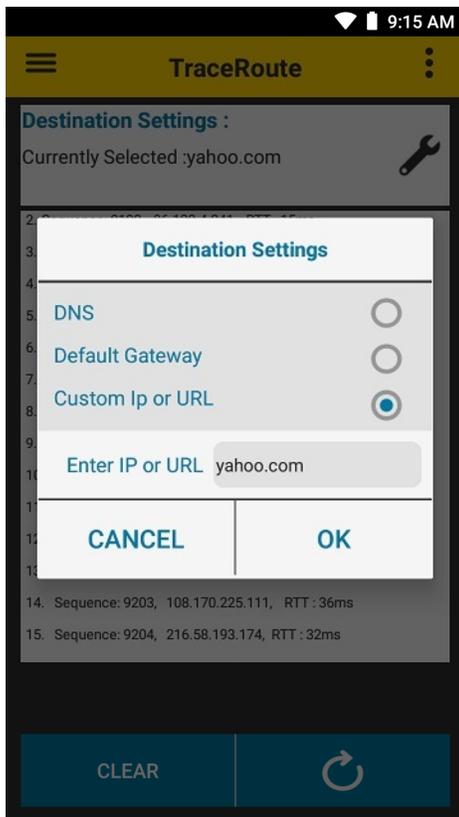
TraceRoute is a self-contained utility that displays the route (path) and round-trip time of packets across segments of the IP network as they travel to a configurable IP destination. Destination options are the current DNS, Default Gateway, or an IP address or URL.

Use TraceRoute to determine the number of network segments required to reach a destination, and the reachability and performance to specific segment.

To use TraceRoute:

1. Touch  > **Networking Tools** > **TraceRoute**.
2. Touch . The **Destination Settings** popup appears.
3. Select a destination type: **DNS**, **Default Gateway**, **Custom IP or URL**.
4. If setting a custom IP or URL, touch the **Enter IP or URL** field and enter the IP or URL.

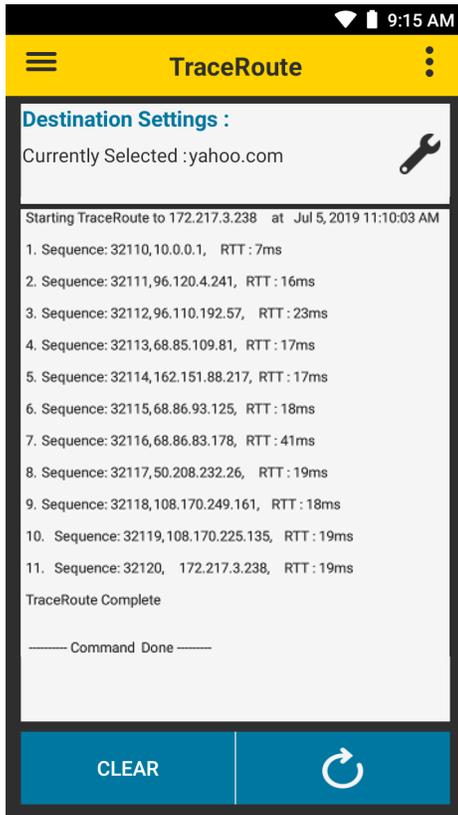
Figure 15 Destination Settings Popup



5. Touch **OK**.

6. Touch . TraceRoute runs using the currently selected destination.

Figure 16 TraceRoute Screen



Device's Coverage View



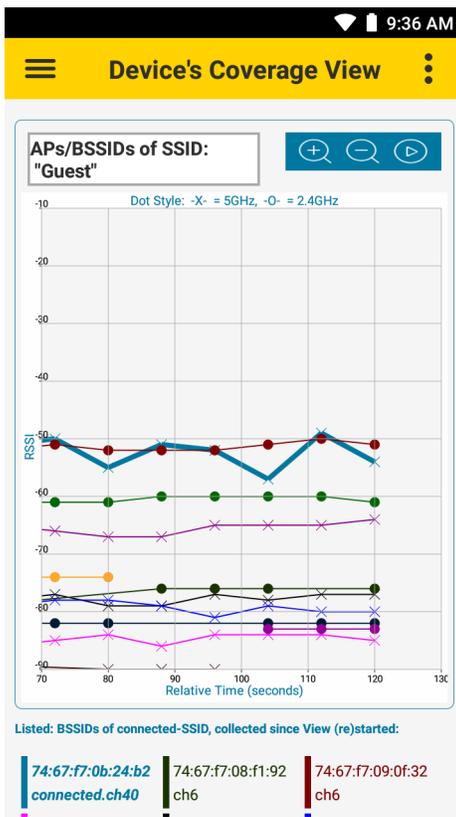
NOTE: Changes to channel (band) preference do not take effect while in Device's Coverage View.

When Android split-screen mode is enabled or disabled, the device automatically exits Device's Coverage View.

Device's Coverage View displays the live RSSI values of BSSIDs of the connected SSID versus relative time (in seconds), with connectivity events. If the device connects to a different SSID, or another WFW Analyzer feature is accessed, **Device's Coverage View** resets.

To display the **Device's Coverage View**, touch **≡ > Device's Coverage View**.

Figure 17 Device's Coverage View



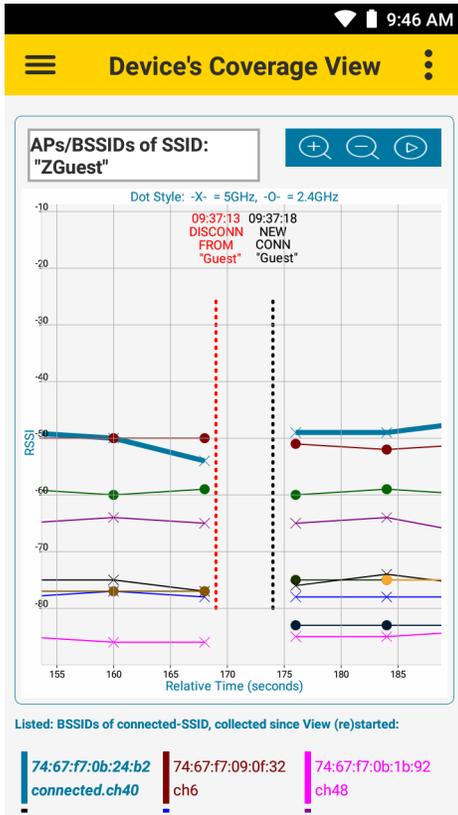
Each line is a connected BSSID with dots marking the RSSI values from scan samples.

The legend at the bottom of the screen matches each BSSID to a color and specifies the currently connected BSSID. The BSSID colors also display as vertical bars on the **Scan List** screen.

Vertical dotted lines designate events which can happen outside of regular scan intervals:

- **VIEW (RE)STARTED** – View started without a Connectivity or Roam event involved
- **ROAMED** – AP hand-off event
- **DISCONN** – Disconnection from SSID
- **NEW CONN** – Connection to SSID.

Figure 18 Device's Coverage View Events



To zoom in and out, place two fingers on the screen and pinch them together (to zoom out) or spread them apart (to zoom in), or touch the and icons. Pan in any direction inside the graph by moving a finger on the screen. Using Zoom or Pan pauses auto-scroll. Touch the icon to enable auto-scroll. Values continue to update even if not in viewing area.

Auto Reachability Test

Use the **Auto Reachability Test** to automatically send a batch of four ICMP packets to the Gateway IP address a couple of seconds after each **CONN** or **ROAMED** event. The result displays on the **Device's Coverage View** screen next to the **CONN** or **ROAMED** event.

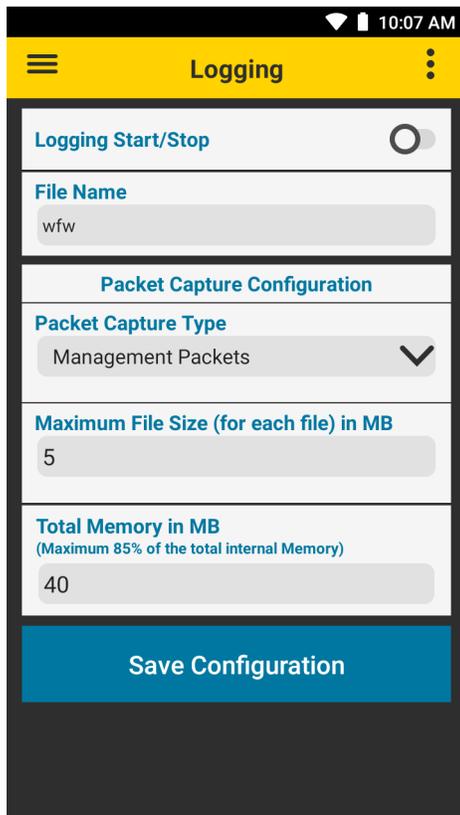
Touch > **Auto Reachability Test** and use the toggle button to enable or disable this test.

Logging

Use **Logging** to store packets in the packet capture (pcap) format. See [Packet Capture on page 37](#).

To display the **Logging** screen, touch **≡ > Logging**.

Figure 19 Logging Screen



- **File Name** - Enter a custom file name. File names contain the user defined name, date, and time. For example, `wfw_2019-2-2_20-59-21.zip`.
- **Packet Capture Type** - Select **Management Packets** or **All Packets**. By default, only management packets can be captured. To capture all packets, including data packets, a password is required. See [Configuration](#).
- **Maximum File Size** - Enter a maximum size in megabytes for each pcap file. When the maximum size is reached, a new file is automatically created.
- **Total Memory** - Enter the total memory, in megabytes, allocated for all pcap files. When the limit is reached, older files are automatically deleted when new logs are saved.
- **Save Configuration** - Save the current configuration.



NOTE: The pcap files are stored in `/sdcard/smu_pcap`.

Logging Management Packets

1. In the **Packet Capture Type** drop-down menu, select **Management Packets**.
2. Touch the toggle switch next to **Logging Start/Stop**.

Logging All Packets

To capture all packets, including data packets, a password is required. For information on how to set a password, see [Configuration](#).

1. In the **Packet Capture Type** drop-down menu, select **All Packets**.
2. Touch the toggle switch next to **Logging Start/Stop**. The **Please enter Password** popup appears.
3. In the password field, enter your WFW Analyzer password.
4. Touch **OK**. Logging is enabled.

Fusion Advanced Configuration

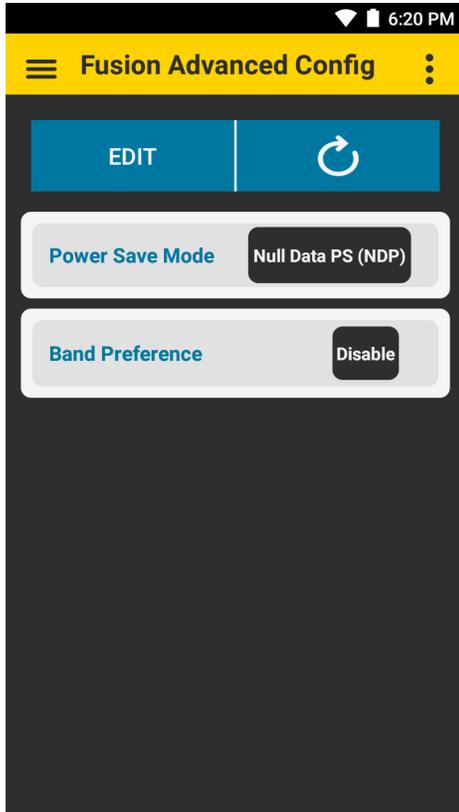


NOTE: This feature requires a password. See [Configuration on page 33](#).

Use the **Fusion Advanced Configuration** screen to view or edit the parameters for power save mode or band preference. A password is required to edit the parameters.

To display the **Fusion Advanced Config** screen, touch **☰ > Fusion Advanced Config**.

Figure 20 Fusion Advanced Config Screen



To enable Fusion advanced configuration:

1. Touch **EDIT**. The **Please enter Password** popup appears.
2. In the password field, enter your WFW Analyzer password.
3. Touch **OK**. Fusion advanced configuration is enabled.

To edit Power Save Mode:

1. Touch the label next to **Power Save Mode**. The Power Save Mode popup appears.
2. Set the power save mode to: **Active (CAM)**, **WMM-PS**, **Null Data PS** (default), **PS Poll**.
3. Touch **OK**.

To edit Band Preference:

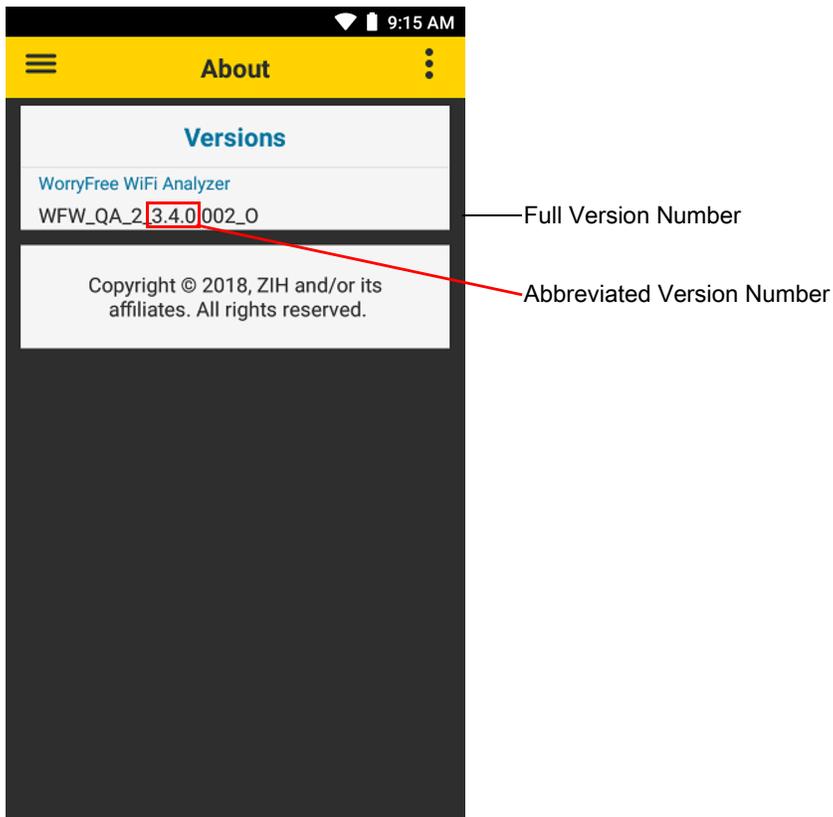
1. Touch the label next to **Band Preference**. The Band Preference popup appears.
2. Set the power save mode to: **Disable** (default), **Prefer 2.4GHz**, **Prefer 5GHz**.
3. Touch **OK**.

About

Use **About** to view the full version number of the WFW Analyzer app.

When contacting Zebra support, please have the full version number available.

Figure 21 About Screen



Camera Preview



NOTE: Not supported on all products.

When Camera Preview is enabled, a live camera view appears on the screen and remains active while WFW Analyzer is open.

Figure 22 Camera Preview



To enable the Camera Preview feature from any screen in WFW Analyzer, touch **☰** > **Camera Preview**. To disable, touch **☰** > **Camera Preview** or touch the X on the top right of the camera view. To move the camera view box, touch and drag anywhere on the screen.

Use Camera Preview to document the location of APs or diagnose issues, such as physical obstructions with low RSSI or poor coverage, by capturing a screenshot. To capture a screenshot, simultaneously press and hold the power key and the volume down key. This saves the entire screen, including the WFW Analyzer app and camera preview to the device storage as a PNG file.

Configuration

Configuration Using Mobility Extensions

Mobility Extensions (MX) allows configuration of WFW Analyzer through staging tools and Mobile Device Management (MDM) solutions with an MX version that supports the **WorryFreeWiFiMgr** Configuration Service Provider (CSP).

For more information on using the **WorryFreeWiFiMgr** CSP, refer to:
techdocs.zebra.com/stagenow/latest/csp/worryfreewifimgr/

Configuration Using StageNow

This section provides instructions on how to use Zebra StageNow to provide an administrator password for WFW Analyzer. For more information on using StageNow, go to techdocs.zebra.com/stagenow/.

The password is required to unlock and use the following protected features in the WFW Analyzer app.

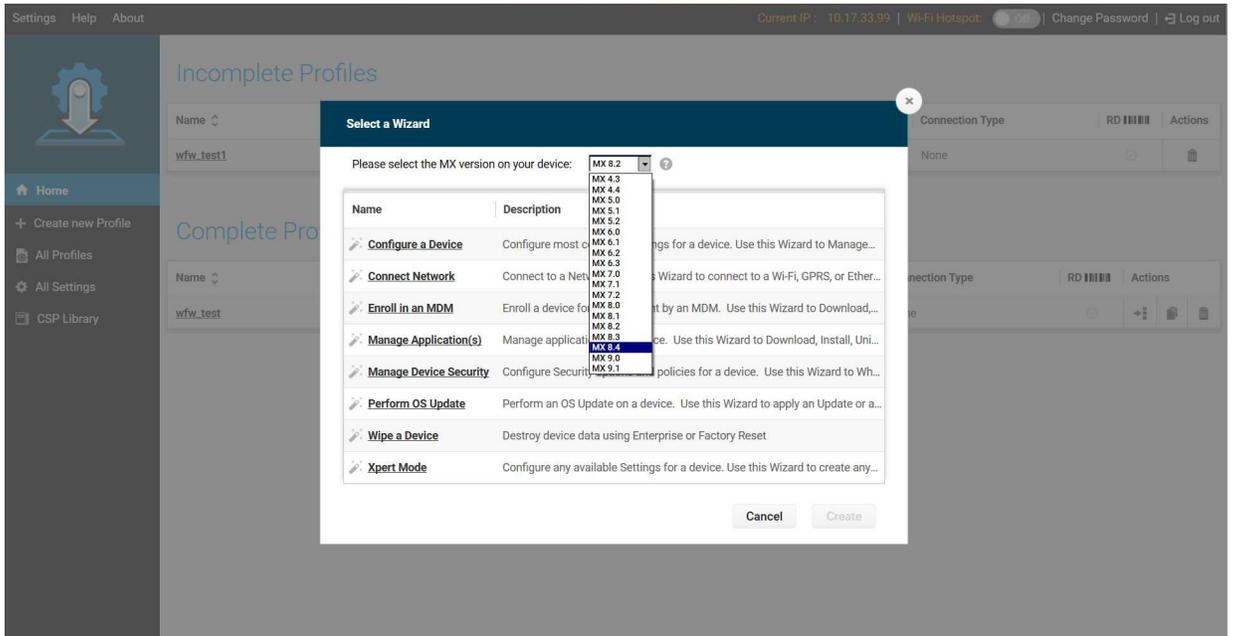
- Fusion Advanced Configuration
- Roaming and Voice Analysis - Enable/Disable pcap capture
- Logging.

Setting the Password

To provide a password for WFW Analyzer using StageNow:

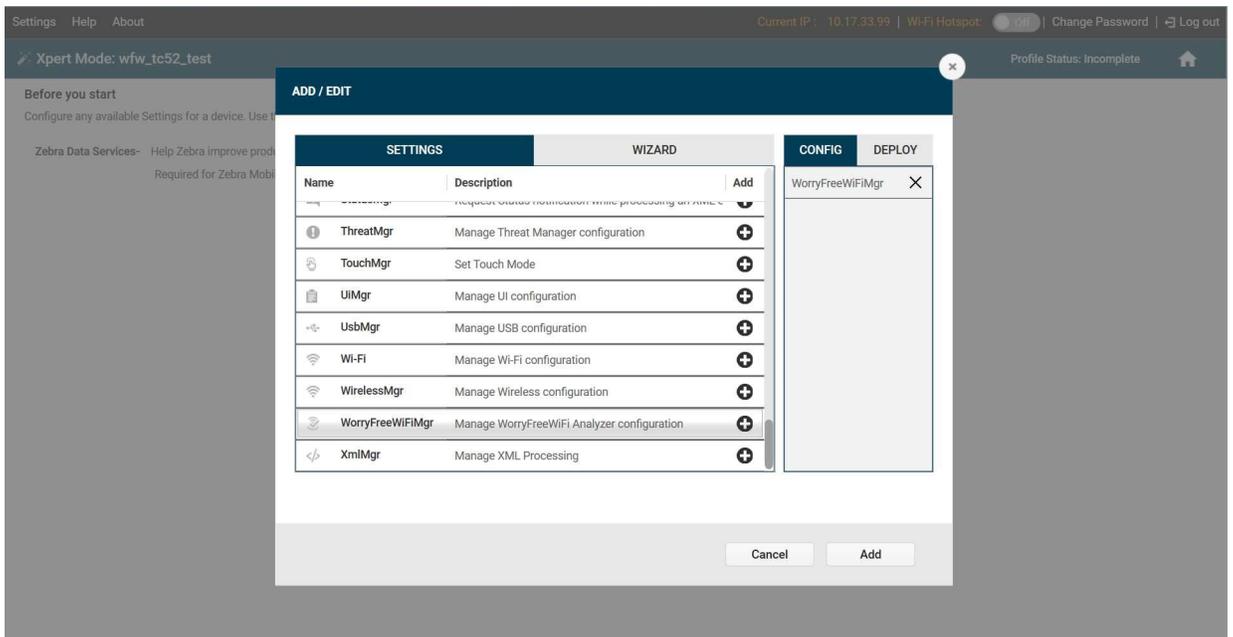
1. On a host computer, open the StageNow application.
2. From the navigation bar on the left side, select **Create new Profile**.
3. In the **Select a Wizard** popup window, select an MX version that is less than or equal to the MX version in the target device.

Figure 23 Select MX Version



4. Select **Xpert Mode**.
5. Select **Create**.
6. In the **Enter Profile** name field, enter a profile name.
7. Select **Start**. The **ADD / EDIT** popup window appears.
8. Scroll down and select **WorryFreeWiFiMgr**.

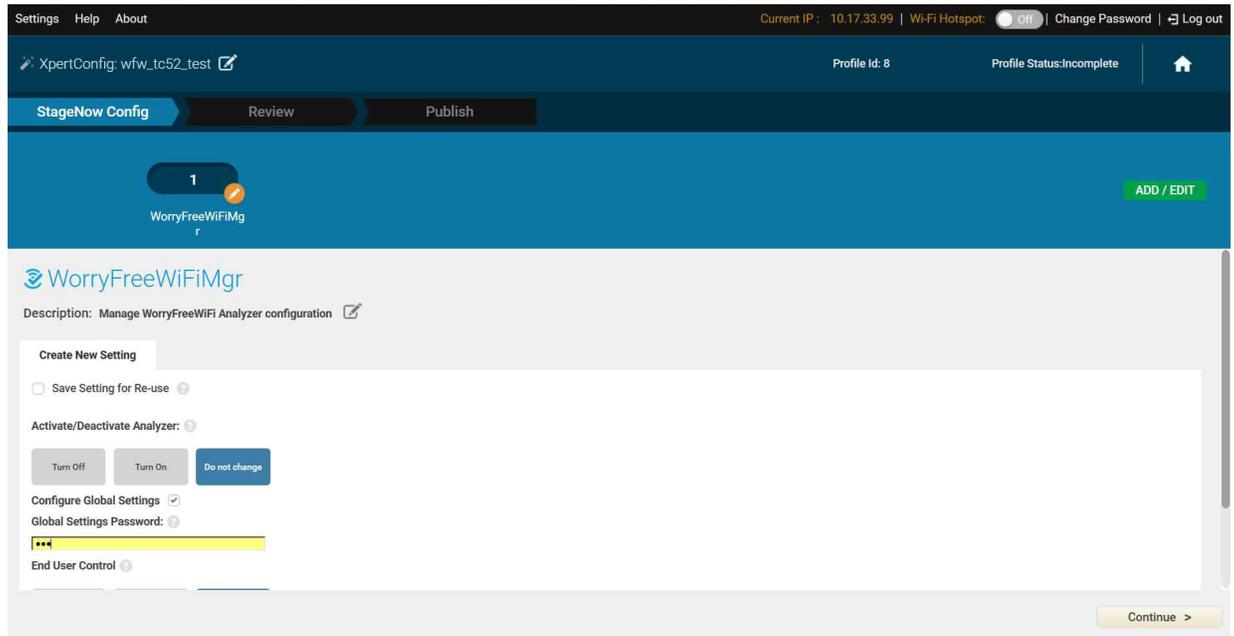
Figure 24 Select WorryFreeWiFiMgr



9. Select the **+** to the left of **WorryFreeWiFiMgr** to add it to the CONFIG list.

10. Select **Add**. The StageNow Config page appears.

Figure 25 StageNow Config



11. Select the **Configure Global Settings** checkbox to enable it.

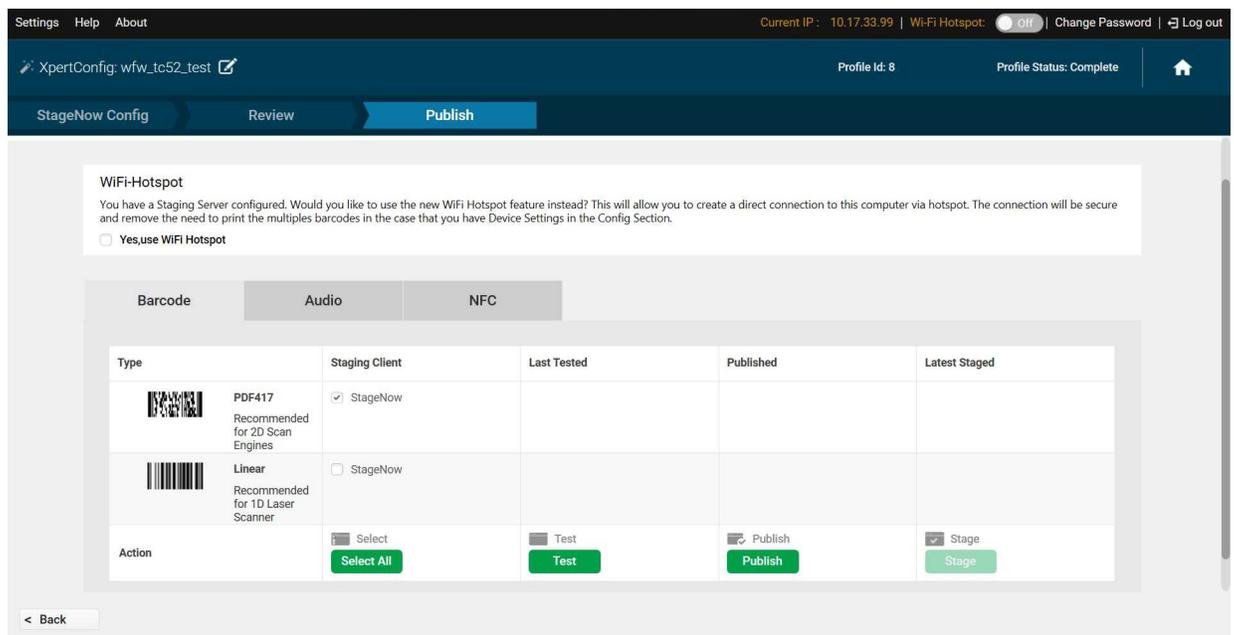
12. In the **Global Settings Password** text field, enter a password.

13. Select **Continue**. The Review tab appears.

14. Select **Complete Profiles**. The Publish tab appears.

15. In the **Barcode** tab, select the **PDF417** option.

Figure 26 StageNow Config - Barcode Tab



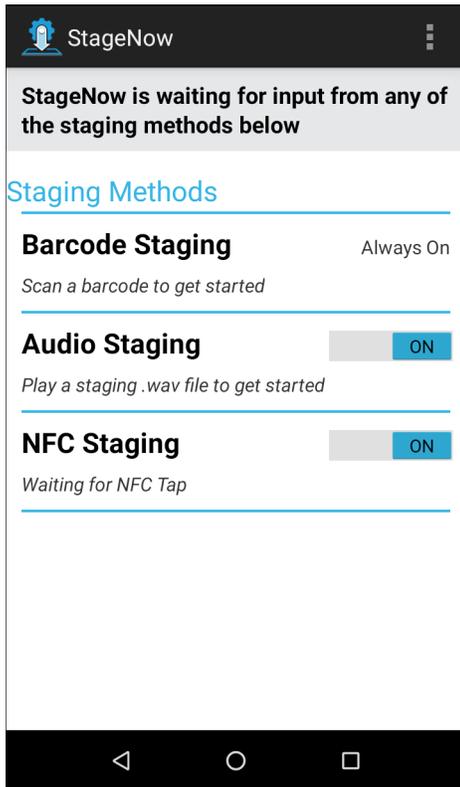
16. Select **Test**. StageNow generates a PDF file.

17. Open the file generated by StageNow. The file contains a StageNow barcode.

To set or reset the password in the WFW Analyzer app:

1. On the target device, open the StageNow app.

Figure 27 StageNow App



2. Use the target device to scan the StageNow barcode from the host computer.

3. After the **Stage Successful** popup screen appears, select **Exit**.

4. Open WFW Analyzer and test the password. For example, touch **≡ > Logging > Logging Start/Stop**.

Packet Capture

Introduction

Packet capture automatically saves pcap files to local storage in the `smu_pcap` folder. To enable and configure packet capture, see [Logging on page 28](#).

To view stored packets:

1. Ensure Logging is stopped
2. Connect the device to the host computer using a USB cable.
3. Transfer the files from the device to the host computer.
4. Unzip the files. If prompted, enter the same WFW Analyzer Security password that was set when the pcap files were created.
5. Use packetizer tools to analyze the pcap files.

Features

The packet capture feature saves incoming and outgoing 802.11 data traffic that is handled by the WiFi stack in its current 802.11-STA role on a device that is connected, or attempting to connect.

- Includes device specific internal outgoing packet attempts and incoming packets.
- Includes broadcast/multicast traffic sent from an access point to connected devices.
- It is not sniffing in receive-only/promiscuous mode like over-the-air sniffers.

WFW Analyzer internal packet captures are:

- Unaffected by the current channel or frequency used by the antenna. Traffic from supported packet types is automatically captured on any channel to which the device connects, roams, or while scanning on off-channels.
- Always in non-fragmented form (802.11 wise). If different forms of MIMO (multiple input multiple output) and MSDU/MPDU Aggregation characteristics are applicable to WLAN over-the-air, it is not reflected in the capture.

Supported Packet Types

WFW Analyzer supports all 802.11-Data / QoS-Data packet types, including:

- All IP packets, including Android stack and apps.
- WLAN-Security: EAP & EAPOL
- Intermediate-protocols. For example: LLC, ARP, DHCP/BOOTP, ICMP
- WLAN-vendor proprietary. For example: WLCPP/IAPP.

Supported Headers and Content

WFW Analyzer supports the following headers and content:

- Radiotap Header
 - Values of the radiotap header are only valid while the device is connected to the network. Values are not accurate when not connected to the network.
 - Timestamp
 - Channel
 - RSSI & Noise
 - Transmit Power of the Device's Transmitted packet.
- 802.11-Headers / sub-headers
 - Type & Sub-Type fields
 - Address Fields: SA, TA, RA, DA, BSSID
- 802.11 Payload (all levels above the MAC level, also know as 802.11-Data type), including LLC header
 - Entire payload in an unencrypted format: w.r.t. WLAN-encryption.

