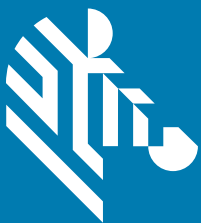


# WorryFree Wi-Fi Analyzer

for Version 3.0.x



**ZEBRA**

**Administrator Guide**  
for Android <sup>TM</sup>

## 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](http://www.zebra.com/copyright).

WARRANTY: For complete warranty information, go to [www.zebra.com/warranty](http://www.zebra.com/warranty).

END USER LICENSE AGREEMENT: For complete EULA information, go to [www.zebra.com/eula](http://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	9/2018	Initial release.
-02 Rev A	7/2019	Add support for logging and password procurement.

# Table of Contents

Terms of Use .....	2
Revision History .....	2
<b>About This Guide .....</b>	<b>6</b>
Introduction .....	6
Product Support .....	6
Best Practices .....	6
Chapter Descriptions .....	7
WFW Analyzer Use Cases .....	7
Notational Conventions .....	9
Provide Documentation Feedback .....	9
<b>Using WFW Analyzer .....</b>	<b>10</b>
Introduction .....	10
Opening WFW Analyzer .....	11
Home Screen .....	12
Status .....	12
Connected IP Network .....	13
Device Information .....	14
Scan List .....	15
Scan Interval .....	16
Filter Options .....	16
Detailed Capabilities for BSSID .....	17
Display Refresh Options .....	18
Connection Analysis .....	19
Module Selections .....	20
Results .....	20
Setting Network Parameters .....	21
Roaming Analysis .....	23
Roaming Analysis Settings .....	24

## Table of Contents

Save Data Options .....	25
Clear Sessions .....	25
Export Saved Data .....	26
Advance Reports .....	26
Monitor and Reports .....	26
Ping Refresh Settings .....	31
Voice Analysis .....	33
Voice Analysis Settings .....	34
Save Data Options .....	35
Clear Sessions .....	35
Export Saved Data .....	36
Advance Reports .....	36
Monitor and Reports .....	36
Networking Tools .....	42
Ping .....	42
Ping Settings .....	43
Device's Coverage View .....	44
Auto Reachability Test .....	45
Logging .....	46
Fusion Advanced Configuration .....	47
About .....	48
Camera Preview .....	49
<b>Configuration .....</b>	<b>50</b>
Configuration Using Mobility Extensions .....	50
Configuration Using StageNow .....	50
Setting the Password .....	50
<b>Report Logger Content .....</b>	<b>54</b>
Introduction .....	54
Content Structure .....	54
Header .....	54
Roaming and Voice Analysis Headers .....	54
INFO Severity Class Headers .....	54
WARNING or ERROR Severity Class Headers .....	55
Voice Analysis Only Headers .....	55
INFO or WARNING Severity Class Headers .....	55
Parameters .....	55
Reasons .....	56
Roaming and Voice Analysis Reasons .....	56
Analyzed Reason Strings .....	56
Standard IEEE Codes for De-Authentication Packets .....	58

## Table of Contents

Voice Analysis Only Reasons .....	58
WARNING Severity Class Headers .....	58
<b>Packet Capture .....</b>	<b>59</b>
Introduction .....	59
Features .....	59
Supported Packet Types .....	60
Supported Headers and Content .....	60

# About This Guide

## Introduction

This guide provides information for the WorryFree Wi-Fi Analyzer (WFW Analyzer) app (formerly SmartMU), which analyses WLAN network connectivity in real-time. View reports of performance and errors in real-time, off-line, or as log files.

## Product Support

WFW Analyzer version 3.0.x is available on the following devices running Android Nougat with LifeGuard update 12 or later.

- MC33
- TC51
- TC51-HC
- TC56
- TC70x
- TC75x

## 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, Roaming, and Voice Analysis features start, the device disconnects and then reconnects to the network. When using these features 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.

## Chapter Descriptions

Topics covered in this guide are:

- [Using WFW Analyzer](#) describes how to use the WFW Analyzer app.
- [Configuration](#) describes how to provide a WFW Analyzer password.
- [Report Logger Content](#) provides a list of report headers and analyzed reasons.
- [Packet Capture](#) provides detailed information about SmartMU 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
Live Wi-Fi Roaming Analysis while using a mobile device in motion	While roaming, view real-time data about the performance and health of the WLAN, AP-handoffs, and network traffic. View real-time detection of issues, causes, and RF environmental parameters.	Roaming Analysis

**Table 1** Use Cases

Summary	Detailed Description	WFW Analyzer Feature
Live voice quality analysis while using a mobile device in motion.	View real-time data about the performance of simulated voice traffic, combined with Roaming Analysis data.  View real-time detection of voice traffic issues, reasons quality measures exceeded thresholds, and RF environmental parameters.	<b>Voice Analysis</b>
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.	<b>Connection Analysis</b>
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.	<b>Logging</b>
Troubleshoot and compare Fusion configuration parameters.	ViewChange 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.	Network Tools > Ping



## 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](mailto:EVM-Techdocs@zebra.com).

# Using WFW Analyzer


## Introduction

This chapter describes the following WFW Analyzer features:

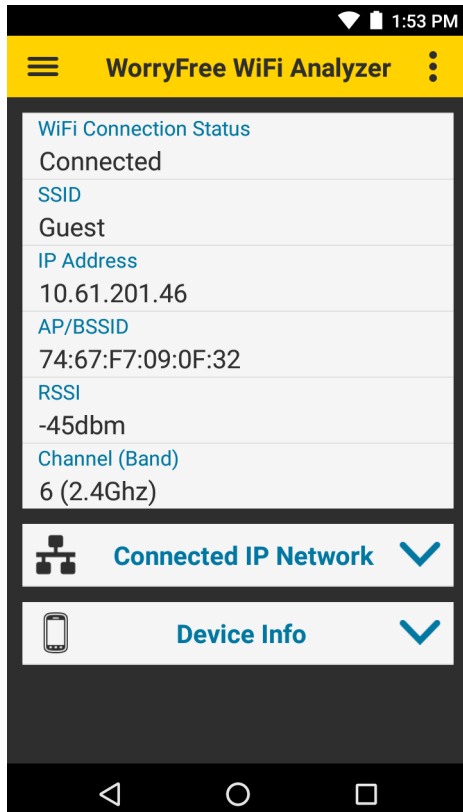
- [Opening WFW Analyzer on page 11](#)
- [Home Screen on page 12](#)
- [Scan List on page 15](#)
- [Connection Analysis on page 19](#)
- [Roaming Analysis on page 23](#)
- [Voice Analysis on page 33](#)
- [Networking Tools on page 42](#)
- [Device's Coverage View on page 44](#)
- [Logging on page 46](#)
- [Fusion Advanced Configuration on page 47](#)
- [About on page 48](#)
- [Camera Preview on page 49.](#)

## 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

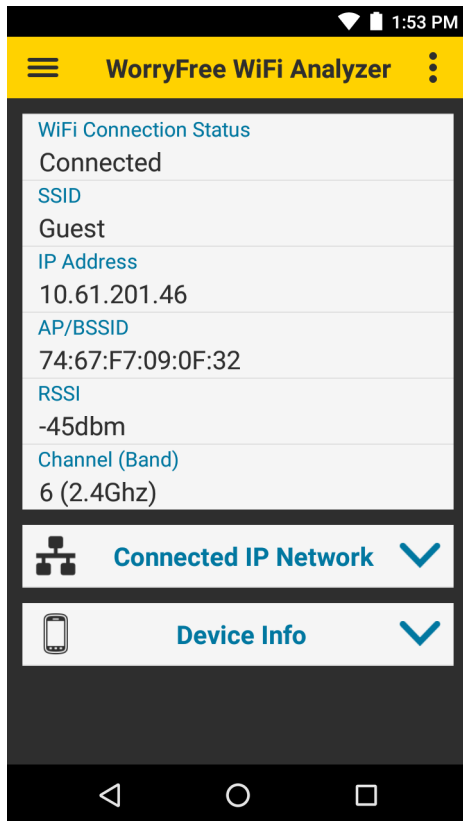


## Home Screen

The **Home** screen displays:

- Status
- Connected IP Network
- Device Information.

**Figure 2** Home Screen



## Status

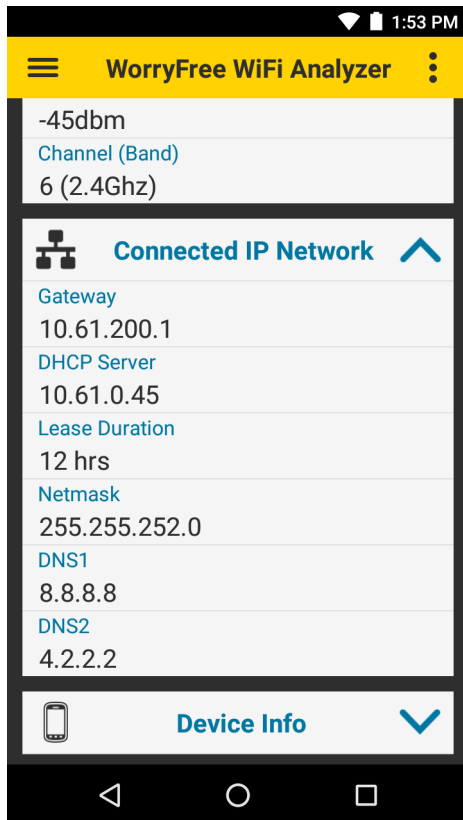
Displays the current device status.

- **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

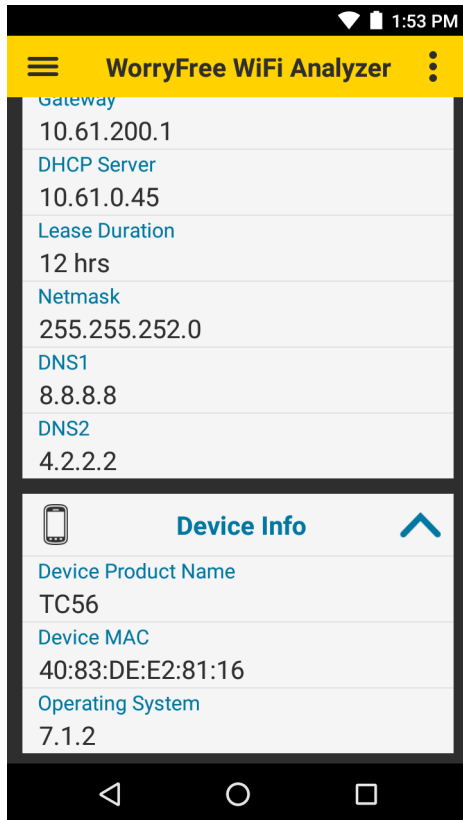


- **Gateway** - IP address of the network gateway
- **DHCP Server** - IP address of the DHCP server
- **Lease Duration** - Amount of time the IP address of the device is leased. The device renews the lease before the lease duration expires.
- **Netmask** - Server subnet mask address
- **DNS1** - Domain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

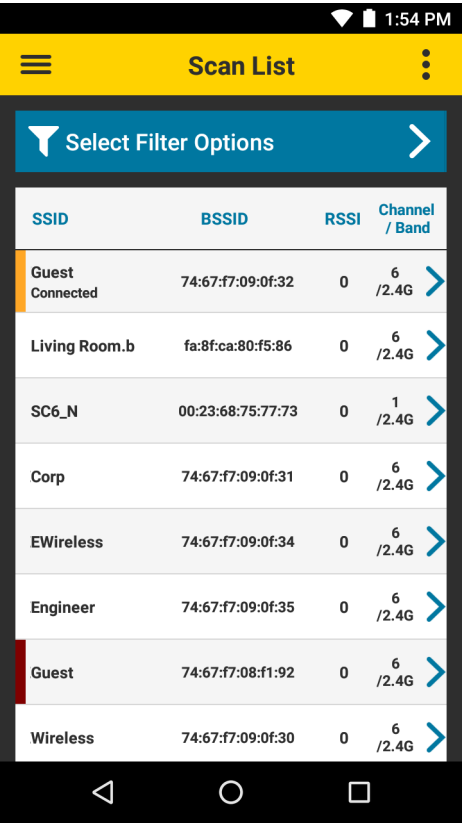
# Scan List

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 16](#).

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



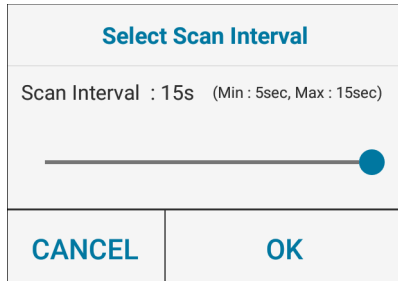
For each BSSID, the following displays:

- **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.

## Scan Interval

Use Scan Interval to change the time interval between scans (range: 5 - 15 seconds, default: 5 seconds).

**Figure 6** Monitor and Reports



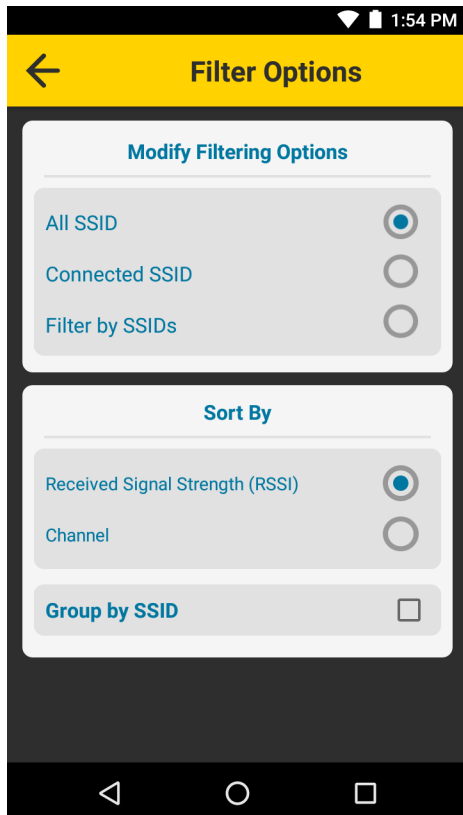
To change the time interval between scans:

1. Touch  $\equiv$  > **Scan List** >  $\vdots$  > **Scan Interval**.
2. Use the slider to set the interval.
3. Touch **OK**.

## Filter Options

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

**Figure 7** 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)

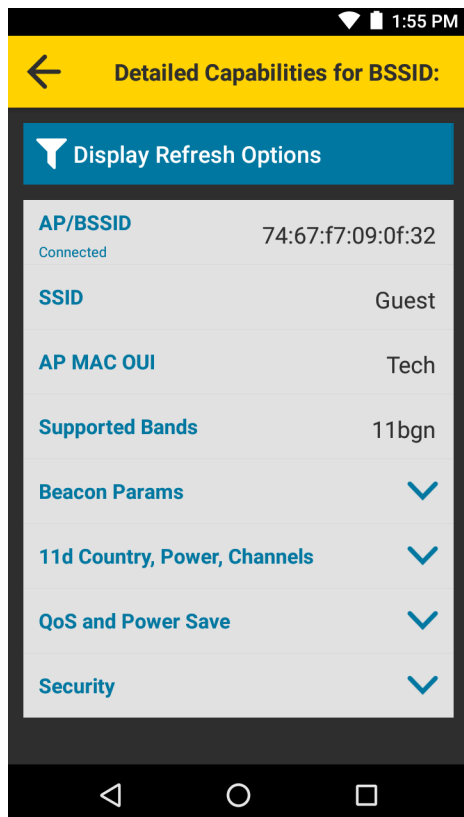


- **Connected SSID - Display BSSIDs of only the connected SSID**
- **Filter by SSIDs** - Touch to display a list of SSIDs. Select an SSID to enable or disable view of its corresponding BSSIDs in the Scan List.
- **Sort By** - Select to sort the Scan List by **Received Signal Strength (RSSI)** (default), 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 8** 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 56.

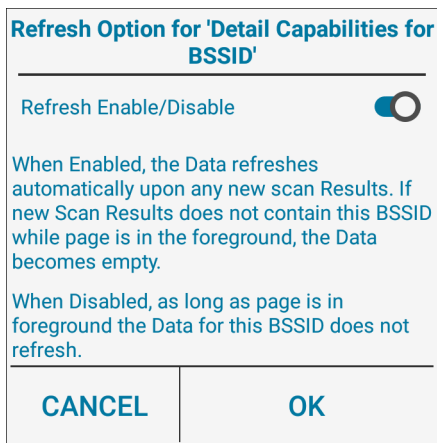
- **Security** - Touch the down arrow next to **Security** to view security WLAN information.

### Display Refresh Options

Use **Display Refresh Options** to enable or disable the automatic refresh of the detailed capabilities information.

Touch **Display Refresh Options** and use the toggle switch, then select **OK**.

**Figure 9** Display Refresh Options



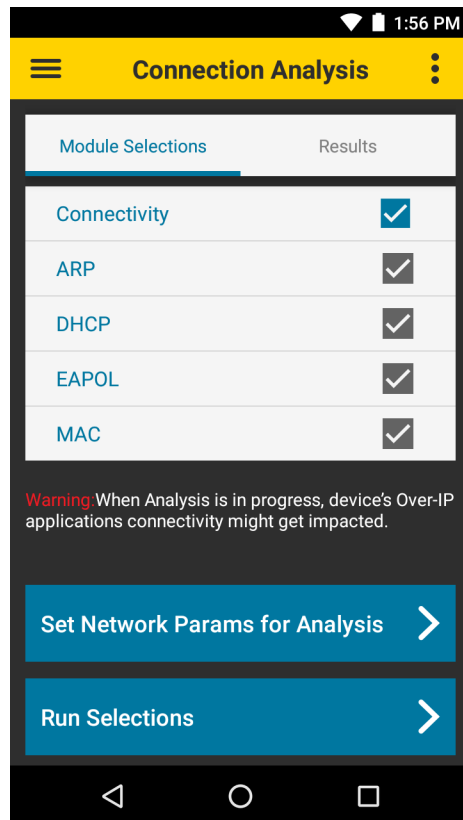
**IMPORTANT:** When **Roaming Analysis** is running with default settings, the **Scan List** displays only **ROAM** events. To change the type of scans displayed, see [Roaming Analysis Settings on page 24](#).

## 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 21](#).

**Figure 10** 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.

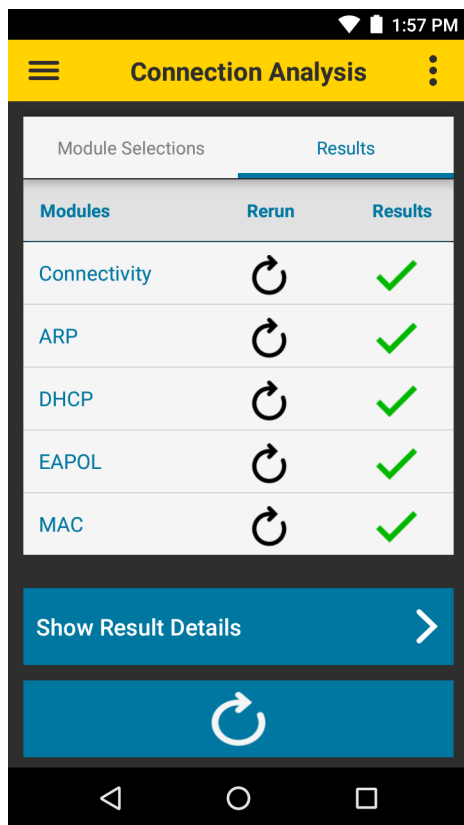
## Results

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.

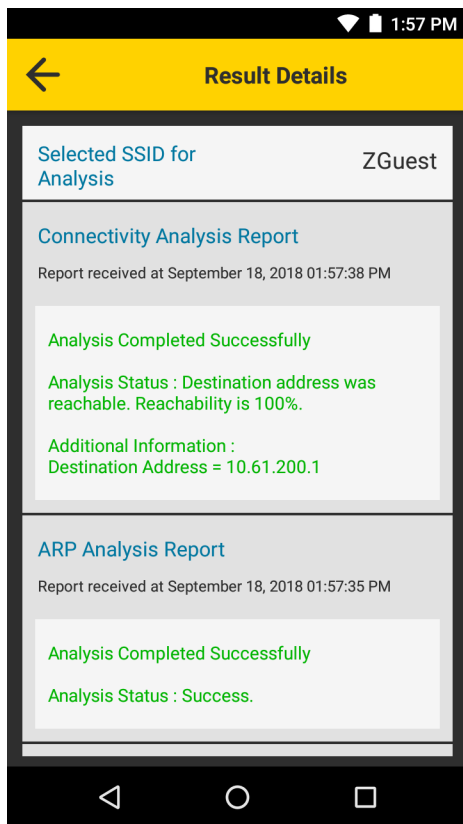
**Figure 11** Connection Analysis Results



Select to rerun the previous connection analysis for a selected layer, or all layers. To select a new network layer to analyze, use the **Module Selections** tab.

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

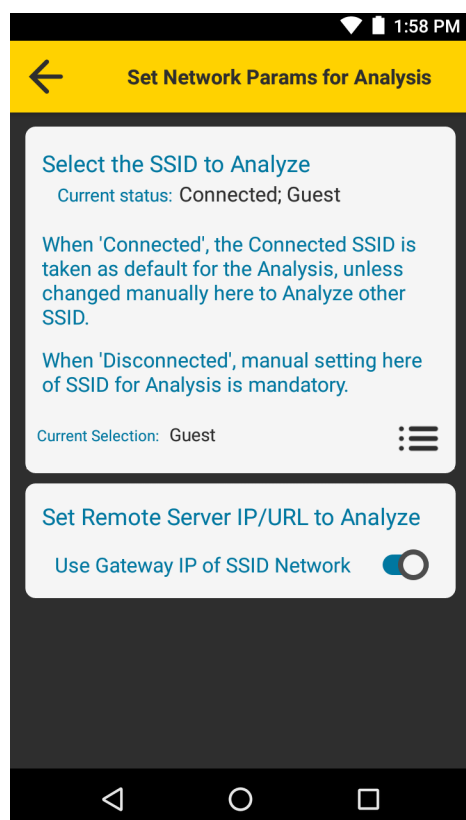
**Figure 12** Connection Analysis Results



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 13** 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 **←**.

## Roaming Analysis

Use **Roaming Analysis** to troubleshoot or monitor real-time WLAN performance, and get analysis reasons in real-time for WLAN connectivity and link quality issues. The analysis data includes reports, packets, traffic statistics, and performance indicators. Analysis is available for open, PSK, and 11r/FT networks.

**Roaming Analysis** runs continuously during a live session and continues to collect data when the WFW Analyzer app is running in the background and when the app is closed. When the device is restarted, the session does not automatically resume.

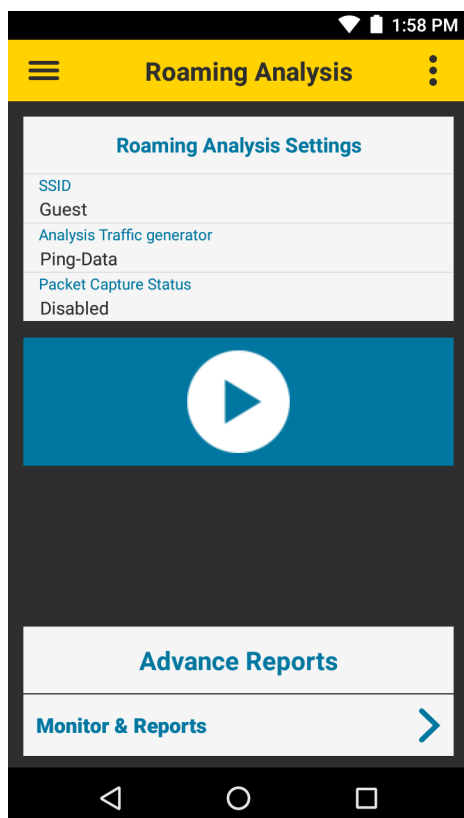
When actively using a voice app while running **Roaming Analysis** with **Settings > Advance Methods > Generate Constant Ping-Data**, all traffic is run in parallel. However, the load of any combined parallel traffic does not impact the device processing itself. In cases where isolating the voice app stream is critical, use **Roaming Analysis** and select **≡ > Roaming Analysis > Settings > Advance Methods > Do not generate ping traffic**.

Use these best practices when running Roaming Analysis:

- It is not recommended to run a live session for more than a several hours. If a session of more than a few hours is required, stop the live session after a few hours, and start a new session.
- It is not recommended to view Scan List or Device's Coverage View, or run Ping, while Roaming Analysis is running.
- It is not recommended to run high throughput traffic or video applications while Roaming Analysis is running.

To start a Roaming Analysis session, touch **≡ > Roaming Analysis > ▶**. To stop a Roaming Analysis session, touch **■**.

**Figure 14** Roaming Analysis



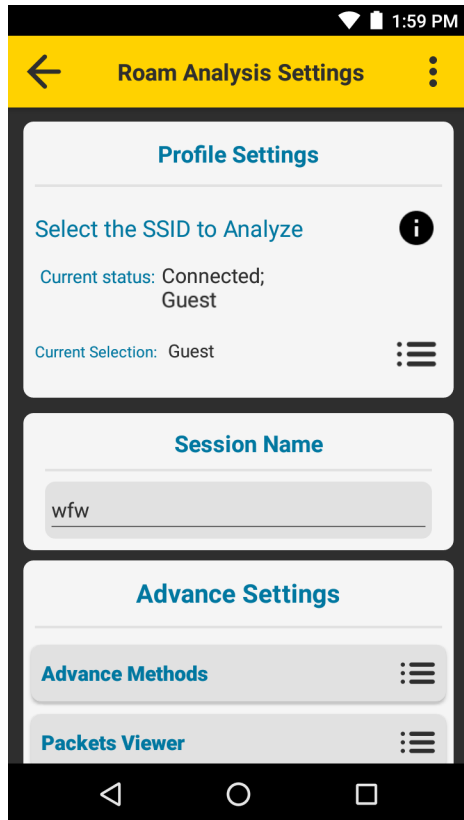
## Roaming Analysis Settings

The main screen displays the current settings:

- **SSID** - Connected WLAN network
- **Analysis Traffic generator** - Method used to generate traffic (default: Ping-Data)
- **Packet Capture Status** - Packet capture status (default: Disabled).

To change the **Roaming Analysis** settings, touch **≡ > Roaming Analysis > ⋮ > Settings**.

Figure 15 Roam Analysis Settings



- **Profile Settings**
  - **Current Status** - Displays the current SSID status.
  - **Current Selection** - Touch **⋮** to select from a list of available SSIDs. When not connected to a WLAN network, this selection is required.
- **Session Name** - Touch to enter a session name. For information on how to clear or save sessions, see [Save Data Options on page 25](#).
- **Advance Settings**
  - **Advance Methods** - Select whether or not to generate traffic (default: Generate Constant Ping-Data traffic). To manually set the IP, URL, or FQDN for the remote server, slide the switch for **Use Gateway IP of SSID Network** to the OFF position.
  - **Packets Viewer** - Select a packet category (default: WLAN Mgmt + Selective Data Packets).
  - **Analysis Report Level** - Select the analysis report level (default: INFO [info | warning | error]).

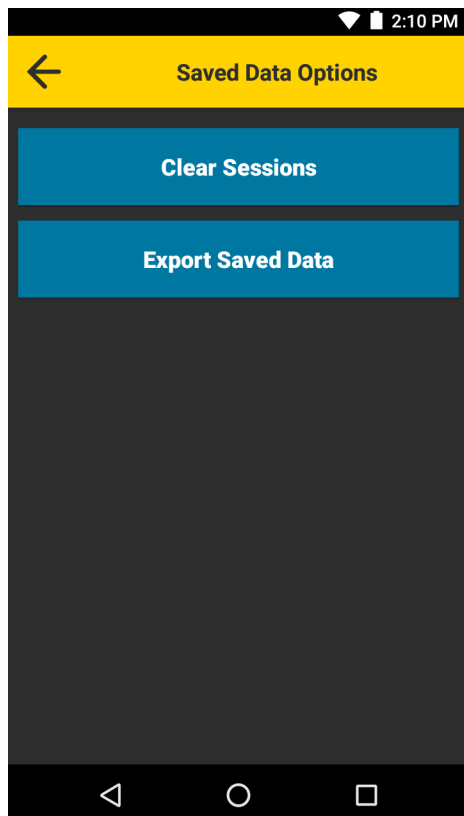


- **Enable/Disable pcap capture** - Enable to store packets in the pcap (packet capture) format. See [Packet Capture on page 59](#).  
A password is required to enable packet capture. See [Configuration on page 50](#).
- **Low Storage Options** - Select an option for managing data when available storage is less than 15%.
- **Scan data for 'Scan List' and 'Coverage View' features, based on** - Select the scan data type to use for Scan List and Device's Coverage View features while **Roaming Analysis** is running (default: Only Roam Scans).
  - **All type scans** - While **Roaming Analysis** is running, **Scan List** and **Device's Coverage View** display data at normal intervals. This setting may cause events from Scan List or Device's Coverage View to affect Roaming Analysis results.
  - **Only Roam Scans** - While **Roaming Analysis** is running, **Scan List** and **Device's Coverage View** only display data collected during roaming events. This setting may cause long delays between events in **Scan List** and **Device's Coverage View**.

## Save Data Options

Use **Save Data Options** to clear or export Roaming Analysis data.

Figure 16 Saved Data Options



### Clear Sessions

Use Clear Sessions to clear all Roaming Analysis session data. Previously collected sessions are removed from the device and become unavailable for off-line viewing. To save session data, see [Export Saved Data on page 26](#).

To clear all Roaming Analysis session data:

1. Touch **≡** > **Roaming Analysis** > **⋮** > **Save Data Options**.
2. Select individual sessions to clear, or touch **Select All** to clear all sessions.
3. Touch **OK**.

### Export Saved Data

Export session data to text files containing JSON objects. The WFW Analyzer app saves the files to the **smu** folder.

To export all saved Roaming Analysis session data:

1. Touch **≡** > **Roaming Analysis** > **⋮** > **Save Data Options**.
2. Select individual sessions to export, or touch **Select All** to export all sessions.
3. Touch **OK**. Text files containing JSON objects are created for each tab in **Roaming Analysis** > **Monitor & Reports**.

To view exported files, ensure Roaming Analysis and logging are not running, connect the device to a host computer using a USB cable, and copy the files from the device to the host computer.

### Advance Reports

While Roaming Analysis is running, session data displays in real-time. When Roaming Analysis is not running, the most recent report displays. To load a previous session while the live session runs in the background or when Roaming Analysis is not running. See [View Options on page 31](#).

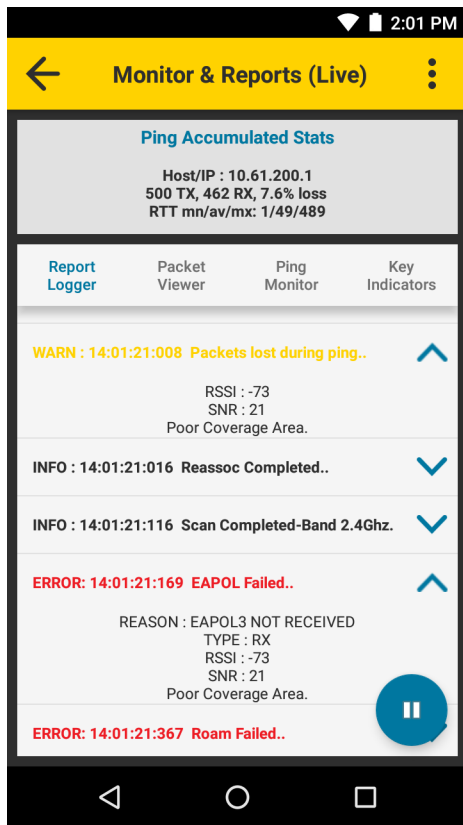
### Monitor and Reports

To view Roaming Analysis reports, touch **≡** > **Roaming Analysis** > **Monitor & Reports**.



**NOTE:** Each time Roaming Analysis starts, WFW Analyzer intentionally causes the device to disconnect and then reconnect to the network. For this reason, the first **Disconnected** error in the Report Logger tab can be ignored.

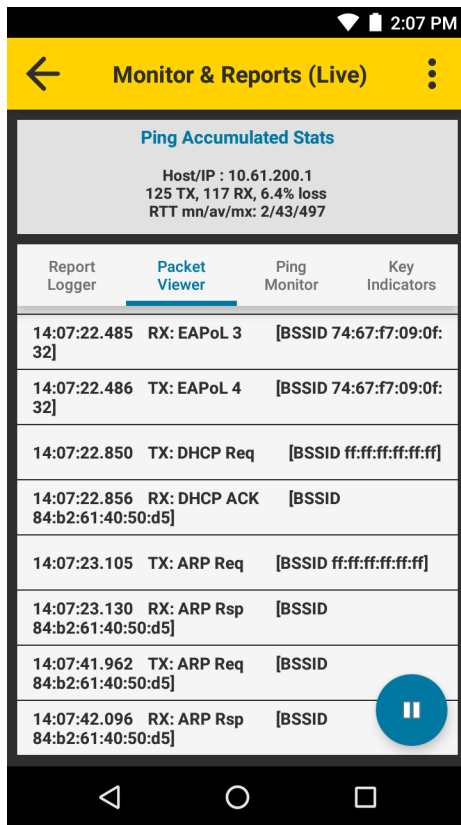
Figure 17 Monitor and Reports



- **Ping Accumulated Stats** - Displays ping data indicators, accumulated in real-time during a live session, or a final summary of a loaded session.
- **Report Logger** - Displays connectivity and Roaming Analysis results. Touch a row to display detailed parameters and reasons of performance thresholds and issues. For more information, see [Report Logger Content on page 54](#).
- **Packet Viewer** - Displays the time, direction, and type of select packets in a session. Touch a packet to view certain fields from its header content. Packet details include 802.11 authentication and association, DHCP, and ARP.

The Packet Viewer does not display all of the packets that are actively analyzed by WFW Analyzer. Analyzed packets are available after an analysis session, with packet capture enabled, ends. See [Roaming Analysis Settings on page 24](#).

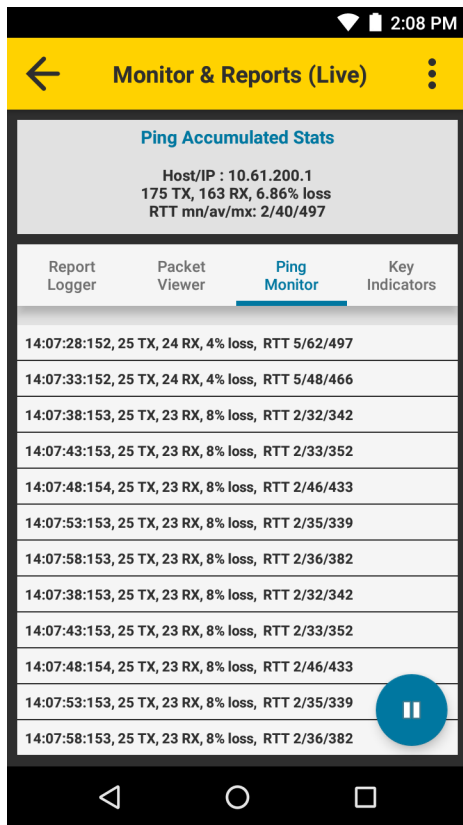
Figure 18 Packet Viewer



- **Ping Monitor** - Displays detailed ping statistics. To change the ping refresh interval, see [Ping Refresh Settings on page 31](#).

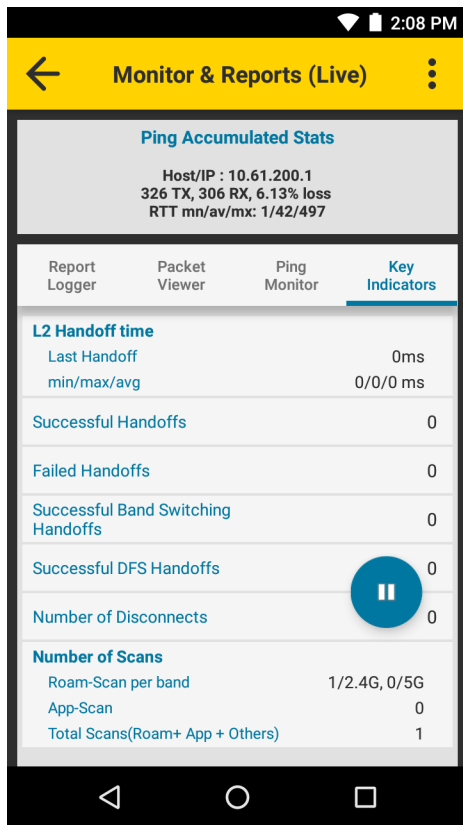
When specific ping errors are detected, such as 100 percent packet loss, or when three or more consecutive packets are lost during ping, touch the information row to view the error report.

Figure 19 Ping Monitor





- **Key Indicators** - Displays a summary of handoffs, disconnects, and the number of scans accumulated during a live session. When a live session is not running, a final summary displays.

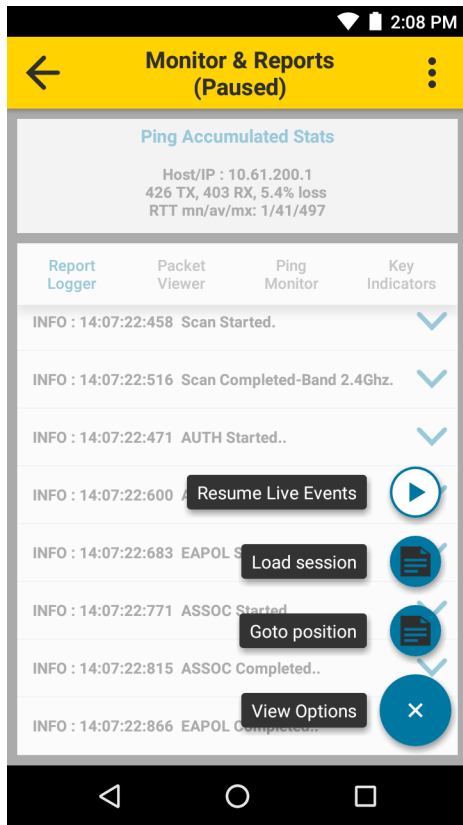
Figure 20 Key Indicators



## View Options

If Roaming Analysis is running, touch  to pause live monitoring. Touch  to display view options.

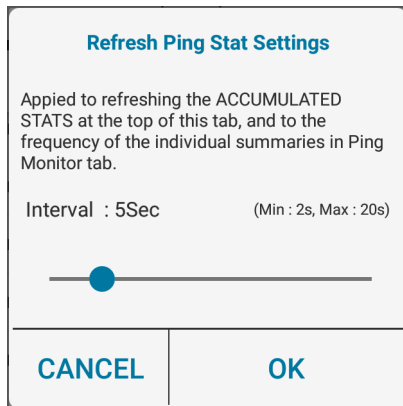
**Figure 21** View Options



- **Resume Live Events** - Touch to resume live monitoring.
- **Load session** - Touch to load a previous session.
- **Goto position** - Use slider and buttons to quickly navigate through long lists of data. Not available in the Key Indicators tab.

## Ping Refresh Settings

Use **Ping Refresh Settings** to change the time interval between pings (range: 2 - 20 seconds, default: 5 seconds).

**Figure 22** Ping Refresh Settings

**Refresh Ping Stat Settings**

Applied to refreshing the ACCUMULATED STATS at the top of this tab, and to the frequency of the individual summaries in Ping Monitor tab.

Interval : 5Sec (Min : 2s, Max : 20s)

**CANCEL** **OK**

To change the time interval between pings:

1. Th ≡ > **Roaming Analysis** > **Monitor & Reports** > ⋮ > **Ping Refresh Settings**.
2. Use the slider to set the interval.
3. Touch **OK**.



## Voice Analysis

Use **Voice Analysis** to troubleshoot or monitor simulated voice traffic performance, and get analysis reasons in real-time for connectivity and link quality issues. The analysis data includes reports, packets, traffic statistics, and performance indicators. Analysis is available for open, PSK, and 11r/FT networks.

**Voice Analysis** runs continuously during a live session and continues to collect data when the WFW Analyzer app is running in the background and when the app is closed. When the device is restarted, the session does not automatically resume.

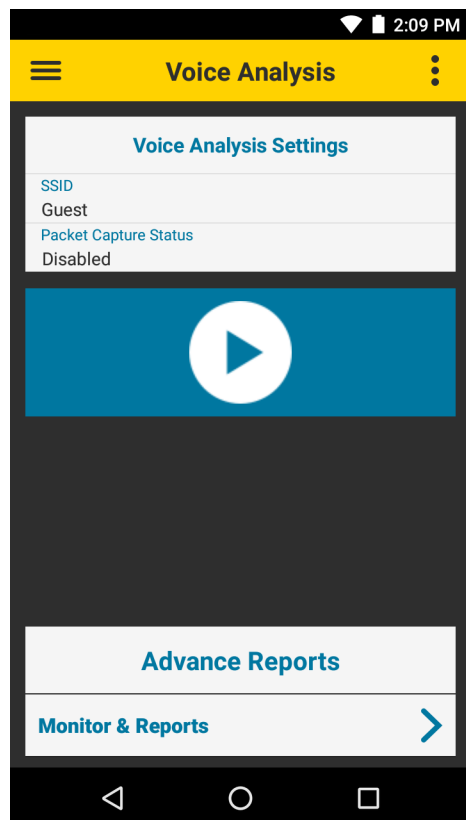
When actively using a voice app while running **Voice Analysis** with **Settings > Advance Methods > Generate Constant Ping-Data**, all traffic is run in parallel. However, the load of any combined parallel traffic does not impact the device processing itself. In cases where isolating the voice app stream is critical, use **Voice Analysis** and select **≡ > Voice Analysis > Settings > Advance Methods > Do not generate ping traffic**.

Use these best practices when running Voice Analysis:

- It is not recommended to run a live session for more than a several hours. If a session of more than a few hours is required, stop the live session after a few hours, and start a new session.
- It is not recommended to view Scan List or Device's Coverage View, or run Ping, while Voice Analysis is running.
- It is not recommended to run high throughput traffic or video applications while Voice Analysis is running.

To start a Voice Analysis session, touch **≡ > Voice Analysis > ▶**. To stop a Voice Analysis sessions, touch **■**.

Figure 23 Voice Analysis




## Voice Analysis Settings

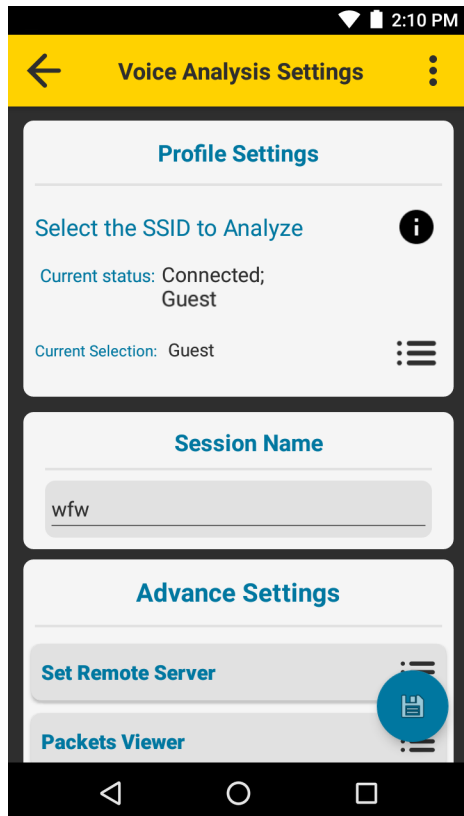
The main screen displays the current settings:

- **SSID** - VoIP network the device is connected to
- **Packet Capture Status** - Packet capture status (default - Disabled).

To change the Voice Analysis settings, touch  $\equiv$  > **Voice Analysis** >  $\vdots$  > **Settings**.

To ensure that the changes to the Voice Analysis settings take effect, touch .

**Figure 24** Voice Analysis Settings



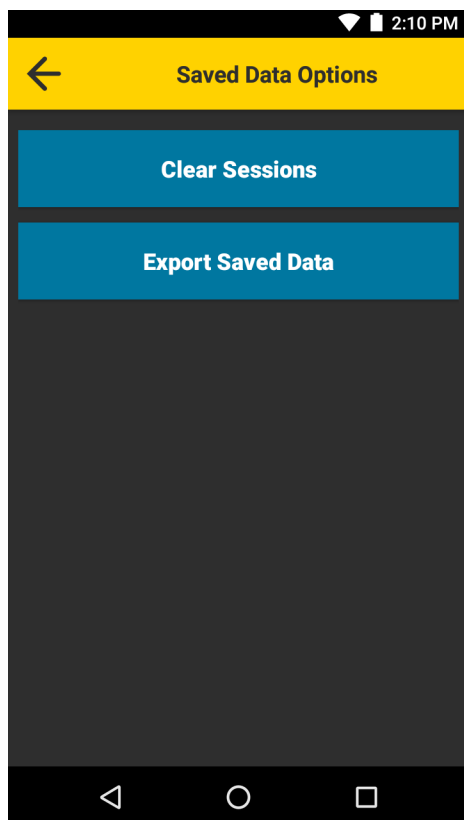
- **Profile Settings**
  - **Current Status** - Displays the current SSID status.
  - **Current Selection** - Touch  $\vdots$  to select from a list of available SSIDs. When not connected to a VoIP network, this selection is required.
- **Session Name** - Touch to enter a session name. For information on how to clear or save sessions, see [Save Data Options on page 35](#).
- **Advance Settings**
  - **Set Remote Server** - To manually set the IP, URL, or FQDN for the remote server, slide the switch for **Use Gateway IP of SSID Network** to the OFF position.
  - **Packets Viewer** - Select a packet category (default: WLAN Mgmt + Selective Data Packets).
  - **Analysis Report Level** - Select the analysis report level (default: INFO [info | warning | error]), and enable or disable some connectivity analysis reporting (default: enabled).

- **Enable/Disable pcap capture** - Enable to store packets in the pcap (packet capture) format. See [Packet Capture on page 59](#).  
A password is required to enable packet capture. See [Configuration on page 50](#).
- **Low Storage Options** - Select an option for managing data when available storage is less than 15%.
- **Scan data for 'Scan List' and 'Coverage View' features, based on** - Select the scan data type to use for Scan List and Coverage View features while Roaming Analysis is running (default: Only Roam Scans).

## Save Data Options

Use **Save Data Options** to clear or export Voice Analysis data.

**Figure 25** Saved Data Options



### Clear Sessions

Use Clear Sessions to clear all Voice Analysis session data. Previously collected sessions are removed from the device and become unavailable for off-line viewing. To save session data, see [Export Saved Data on page 36](#).

To clear all Voice Analysis session data:

1. Touch **≡ > Voice Analysis > ⋮ > Save Data Options**.
2. Select individual sessions to clear, or touch **Select All** to clear all sessions.
3. Touch **OK**.

## Export Saved Data

Export session data to text files containing JSON objects. The WFW Analyzer app saves the files to the **smu** folder.

To export all saved Voice Analysis session data:

1. Touch **≡ > Voice Analysis > ⋮ > Save Data Options**.
2. Select individual sessions to export, or touch **Select All** to export all sessions.
3. Touch **OK**. Text files containing JSON objects are created for each tab in **Voice Analysis > Monitor & Reports**.

To view exported files, ensure Voice Analysis and logging are not running, connect the device to a host computer using a USB cable, and copy the files from the device to the host computer.

## Advance Reports

While Voice Analysis is running, session data displays in real time. When Voice Analysis is not running, the most recent report displays. To load a previous session while the live session runs in the background or when Voice Analysis is not running. See [View Options on page 41](#).

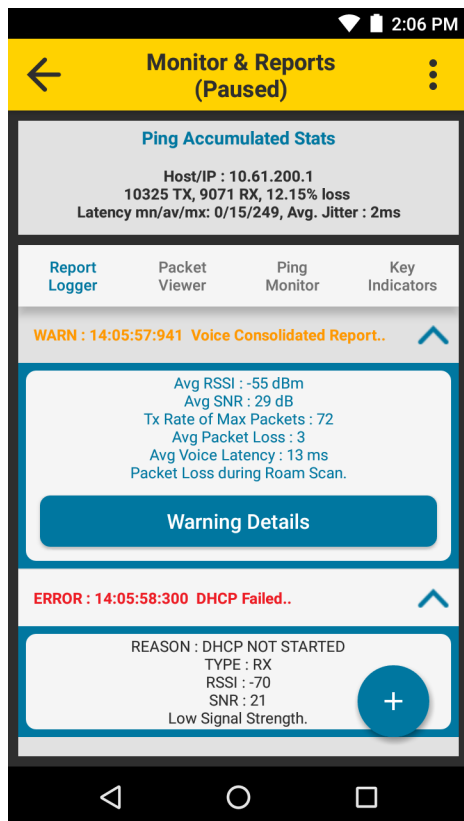
## Monitor and Reports

To view Voice Analysis reports, touch **≡ > Voice Analysis > Monitor & Reports**.



**NOTE:** Each time Voice Analysis starts, WFW Analyzer intentionally causes the device to disconnect and then reconnect to the network. For this reason, the first **Disconnected** error in the Report Logger tab can be ignored.

Figure 26 Monitor and Reports



- **Ping Accumulated Stats** - Displays ping data indicators, accumulated in real-time during a live session, or a final summary of a loaded session.
- **Report Logger** - Displays connectivity and Voice Analysis results. Touch a row to display detailed parameters and reasons of performance thresholds and issues. See [Report Logger Content on page 54](#).

Rows containing a warning message display the **Warning Details** button. Touch **Warning Details** to display one or more sub-reports.

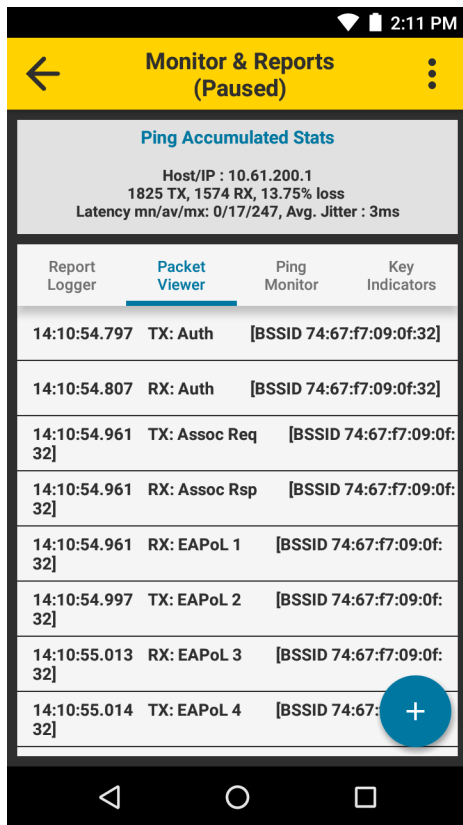
**Figure 27** Sub-Reports

Sub-Reports	
SUB REPORT : PACKET LOSS EXCEEDED	
TimeStamp	14:05:48:904
RSSI	-67 dBm
SNR	24 dB
Tx Rate of Max Packets	19
Packet Loss (%)	46
Voice Latency	5 ms
Reason	Low Signal Strength.
OK	

- **Packet Viewer** - Displays the time, direction, and type of select packets in a session. Touch a packet to view certain fields from its header content. Packet details include 802.11 authentication and association, DHCP, and ARP.

Raw analyzed packets are available after an analysis session, with packet capture enabled, ends. See [Voice Analysis Settings on page 34](#).

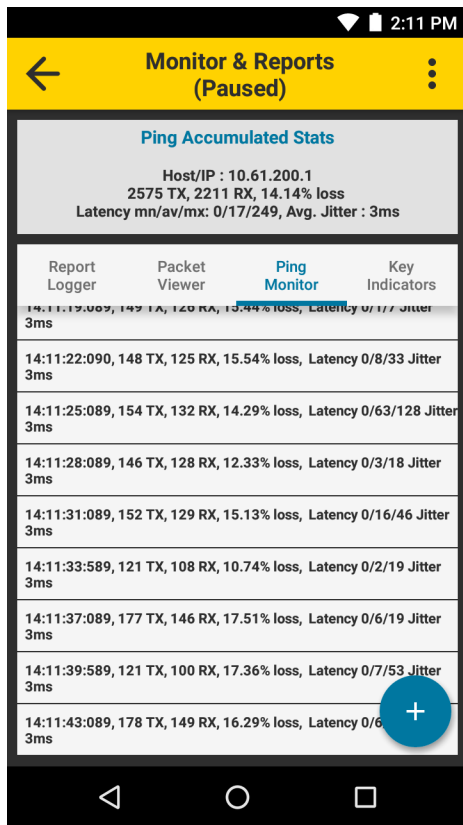
Figure 28 Packet Viewer



- **Ping Monitor** - Displays detailed ping statistics.

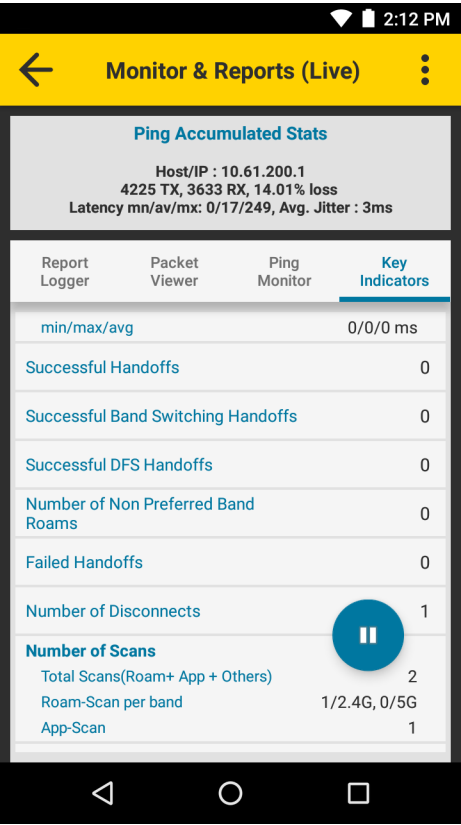
When specific ping errors are detected, such as 100 percent packet loss, or when three or more consecutive packets are lost during ping, touch the information row to view an error report.

Figure 29 Ping Monitor



- **Key Indicators** - Displays a summary of handoffs, disconnects, the number of scans, and additional voice traffic events accumulated during a live session. When a live session is not running, a final summary displays.

Figure 30 Key Indicators

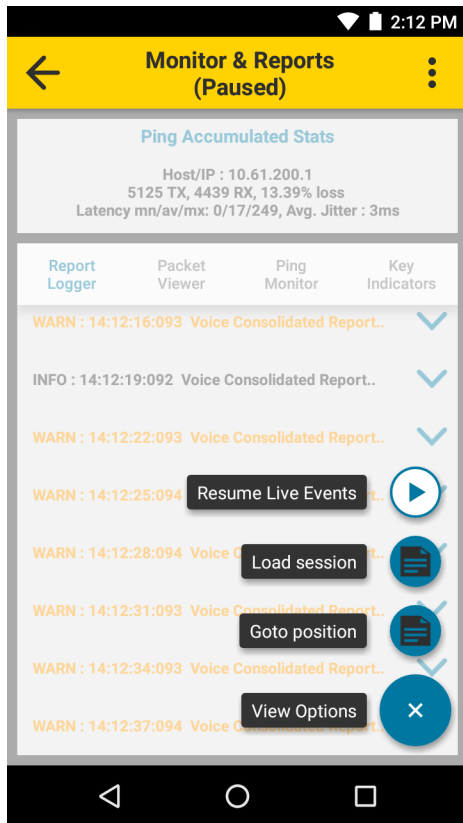




## View Options

If Voice Analysis is running, touch **"** to pause live monitoring. Touch **+** to display view options.

Figure 31 View Options



- **Resume Live Events** - Touch to resume live monitoring.
- **Load session** - Touch to load a previous session.
- **Goto position** - Use slider and buttons to quickly navigate through long lists of data. Not available in the Key Indicators tab.



## 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.

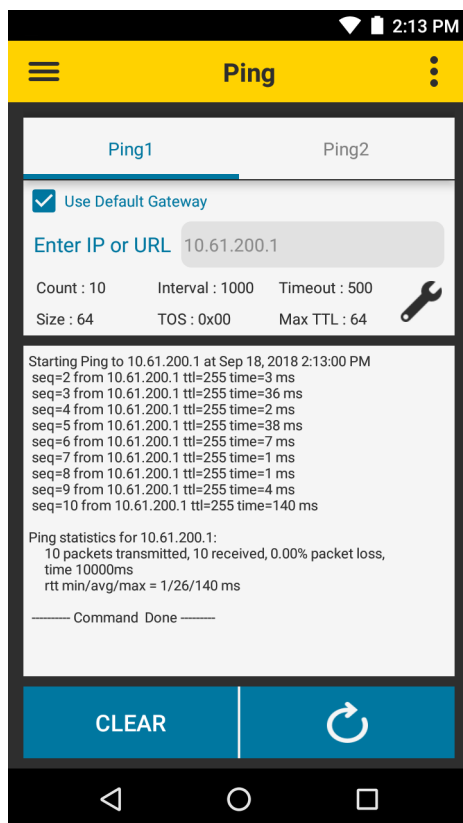
It is not recommended to use Ping while Voice Analysis is running. To use Ping while Roaming Analysis is running, select  > **Roaming Analysis** >  > **Settings** > **Advance Settings** > **Advance Methods** > **Do not generate ping traffic**.

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 32** Ping Screen



## Ping Settings


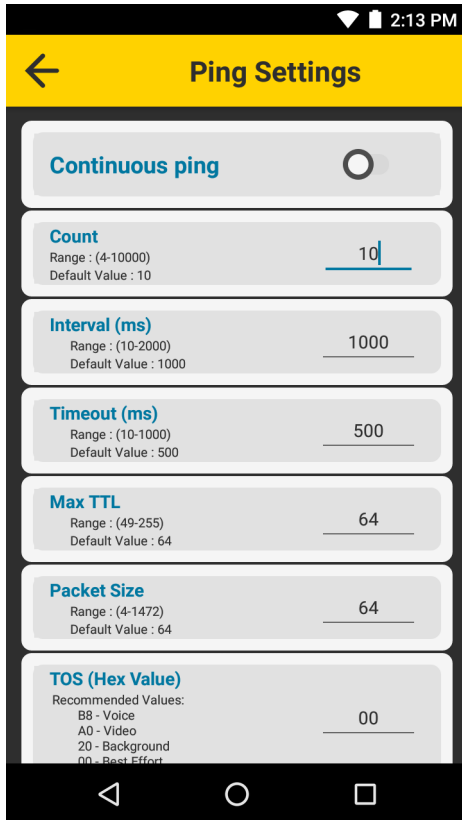
**Ping Settings** provides options for configuring ping input settings. To configure ping input settings, touch .

Figure 33 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).

## Device's Coverage View

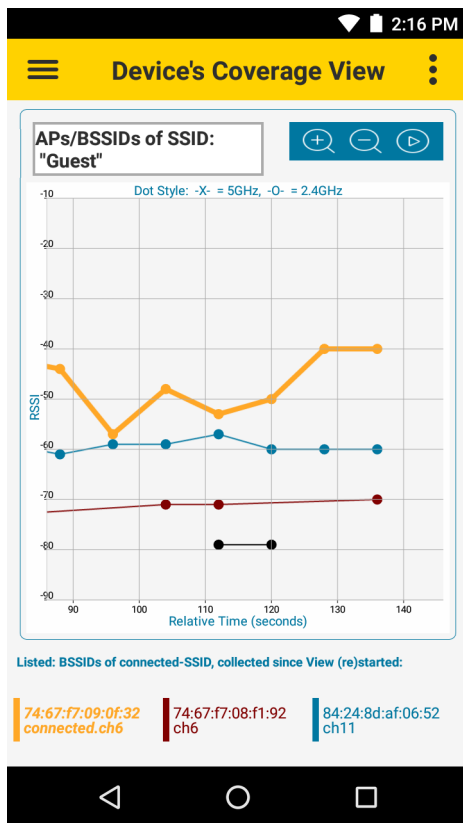


**NOTE:** Changes to channel (band) preference do not take effect while in Device's Coverage View. When Android split-screen mode is enabled or disabled, the device automatically exits Device's Coverage View.

**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 34** 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.

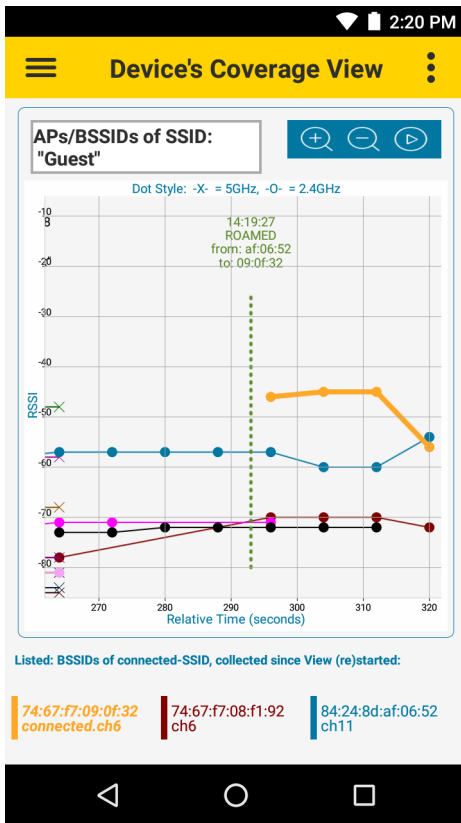
Vertical dotted lines designate events which can happen outside of regular scan intervals:

- **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.



**IMPORTANT:** By default, when the **Roaming Analysis** or **Voice Analysis** feature is running in the background, the **Device's Coverage View** only displays RSSI values when available from the device's internal scanning and roaming logics. RSSI values do not display in fixed scan interval spacing. To change the default setting, see [Roaming Analysis Settings on page 24](#) or [Voice Analysis Settings on page 34](#).

**Figure 35** 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



**NOTE:** This feature requires a password. See [Configuration on page 50](#).

Use **Logging** to store packets in the packet capture (pcap) format. See [Packet Capture on page 59](#).

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

**Figure 36** Logging Screen

- **File Path/Name** - Touch to 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`.
- **Maximum File Size** - Touch to enter a maximum size in megabytes for each pcap file. When the maximum size is reached, a new file is automatically created.
- **Total Memory** - Touch to 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** - Touch to save the current configuration.

To start logging,

1. Touch the toggle switch next to **Logging Start/Stop**. The **Please enter Password** popup appears.
2. In the password field, enter your WFW Analyzer password.
3. Touch **OK**. Logging is enabled.



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

## Fusion Advanced Configuration

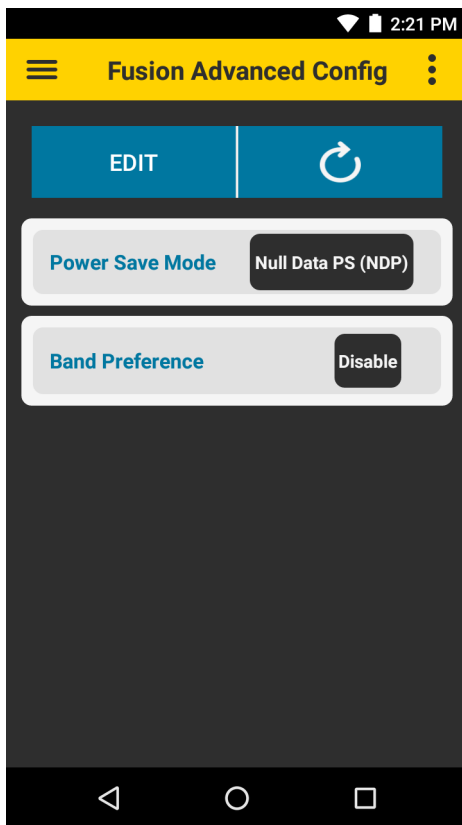


**NOTE:** This feature requires a password. See [Configuration on page 50](#).

Use the **Fusion Advanced Config** screen to set the power save mode or band preference.

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

**Figure 37** 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**.

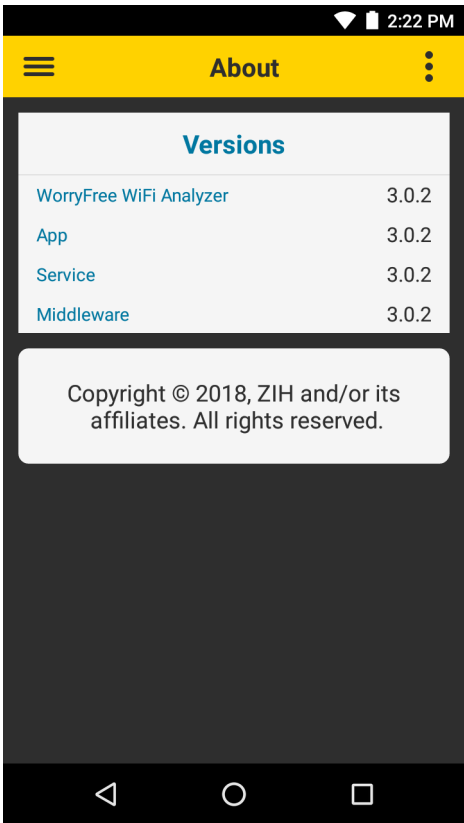
To edit Band Preference:

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 version number for the WFW Analyzer app.  
When contacting Zebra support, please have App, Service, and Middleware version numbers available.

Figure 38 About Screen

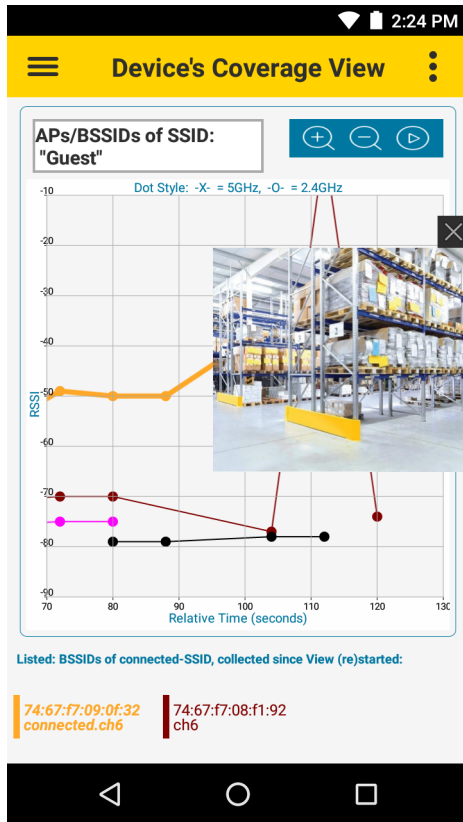




## Camera Preview

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

**Figure 39** 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/](https://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/](https://techdocs.zebra.com/stagenow/).

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

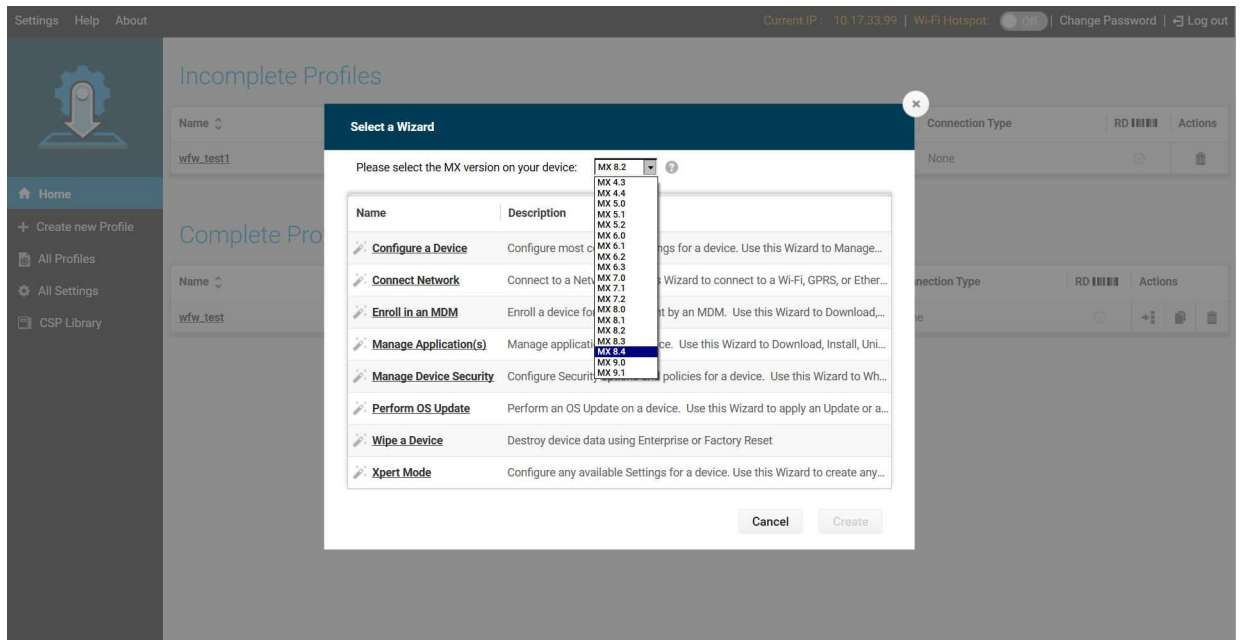
- Fusion Advanced Configuration
- Roaming and Voice Analysis - Enable/Disable pcap capture
- Logging.

## Setting the Password

To provide a password for WFW Analyzer using StageNow:

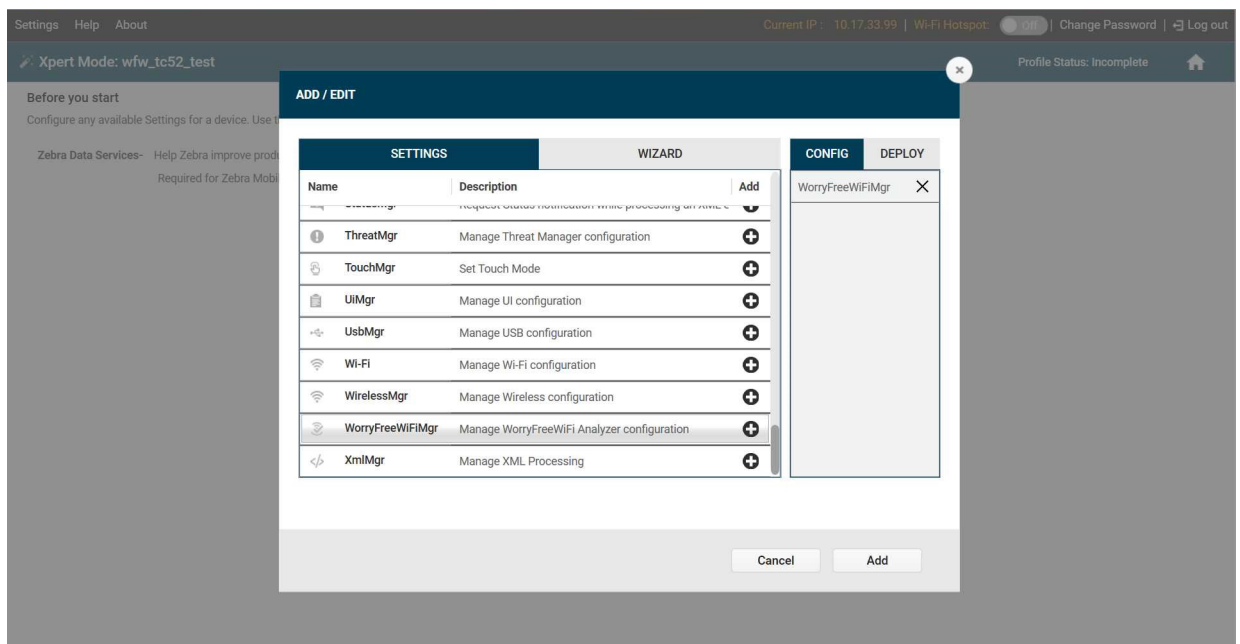
1. On a host computer, open the StageNow application.
2. From the navigation bar on the left side, select **Create new Profile**.
3. In the **Select a Wizard** popup window, select an MX version that is less than or equal to the MX version in the target device.

**Figure 40** 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 41** 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 42** StageNow Config

Settings Help About Current IP: 10.17.33.99 | Wi-Fi Hotspot: ☐ On | Change Password | Log out

XpertConfig: wfw\_tc52\_test Profile Id: 8 Profile Status: Incomplete

**StageNow Config** Review Publish

1 WorryFreeWiFiMgr ADD / EDIT

WorryFreeWiFiMgr

Description: Manage WorryFreeWiFi Analyzer configuration

Create New Setting

☐ Save Setting for Re-use

Activate/Deactivate Analyzer:

Turn Off Turn On Do not change

Configure Global Settings ☒

Global Settings Password:

End User Control

Continue >

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 43** StageNow Config - Barcode Tab

Settings Help About Current IP: 10.17.33.99 | Wi-Fi Hotspot: ☐ Off | Change Password | Log out

XpertConfig: wfw\_tc52\_test Profile Id: 8 Profile Status: Complete

StageNow Config Review **Publish**

WiFi-Hotspot

You have a Staging Server configured. Would you like to use the new WiFi Hotspot feature instead? This will allow you to create a direct connection to this computer via hotspot. The connection will be secure and remove the need to print the multiples barcodes in the case that you have Device Settings in the Config Section.

☐ Yes, use WiFi Hotspot

Barcode Audio NFC

Type	Staging Client	Last Tested	Published	Latest Staged
PDF417 Recommended for 2D Scan Engines	<input checked="" type="checkbox"/> StageNow			
Linear Recommended for 1D Laser Scanner	<input type="checkbox"/> StageNow			
Action	Select <b>Select All</b>	Test <b>Test</b>	Publish <b>Publish</b>	Stage <b>Stage</b>

< Back

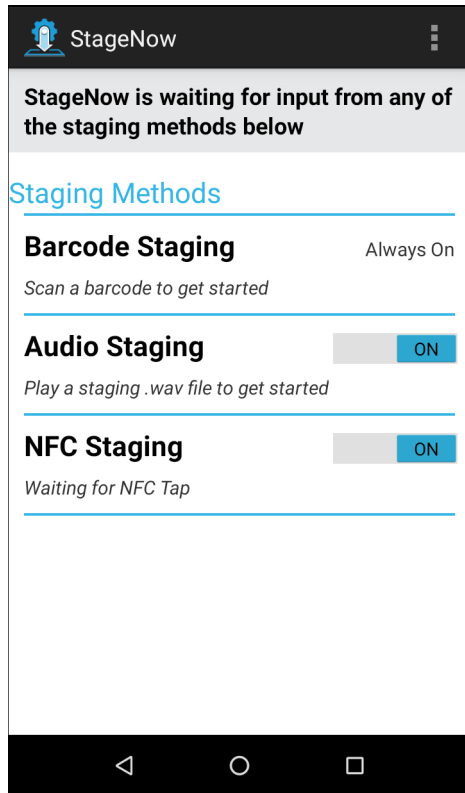
16. Select **Test**. StageNow generates a PDF file.

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 44** 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**.

# Report Logger Content

## Introduction

This chapter provides detailed information about the **Report Logger** tab of the **Roaming Analysis** and **Voice Analysis** features.

To view Roaming Analysis reports, touch ≡ > **Roaming Analysis** > **Monitor & Reports** > **Report Logger**.

To view Voice Analysis reports, touch ≡ > **Voice Analysis** > **Monitor & Reports** > **Report Logger**.

## Content Structure

Events found in the Report Logger tab are structured in the following order:

- Header
- Parameters
- Reasons

## Header

The header contains the severity class (INFO, WARNING, ERROR), the time the event occurred, and a short description. In the default view, only the header is visible. Touch a header for an expanded view that lists parameters and reasons, when applicable.

## Roaming and Voice Analysis Headers

### INFO Severity Class Headers

- Roam Analysis Started
- Roam Analysis Stopped
- AUTH Started (802.11 Auth)
- AUTH Completed (802.11 Auth)
- ASSOC Started (802.11 Assoc)
- ASSOC Completed (802.11 Assoc)
- EAPOL STARTED
- EAPOL Completed

- DHCP Started
- DHCP Completed
- ARP Started
- ARP Completed
- Connection Completed (Full connection attempt completed)
- Roam Started
- Reassoc Completed (802.11 Reassoc)
- Roam Completed
- Scan Started
- Scan Completed
- Device storage space reached 60%
- Disconnect Suppression Triggered
- Disconnect Suppression Completed.

### **WARNING or ERROR Severity Class Headers**

- Connection Failed (Full connection attempt failed)
- Roam Failed (Roam attempt failed)
- Authentication Failed (802.11 Auth attempt failed)
- Association Failed (802.11 Assoc attempt failed)
- EAPOL Failed (EAPOL handshake attempt failed)
- DHCP Failed (DHCP attempt failed)
- ARP Failed (ARP attempt failed)
- Disconnected (Fully Disconnected from Wifi)
- Device storage space reached 70%
- Device storage space reached 80%
- Device storage space reached 90%
- Roam Retry
- Frequent Roams Seen.

### **Voice Analysis Only Headers**

#### **INFO or WARNING Severity Class Headers**

- Voice Analysis Started
- Voice Analysis Stopped
- Voice Consolidated Report.

## **Parameters**

Standard Wi-Fi parameters are located directly under the header when applicable.

## Reasons

Analyzed reasons are provided for the WARNING and ERROR severity classes when applicable.

### Roaming and Voice Analysis Reasons

#### Analyzed Reason Strings

- Timeout happened between substate machines  
For example: Auth response came, but Assoc request was not sent
- Packet State machine Succeeded but Framework did not notify the state change
- Packet State machine Success but Framework notified wrong state change
- Analysis could not start due to MAC Analysis Failed
- Analysis could not start due to EAPOL Analysis Failed
- Analysis could not start due to DHCP Analysis Failed
- Analysis could not start due to ARP Analysis Failed
- Keynonce of eapol1 and eapol3 not equal
- ReplayCounter of eapol1 not equal to eapol2 or eapol3 is not equal to (eapol1 + 1)
- DHCP\_INVALID
- DHCP\_DECLINE
- DHCP\_NAK
- DHCP\_RELEASE
- NO DHCP server(s) found
- DHCP server didn't respond to the request
- Device failed to start discover after NAK
- AP of selected SSID to analyse is not in vicinity
- EAPOL four way handshake timeout
- Analysis is been done on an Open/WEP Profile Hence EAPOL is not applicable
- Authentication has Timedout
- Association has Timedout
- WiFi is turn off
- Unable to reach the destination address
- Destination address was reachable But Reachability is poor
- Destination address was reachable But Reachability is only 50%
- Destination address was reachable But Reachability is 75%
- Destination address was reachable Reachability is 100%
- Success
- Unable to reach gateway through arp
- Gateway IP is not available to test arp reachability



- Association not started
- EAPOL Key 1 not started
- DHCP not started
- ARP not started
- EAPOL Key 2 not sent
- EAPOL Key 3 not received
- EAPOL Key 4 not sent
- DHCP Request not started
- Ping test not started
- Undefined Error
- Device Roamed from Non Preferred Band to Preferred Band AP
- Device Roamed to Non Preferred Band
- Device failed to Roam to Good Signal Strength Access Points are seen in Preferred Band
- Device failed to Roam to Preferred Band after Roam Scan
- Roam Candidate AP's RSSI is greater than Previous AP's RSSI
- Delta RSSI of Candidate AP's and Previous AP is not greater than 5 dbms
- Candidate AP is not the Best AP in the Scan List
- Candidate AP is also not the Second Best AP in the Scan List
- Gradual Roam. Current and previous RSSI average difference is 0-5 dbm
- Sporadic Roam. Current and previous RSSI average difference is greater than 5 dbm
- Roam due to connected SSID packet not found in scan cache
- Extreme Roam. Instant RSSI and current RSSI average difference is greater than 6 dbm
- Roam due to Very Weak AP Signal. Less than -85 dbm
- No Access Points are seen in Preferred Band
- Low Signal Strength Access Points are seen in Preferred Band
- Unknown Scenario
- Disconnect Reason Unknown
- Disconnect Reason - Screen OFF
- Disconnect Reason - WiFi Disabling
- Disconnect Reason - WiFi Disabled
- Disconnect Reason - New Profile Added in UI
- Disconnect Reason - Profile Updated in UI
- Disconnect Reason - Profile Deleted in UI
- Disconnect Reason - Deauth Packet from AP
- Disconnect Reason - Profile Roam from UI
- Disconnect Reason - Deauth packet from Driver
- Low Signal Strength.(condition: formula made of RSSI, TX Loss , RX Loss)

- High Interference.(condition: formula made of SNR, TX Loss , RX Loss)
- High Channel Load.(condition: formula made of AP's IE load, TX Loss , RX Loss)
- Poor Coverage Area.(condition: scan yields weaker than -65 dBm 'best' coverage)
- Tx Power and Data Rate Mismatch.

### Standard IEEE Codes for De-Authentication Packets

When the device receives a de-authentication packet from the AP, the analyzed reason strings may include an IEEE 802.11 standard reason code. The reason code is retrieved directly from the 802.11 packet. The reason code value, located in the expanded view, is prefixed with **DEAUTH CODE**.

To view the meanings of de-authentication code values, refer to the reason codes table, found in the IEEE 802.11 standard.

## Voice Analysis Only Reasons

### WARNING Severity Class Headers

Rows containing a warning message display the **Warning Details** button. Touch **Warning Details** to display one or more sub-reports.

Each sub-report contains one of the following parameters:

- CONSECUTIVE PACKET LOSS type - More than 3 packets lost consecutively within a sub-window
- PACKET LOSS EXCEEDED type - More than 20% packets lost within a sub-window
- LATENCY EXCEEDED type - Latency yielded value larger than 200ms
- JITTER EXCEEDED type - Jitter yielded value larger than 100ms.

The CONSECUTIVE PACKET LOSS and PACKET LOSS EXCEEDED parameters may also provide one of the follow analyzed reasons:

- Packet Loss during Power Save
- Packet Loss during Roam Scan
- Packet Loss during Low Signal Strength
- Packet Loss during High Interference
- Packet Loss during High Channel Load
- Packet Loss in Poor Coverage Area
- Packet Loss - Loss condition happened with none of the above situations.

# Packet Capture

## Introduction

Packet capture automatically saves pcap files to local storage in the `smu_pcap` folder as password protected ZIP files. To set the password, see [Configuration on page 50](#).

To enable packet capture, use one of the following methods:

- [Roaming Analysis Settings on page 24](#)
- [Voice Analysis Settings on page 34](#)
- [Logging on page 46](#)

To view stored packets:

1. Ensure Roaming Analysis, Voice Analysis, and logging are 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. When prompted, enter the same WFW Analyzer 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 traffic that is handled by the WiFi stack in its current 802.11-STA role. For example, a device that is connected, or attempting to connect.

- Includes internal outgoing packet attempts, and incoming packets.
- 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.
- Not encrypted (WLAN encryption).
- 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 the following 802.11-Mgmt packet types:

- Probe Response. Including all 'home' and 'off-channels' scans Responses.
- Authentication req/rsp. Info-Elements content of Auth of FT/11r are not captured.
- (Re)-Association request/response
- De-authentication
- Disassociation.

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
  - Sub-headers of 802.11-Mgmt: View all Info-Elements from Tagged sections, except for Auth of FT/11r.
  - Bits of Capabilities-Information sub-header in Probe-Response: Not supported for other types.
- 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.

