

Wireless Analyzer



ZEBRA

Administrator Guide for Android™

2023/06/12

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. ©2023 Zebra Technologies Corporation and/or its affiliates. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements.

For further information regarding legal and proprietary statements, please go to:

SOFTWARE: zebra.com/linkoslegal

COPYRIGHTS: zebra.com/copyright

PATENTS: ip.zebra.com

WARRANTY: zebra.com/warranty

END USER LICENSE AGREEMENT: 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.

Contents

Introduction.....	6
Operational Requirements and Best Practices.....	7
Use Cases and Features.....	8
User Interface Navigation.....	10
Opening Analyzer.....	10
Enabling and Disabling the Analyzer.....	11
Common Layouts and Menus.....	11
About Page.....	13
Interactive Menu Options.....	14
Saved Data Options.....	15
Clear Sessions.....	15
Export Saved Data.....	15
Camera Preview.....	15
Using Features.....	17
Home Screen.....	17
Status.....	18
Connected IP Network.....	18
Device Information.....	19
Scan List.....	20
Scan List Settings.....	21

Detailed Capabilities for BSSID.....	21
Connection Analysis.....	25
Module Selections.....	26
Load, Delete, and Export Sessions.....	28
Connection Analysis Settings.....	29
Roaming Analysis.....	30
Roam Analysis Settings.....	30
Advanced Reports.....	33
Voice Analysis.....	39
Voice Analysis Settings.....	40
Advance Reports.....	43
Networking Tools.....	45
Ping.....	45
TraceRoute.....	47
Device's Coverage View.....	48
Coverage View Settings.....	51
Logging.....	52
Advanced Configuration.....	53
Appendix A: Configuration.....	55
Introduction.....	55
Configuration of Password Using StageNow.....	56
Setting the Password.....	56
Appendix B: Packet Capture.....	60
Introduction.....	60
Packet Capture Content.....	60
Supported Packet Types.....	61
Supported Headers and Content.....	61
Appendix C: Report Logger.....	62
Introduction.....	62
Content Format.....	62

Header - Event Types.....	62
Roaming and Voice Analysis Headers.....	62
Voice Analysis Only Headers.....	64
Additional Parameters (when line item is expanded).....	64
Roaming and Voice Analysis Reasons.....	64

Introduction

This guide provides information for the Zebra's **Wireless Analyzer** Application (formerly known as WorryFree Wi-Fi Analyzer or WFW Analyzer). The exact application name and user interface might differ slightly on different Zebra operating systems. This Administrator Guide is inclusive of both older and newer names and uses the term **Analyzer** for short.

The icon below graphically represents the Analyzer Application.



The **Analyzer** application is supported in Zebra's device types and OS versions mentioned in Zebra's **Wireless Analyzer** portal site:

zebra.com/us/en/support-downloads/software/productivity-apps/wireless-analyzer.html

The Analyzer is an admin/technical power tool Application, which is prohibited for end-user access. If mishandled, it can interrupt the Wi-Fi connectivity and performance of the device. The Analyzer is an application user interface for purposes of viewing and operating its supported features directly on the device. It is not communicating with or uploading data to any centralized service solution.

Zebra has a separate Wireless Insights product that uses the same device resources as the Wireless Analyzer. If the Wireless Insights product is deployed and enabled on device(s) under a centralized solution of certain Zebra Partners, then the Analyzer Application shall not be used on the same device unless done so by trained Zebra personnel, or with guidance on how to switch between the two safely.

The Analyzer version is built-in inside the product and might sometimes evolve if the product build number is upgraded to a later respective one. However, the Analyzer version cannot be upgraded or downgraded on a given product build number.

The Analyzer is disabled by default in the Zebra device software. It can be manually enabled and disabled any time from the application user interface if the application is allowed and accessible for use, or from Device Management and staging tools powered by Zebra Mobility Extensions (MX). The analyzer includes multiple independent features targeting different purposes and use-cases, detailed in [Use Cases](#).

Operational Requirements and Best Practices

This section describes the best operational and administrative experience while using the Analyzer User Interface.

- The Analyzer must be activated if it was not activated before, and the Android's Wi-Fi must be enabled. See more details on Activation in respective chapter.
- If the specific device model is one that requires a Mobility DNA license (per the Product Support table), then the installation of that license is a pre-requisite to the activating the Analyzer step.
- The Analyzer requires that the Android Locationing service be globally enabled in the device (default in Android). When enabled, the Analyzer is automatically permitted to use it. There is no need to manually enable permission for it.
- When the device is a production end-user unit on which the Analyzer is used by an administrator or any facilitator, and before the unit is returned to the end-user, it is recommended to not only stop the running feature, but to also de-activate the Analyzer.
- The Analyzer is saving features data (sessions database) in the device's local storage for feature management purposes, and for exporting actions further detailed in the document. That database file is secure and accessible by the Analyzer only in runtime, and must not be deleted.
- Do not change the Wi-Fi settings on the device while using the Analyzer features.
- The Analyzer cannot run multiple features in parallel, with the exception of logging. Logging is the only feature that can run either in standalone or together with each of the other features.
- Changing the font and display size on the device from the default settings is not recommended as it may cause the app to not display correctly.
- Using Multi-Window mode is not recommended as it may cause the app to not display correctly.
- When using the app on an Android device, the primary user must be logged in as the multi-user feature is not supported by the Analyzer app.

Use Cases and Features

Analysis Data provided by Analyzer saves time and costs by enabling administrators and technicians to quickly create action-items from the data on how to improve or mitigate performance issues. Actions may include reconfiguring the RF or WLAN system, reconfiguring the device, or other issues that require attention. The following table describes some of the more common Analyzer use cases.

Table 1 Use Cases and Analyzer Features

Use Case	Detailed Description	Analyzer Feature
Basic connectivity information	View the status of the connected device, including the connected AP, RSSI, channel, IP/DHCP/DNS, MAC address, and more.	Home screen of the Wireless Analyzer
Wi-Fi surveys and coverage from the connected device view	<ul style="list-style-type: none">• 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 configuration, retrieved directly from the information elements of the AP's beacons.	Scan List; Device Coverage View
Wi-Fi Roaming Analysis	<ul style="list-style-type: none">• 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.• Can be used in Passive mode without any consumption of resources, or in Active mode with additional synthetic data traffic.	Roaming Analysis

Table 1 Use Cases and Analyzer Features (Continued)

Use Case	Detailed Description	Analyzer Feature
Voice Quality Analysis	<ul style="list-style-type: none"> View real-time data about the performance of voice traffic, combined with Roaming Analysis data of the Roaming Analysis feature (inclusive). In Passive mode - it detects SIP calls in runtime of the Device's Voice applications (if deployed), and produces periodic quality reports about the voice traffic. In Active mode – it generates synthetic 'voice' traffic and produces periodic quality reports about that traffic. 	Voice Analysis
Wi-Fi Connection Analysis	On demand inspection and troubleshooting of initial full associations to the SSID and IP network, including causes and reasons of connection failure (if applicable) from each sub-layer of the connection.	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 data.	Logging
Troubleshoot and compare Fusion configuration parameters.	<ul style="list-style-type: none"> View and Change 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	<ul style="list-style-type: none"> 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 . 	Network Tools > Ping/Trace Route

User Interface Navigation

This section describes how to navigate the Analyzer Application user interface screens.

Opening Analyzer

This section describes how to open the Wireless Analyzer Application on your mobile device.



NOTE: Before using the Analyzer app, ensure that Wi-Fi is enabled on your mobile device.


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

Figure 1 Analyzer Screen



Enabling and Disabling the Analyzer

This section describes how to enable and disable the Analyzer.

By default, the Analyzer is not configured with a Zebra operating system, it must be activated for use with runtime features.

1. To activate the Analyzer from the Main Menu or Home Screen, tap the **Analyzer Not Activated** switch. The Wi-Fi connection will restart itself. This same operation can be administered from MDM tools or Staging operations.
2. To deactivate the Analyzer from the Main Menu or Home Screen when not using the analysis features, tap the **Analyzer Activated** switch to change to Not Activated. The Wi-Fi connection will restart itself. This same operation can be administered from MDM tools or Staging operations.

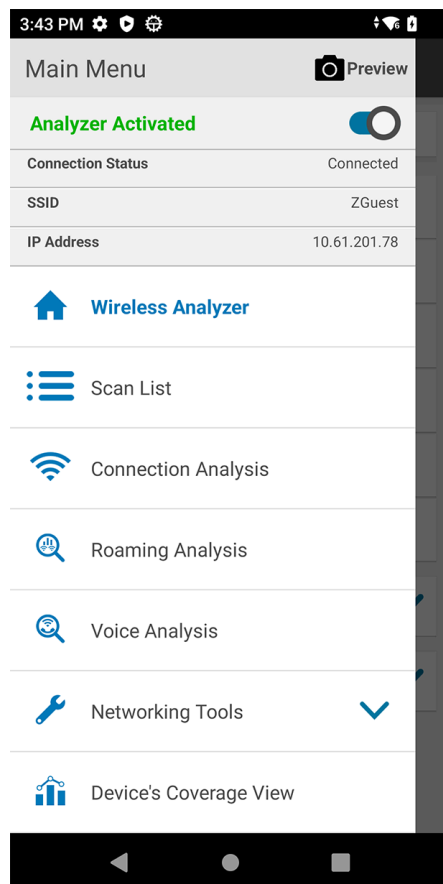
Common Layouts and Menus

This section details some common user interface layouts and menu options.

The application home page is highlighted by a Wireless Analyzer banner at the top.

The main features of the app are accessible from the Main Menu, which can be accessed by tapping the hamburger menu at the top left of the screen, or by dragging the left slide-in drawer. This can be done from any page or sub-page of the application.

Figure 2 Main Menu



When inside a feature page, for example Voice Analysis, it is displayed on the banner at the top of the screen.




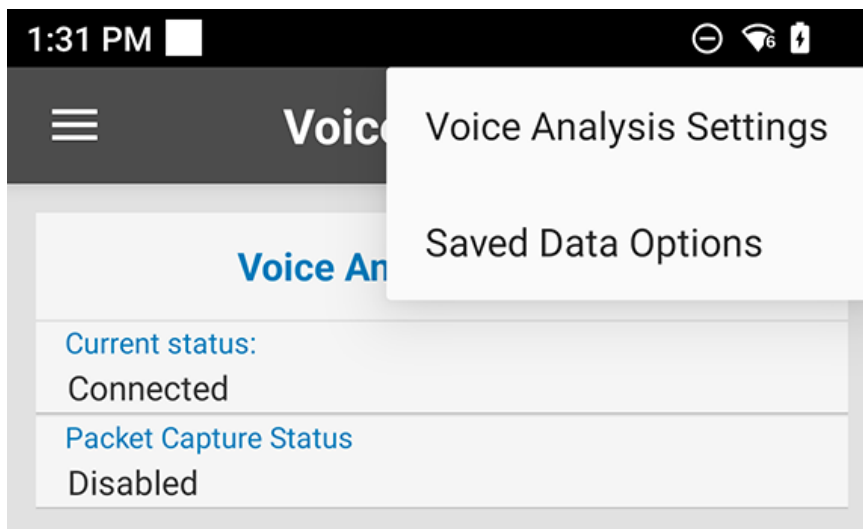
Tap  in the top right corner of the screen to access a feature-specific Settings page and other global actions.

Figure 3 Settings Drop-down



Each feature has additional user interactions on the page as described in other sections.

About Page

This section describes shows the About and the Wireless Analyzer version. Have this number available when contacting Zebra support.

Figure 4 About Screen



Interactive Menu Options

This section details additional interactive options of the Analyzer, including the use of a Floating Menu Action Button.

If you are viewing a session this is not currently capturing data, tap  to display the Floating Menu.



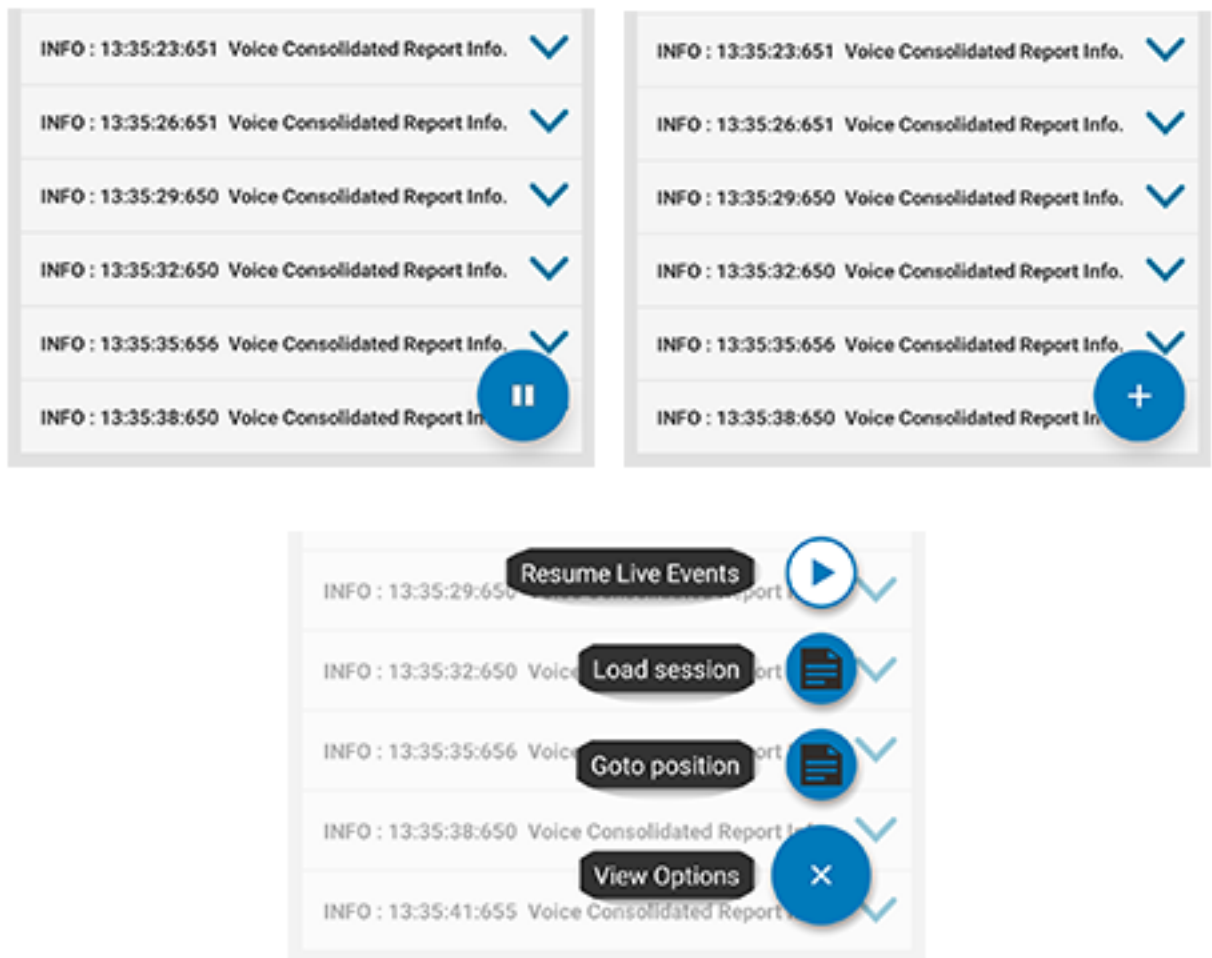
If viewing a session that is currently capturing data, tap  to pause the session (which saves the data in the background), then tap  to display the Floating Menu. Tap **Resume Live Events** to return to the live timeline.

Figure 5



- **Resume Live Events:** Tap to resume live monitoring.
- **Load Session:** Tap to load any saved sessions in the pop-up box.
- **Goto Position:** Use the slider and buttons to navigate through data.







Saved Data Options

This section describes the steps needed to clear Analysis session data, or export saved data.

Features of the Analyzer include:

- The ability to save data in the SD card in session context.
- Manage and export stored sessions.

To access the Clear and Export UI options:

- If in Roaming Analysis and Voice Analysis features: Tap  > Analysis >  > Save Data Options
- If in Connection Analysis feature: Navigate to the Result Details page and tap the Floating Menu 
- If in Device Coverage View feature: Tap  > Device Coverage View >  > Coverage View Settings >  > Wireless Analyzer Database Options

Clear Sessions

This section shows the steps needed to clear selected or all Analysis session data.

In some features the Clear Sessions function might be called Delete Sessions, but in either case, previously collected sessions are removed from the device and become unavailable for off-line viewing.

To clear Analysis session data:

1. Select the session to clear, or tap **Select All** to clear all sessions.
2. Tap **OK**.

Export Saved Data

This section details how to export session data to text files containing JSON objects.

The Analyzer app saves the files to the smu folder.

To export all saved Analysis session data:

1. Select the session to export, or tap **Select All** to export all sessions.
2. Tap **OK**.



NOTE: For Roaming Analysis and Voice Analysis features, text files containing JSON objects are created separately for each tab in Analysis > Monitor & Reports.



To view the exported files, ensure Analysis and logging are not running and collect files from the device either locally or remotely, depending on the SD card access method available and permitted.

Camera Preview

This section explains how a device with a camera can use a Camera Preview overlay box on any page or sub-page of the Analyzer.

During a live capturing session, the user can capture the Analyzer data while recording the physical location of the device. The Camera Preview window is displayed, the camera is aimed forward, and the Android device is used to shoot or record the Analyzer screen.

For example, during a Roaming Analysis or Coverage View session, there might be a Wi-Fi troubleshooting situation showing the location and the motion of the device in the physical environment, while the data is streaming with timestamp information. The correlation between the events data and the screen captures of where the issue occurred could provide important context, in addition to a better analysis.

To access the Camera Preview, tap , and tap  Preview .



You can drag the preview box to any place on the screen so it does not obscure important data. You can use the built-in tools on the Android device to record the screen to video, or to take a screenshot.

Figure 6 Camera View



Using Features

This section describes these Analyzer Application operations and features and how to use them.

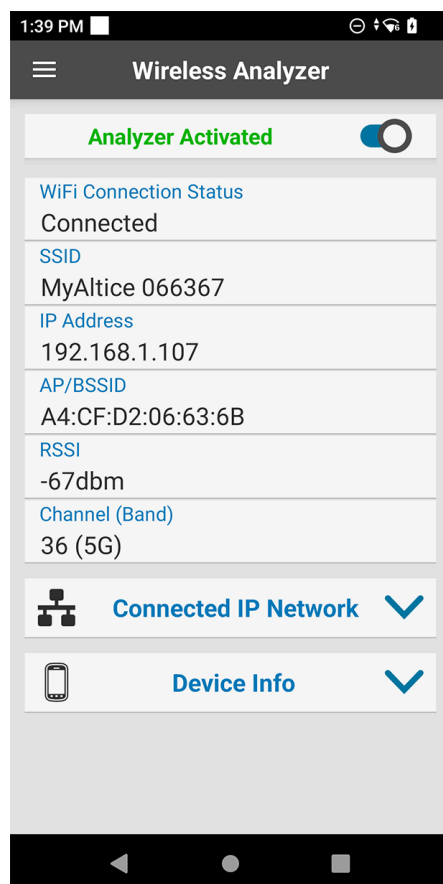
Home Screen

This section describes how to read the information on the Analyzer home screen.

The Home Screen displays:

- Device Status
- Connected IP Network
- Device Information

Figure 7 Home Screen



Home Screen information continues to update when analysis and data collection are disabled.

Status

The Home Screen displays the following device status information:

- Wi-Fi Connection Status
- SSID: Name of connected WLAN network
- IP Address
- AP/BSSID: Basic Service Set ID of the Access Point to which the device is connected
- RSSI: Received Signal Strength Indicator of the AP to which the device is connected
- Channel (Band): Displays the channel and the band of the AP to which the device is connected

Connected IP Network


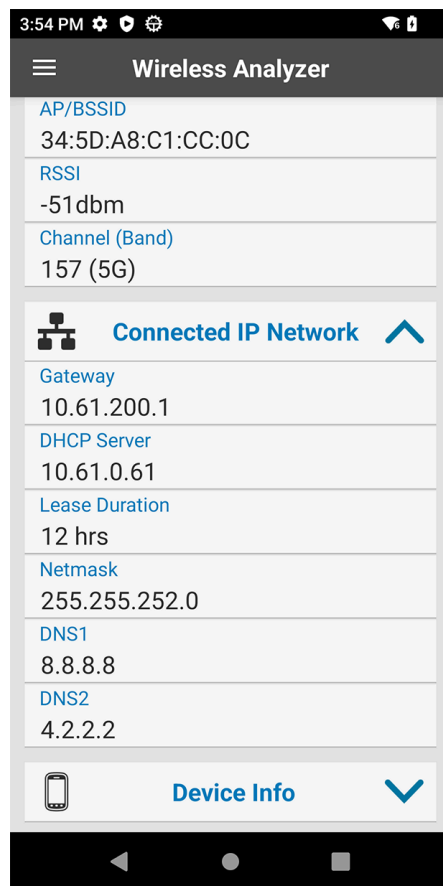
To view the following details of the connected IP network, tap  .

Figure 8 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: Domain Name System 2 (DNS2) address

Device Information

To view the Device info, tap .

Figure 9 Device Info



- Device Product Name
- Device MAC: the physical Wi-Fi hardware MAC address
- Wi-Fi MAC: the Wi-Fi Connected MAC address of the device. If the device is configured with Wi-Fi feature Random MAC enabled (default on Android 11 and above), then this Wi-Fi MAC will reflect the Random MAC of the current connection, which is different than the Device MAC. If the device is configured with Wi-Fi feature Random MAC disabled (intentionally disabled / non-default on Android 11 or above, or default on Android 10), then this Wi-Fi MAC will have the same value as the Device MAC.
- Operating System: the Android dessert version

Scan List

Scan List 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.


To view the Scan List, tap  > **Scan List**

Figure 10 Scan List



SSID	BSSID	RSSI	Channel / Band
ZGuest Connected	34:5d:a8:c1:cc:0c	-49	157 /5G
ZESIMTest	3c:37:86:cf:3a:d5	-40	1 /2.4G
ZESIMTest-5G	3c:37:86:cf:3a:d4	-50	153 /5G
WiFi6-TEST	34:5d:a8:c1:cc:0a	-50	157 /5G
ZDemo	34:5d:a8:c1:cc:0e	-50	157 /5G
ZWireless	34:5d:a8:c1:cc:0b	-51	157 /5G
ZScan	34:5d:a8:c1:cc:0d	-51	157 /5G
ZCorp	34:5d:a8:c1:cc:0f	-51	157 /5G
TSD_MSP4	b4:c7:99:4f:16:90	-60	1 /2.4G
ETGAP01-5G	80:37:73:d5:fc:9f	-61	153 /5G
VT_19a	50:06:04:7b:16:2b	-62	44 /5G

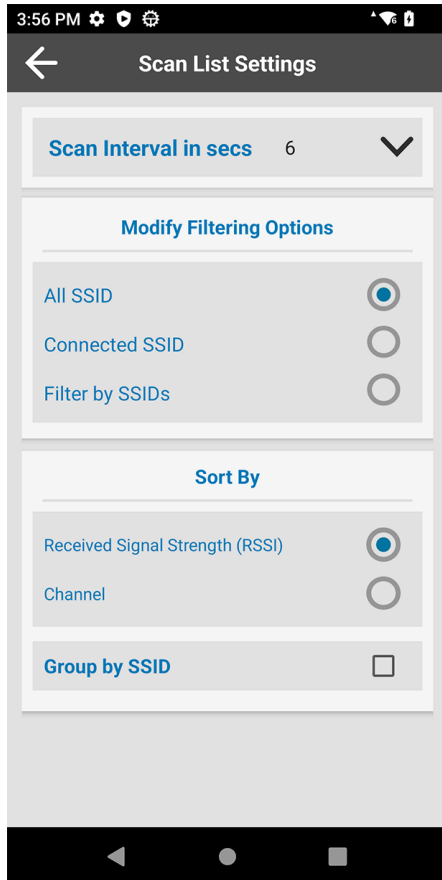
For each BSSID, the following information is displayed:

- SSID - Name of an 802.11 wireless local area network (LAN).
- BSSID - MAC address of the access point BSSID.
- RSSI - Received signal strength in dBm. The closer the dBm number is to 0, the stronger the signal.
- Channel/Band - Channel and frequency band.

Scan List Settings

Go to the **Scan List** screen and tap , then select **Scan List Settings**.

Figure 11 Scan List Settings



- Scan Interval: Select to set the fixed interval between ongoing scans. Note that the interval options available in the drop-down box are not configurable and they may vary in different device models.
- 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.
 - Group by SSID: Select to group SSIDs with the same name. SSIDs are listed in alphabetical order.

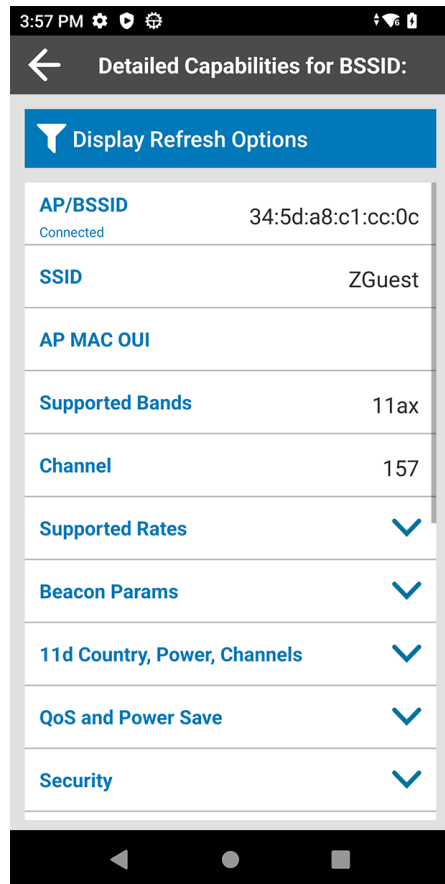
Detailed Capabilities for BSSID

Data depicted in the Detailed Capabilities views is retrieved directly from Scan packets (probes and beacons) advertised over the air by the corresponding AP/BSSID.

A physical AP is typically dual or tri band (2.4GHz, 5GHz, and 6GHz if applicable), where each band of the AP has a unique BSSID identifier. Each BSSID of the same AP (and multiple other APs) is listed as a unique BSSID item on the Scan List main screen, and the detailed capabilities views reflect the specific one.

Go to the **Scan List** screen and tap a BSSID to display detailed capabilities.

Figure 12 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 affiliated physical bands, for example: 11b, 11g, 11bg, 11bgn, 11a, 11an, 11ac, 11ax
- **Channel:** Displays the BSSID's channel number
- **Supported Rates:** Tap the down arrow next to **Supported Rates** to view the BSSID's supported rates of legacy data-rates, not including indexes of Modulation Coding Scheme (MCS) if applicable.


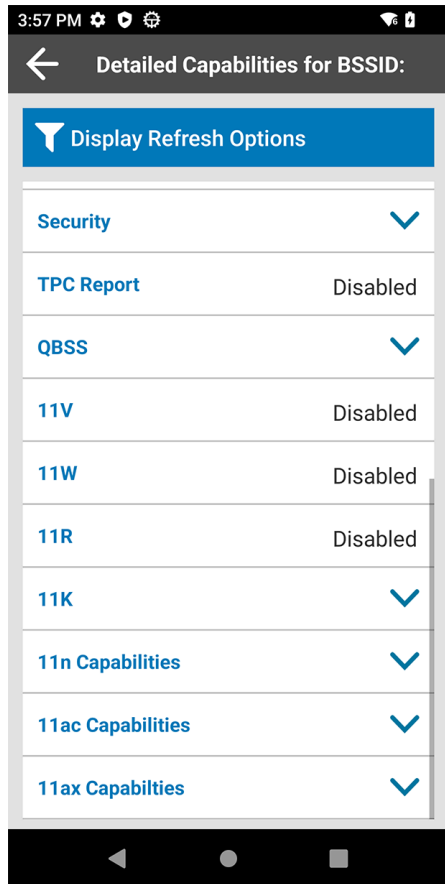



- Beacon Params: Tap the down arrow next to **Beacon Params** to view the BSSID's beacon interval and the beacon Delivery Traffic Indication Message (DTIM) period value.
- 11d Country, Power, Channels: Tap the down arrow to view the BSSID's details which are contained in 802.11d (Country Code) element, if advertised by the BSSID.
- QoS and Power Save: Tap the down arrow next to **QoS and Power Save** to view the BSSID's QoS and Power Save information, if advertised by the BSSID.
- Security: Tap  next to **Security** to view the BSSID's WLAN-security information.

Figure 13 Detailed Capabilities for BSSID cont.



- TPC Report: Tap  next to **TPC Report** to view the BSSID's Transmit Power Control value, if enabled and advertised.
- QBSS: Tap  next to **QBSS** to view the BSSID's QoS enhanced basic service set values such as station count, channel utilization, and available admission value.
- 11V: Tap  next to **11v** to see if the BSSID's BSS Transition is enabled.
- 11W: Displays if 11w is enabled
- 11R: Displays if 11r is enabled

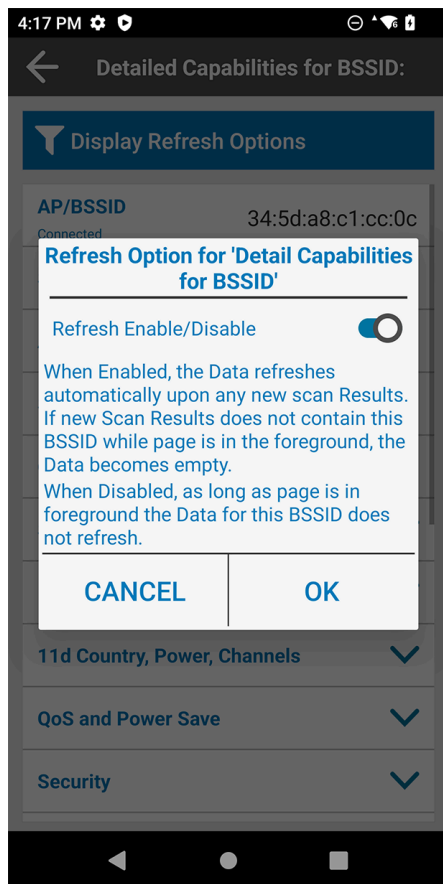
- 11K: Tap the down arrow next to **11k** to see if the BSSID's neighbor report is enabled.
- 11n Capabilities: Tap the down arrow to view the BSSID's HT element (selective HT fields shown).
- 11ac Capabilities: Tap the down arrow to view the BSSID's VHT element (selective VHT fields shown).
- 11ax Capabilities: Tap the down arrow to view the BSSID's HE element (selective HE fields shown).

Display Refresh Options for the Detailed Capabilities Page

Use this feature to Enable or Disable a refresh logic for this page according to the following dynamics:

- When enabled, the data refreshes automatically upon any new Scan Results. If new Scan Results does not contain this BSSID while the page is in the foreground, the data becomes empty.
- When disabled, and as long as the page is in the foreground, the data for this BSSID does not refresh from new scan data and remains locked on the screen.
- Tap **Display Refresh Options** to control the Enable/Disable feature.

Figure 14 Display Refresh Options

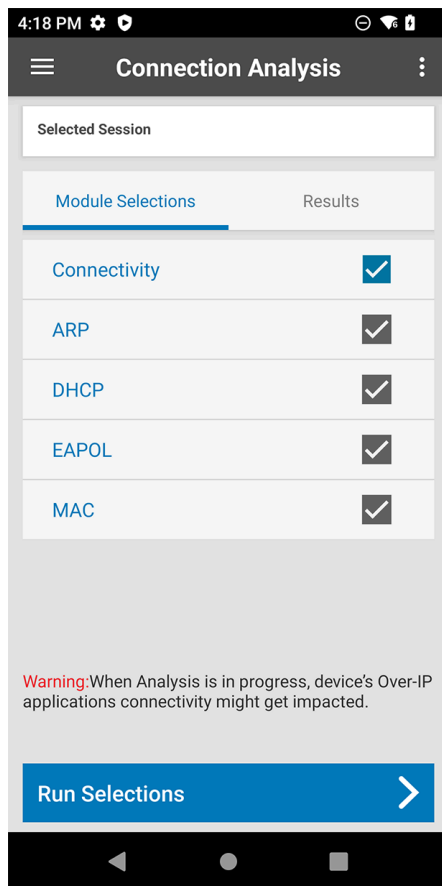


Connection Analysis

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 runs on the connected WLAN network, unless configured differently in Settings. See [Connection Analysis Setting](#).

Figure 15 Connection Analysis



- **Connectivity:** The Analyzer initiates this test only after the MAC, EAPOL, and DHCP are completed successfully, and it 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):** The Analyzer initiates this test only after the MAC, EAPOL, and DHCP are completed successfully, and it analyzes the ARP process using resolved parameters from the DHCP layer.

- **Dynamic Host Configuration Protocol (DHCP):** As part of running the Connection Analysis feature, the DHCP is initiated automatically by Android, and the Analyzer passively analyzes the native Android DHCP process.
- **Extensible Authentication Protocol over LAN (EAPOL):** As part of running the Connection Analysis feature, the EAPOL (if applicable to the network) is initiated automatically by the Wi-Fi Stack connection, and the Analyzer passively analyzes the EAPOL process. If the EAPOL is not required, for example, with an open network, the analysis is skipped.
- **Media Access Control (MAC):** As part of running the Connection Analysis feature, the MAC connection (authentication and association) is initiated automatically by the Wi-Fi Stack connection, and the Analyzer passively analyzes the 802.11 exchange with the AP/BSSID.

Module Selections

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


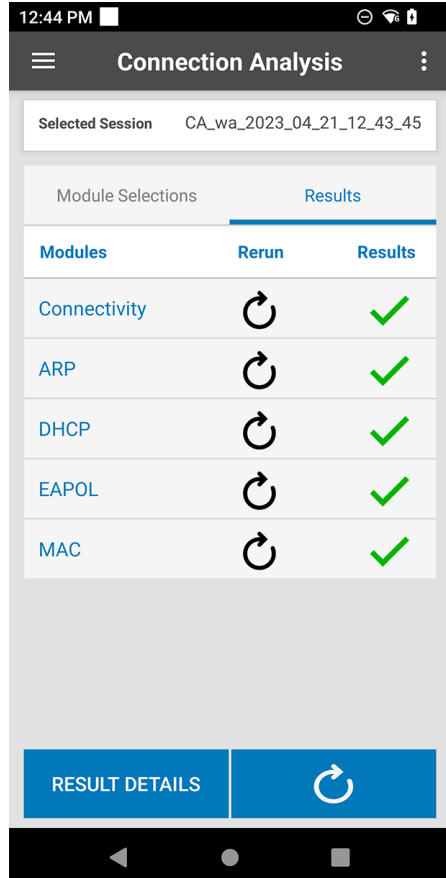
1. Tap  > **Connection Analysis** > **Module Selections**.
2. Tap a network layer to select it. The box next to the selected layer is checked and turns blue. The network layers below it are automatically checked and turn gray. To clear all selections, tap the blue check box.
3. Select **Run Selections**. The **Results** tab displays.
4. When an analysis is complete the results display in the **Results** tab.

Figure 16 Connection Analysis Results




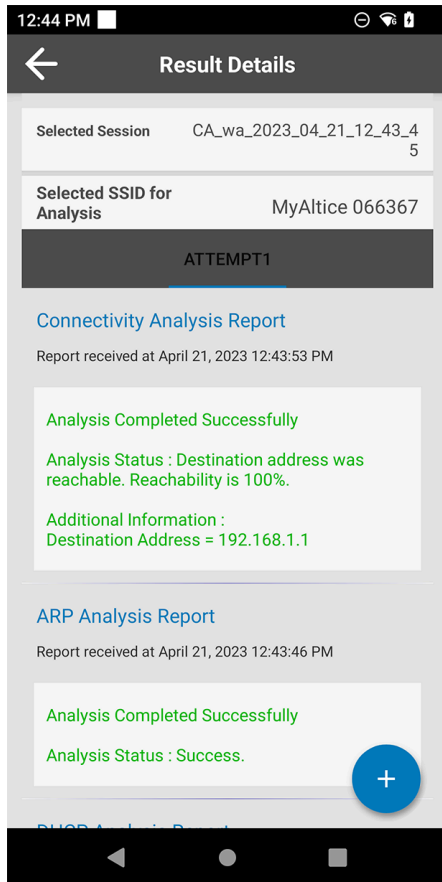

5. Select  to rerun connection analysis for a selected layer or all layers.
6. Tap **Show Result Details** to display detailed analysis reports for each network layer.
7. The **Results Details** screen displays the network layers in the same order as they appear on the **Results** tab.

Figure 17 Result Details



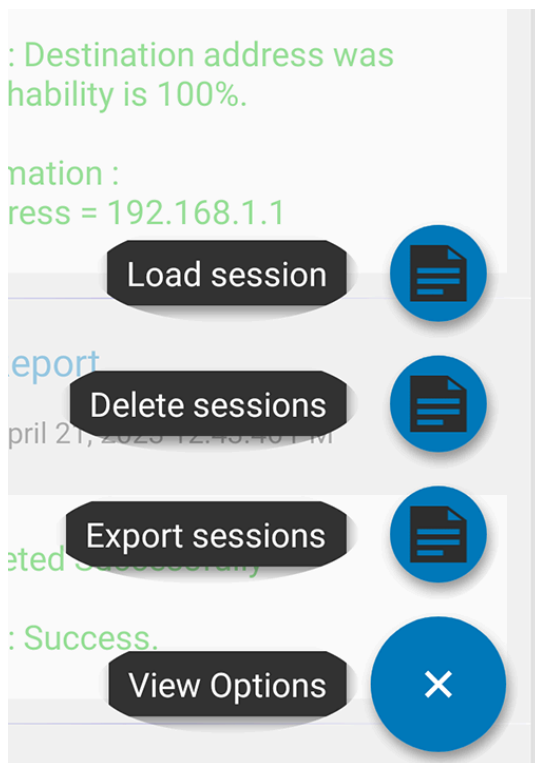
NOTE: In cases where the basic connection layers (MAC, EAPOL and DHCP) are failing for any reason, it is expected that the Wi-Fi and Android will attempt to reconnect automatically. In that case, the view of the **Results Details** will show each **Attempt** detail in a separate tab. The dark gray bar will have multiple Tabs, for example ATTEMPT1, ATTEMPT2, and pressing on each expands the details view.

Load, Delete, and Export Sessions

Tap  to display the Floating Menu action button in the **Results Details** page.

If you need to load a previously captured session, click **Load session** and select from the listed sessions in the dialog box. If you need to delete or export connection analysis session(s), the operations of **Delete sessions** and **Export sessions** are described in [Saved Data Options](#).

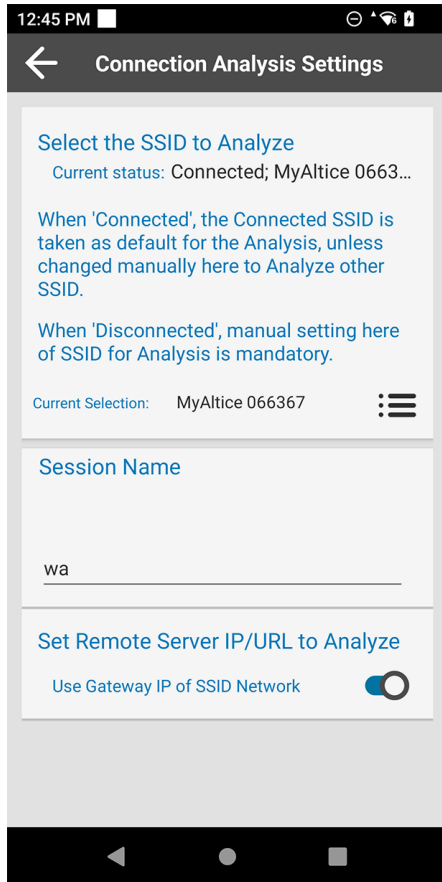
Figure 18 Load, Delete, and Export Sessions





Connection Analysis Settings

Tap  and select **Connection Analysis Settings**. By default, analysis runs on the connected WLAN network.

Figure 19 Connection Analysis Settings




To select a different network:

1. Tap . A list of previously saved networks displays.
2. Tap **Network**.
3. Select **OK**.
4. Select .

Session Name: The Connection Analysis test session is saved to the Analyzer database with a prefix (for example, “wa” shown, can be configurable) appended with date & time stamp. The results of the session

are loaded and viewed in the previous Result Detailed page, by pressing  on that page.

A reachability test is performed by default to the connection’s Gateway IP address. To configure a remote destination that is not the Gateway IP, such as any remote IP address, URL, or Fully Qualified Domain Name (FQDN):

- Tap the switch next to **Use Gateway IP of SSID Network**.
- Enter the remote IP, URL, or FQDN.
- 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.




Roaming Analysis runs continuously and collects data when the Analyzer is running in the background, including when the app is closed. If the device is restarted, and if the Analysis mode of the session is Passive, the session will resume automatically after the restart. If the Analysis mode is Active, it will not resume automatically after the restart.

Use these best practices when running Roaming Analysis:

- In Active mode, if a session of more than six hours is required, stop the live session and start another.
- It is not recommended to run high throughput applications while Analysis is in Active mode.
- It is not recommended to run any other feature in parallel to Analysis, except Logging (packet capture), if needed, for short, selective parallel periods. This is applicable to both Active and Passive modes.

Before starting Roaming Analysis, it is important to making sure that the Settings of the Analysis are set appropriately to the use case and purpose. Use Cases can be reviewed in [Table 1](#) at the beginning of this document.

Please review the Roaming Analysis Settings section before starting the Analysis session.

- To start a Roaming Analysis, tap  > Roaming Analysis > .
- To stop a Roaming Analysis, tap .

Roam Analysis Settings


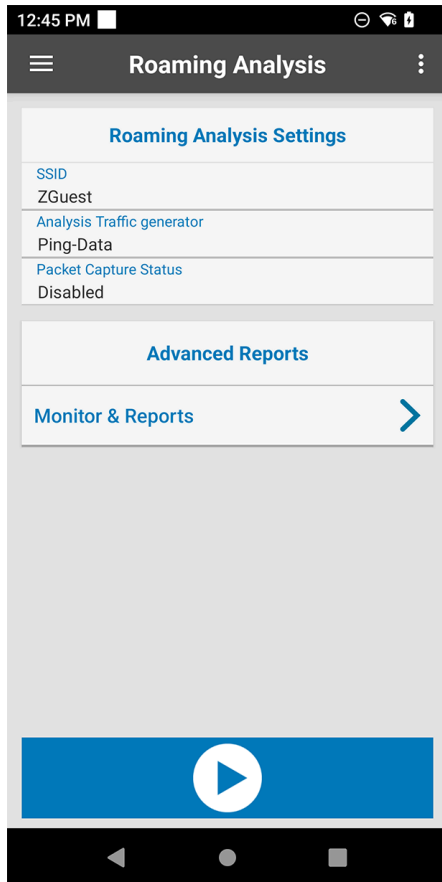
Tap  and select Roam Analysis Settings.


Figure 20 Roaming Analysis Settings



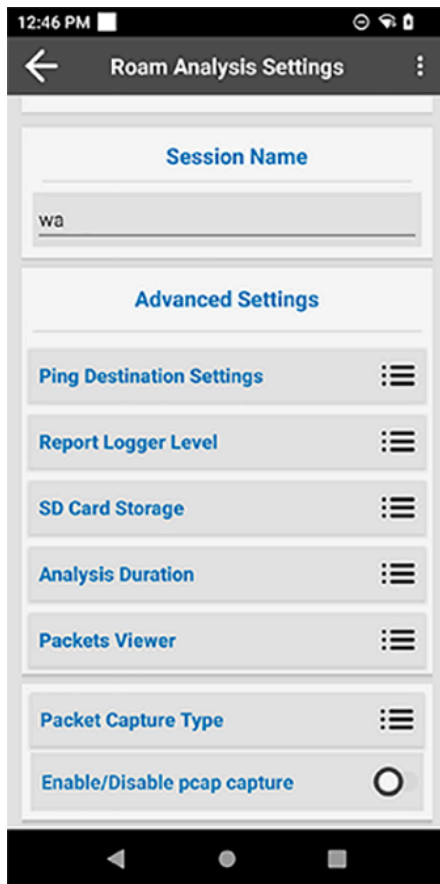
Go to **Analysis Mode** and select the the roaming analysis mode to be performed by the Analyzer.

- Select **Passive** mode and the Analysis only produces reports and data related to the device's Roaming events (handing-off between Access Points), and further provides causes & reasons to Roaming performance issues and failures.
- Select **Active** mode and the Analysis facilitates continuous synthetic ping traffic to a configurable destination. The synthetic traffic is automatically evaluated and produces an additional set of metrics. The ping traffic in this mode simulates continuous data traffic.

Profile Settings is only applicable to Active mode and displays the following:

- Current Status: Displays the current SSID status.
- Current Selection: Tap  to select from a list of available SSIDs. When not connected to a WLAN network, this selection is required.

Go to **Session Name** to enter the desired session name.

Figure 21 Advanced Settings

When in **Advanced Settings**, the following menu appears:

- **Ping Destination Settings:** This setting is applicable only to Active mode. Select whether or not to generate traffic, the default being Generate Constant 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.
- **Report Logger Level:** Select the analysis report level (default: INFO [info | warning | error]).

- **SD Card Storage:** Select a preference for an action which will be taken by the Analyzer if the storage space reaches 80% full:
 - Select **Only Display Live Data** when it is important to keep getting and viewing the live events during the test while the Report Logger is in the foreground, and to avoid deleting old saved data.
 - Select the **Clear space for saving more data.** Delete old data of current session option when it is less important to save old data and more important to save the new incoming data.
 - **Session Storage Duration:** Select the maximum duration for which to save the latest ongoing new data, and any data beyond that duration will be recycled.



NOTE: When in Active Analysis mode, the default is the **Clear Space for saving more data**. In Passive Analysis mode, the default is **Only Display Live Data**.

- **Analysis Duration:** This setting is only applicable to Active mode. Select the maximum duration that the Active analysis will run. The duration cannot be less than the Session Storage Duration of the SD Card Storage, if Active mode remains with its default of **Clear space for saving more data**.
- **Packets Viewer:** This setting is applicable only to Active mode. Select a packet category (default: WLAN Mgmt + Selective Data Packets) to determine which packets are posted in the Packet Viewer Tab.
- **Packet Capture Type:** When enabling the pcap capture, first select the category of Packet Types to be captured and stored in the sdcard. See more in Packet Capture.
 - **Management Packets:** Select this option (default), to capture and save the device's transmitted and received 802.11 Mgmt, plus EAP/EAPOL, DHCP, ARP, ICMP, and DNS.
 - **All Packets:** Select this option to capture and save the Management Packets, as well as all the other device's transmitted and received 802.11 data traffic, for example all the device's operating system and applications transmitted & received IP-unicast traffic data, as well as all received IP-multicast/broadcast traffic.



NOTE: The All Packets selection requires a pre-provisioned password. In this setting, the stored packets are encrypted with the password in the sdcard. See [Configuration](#).

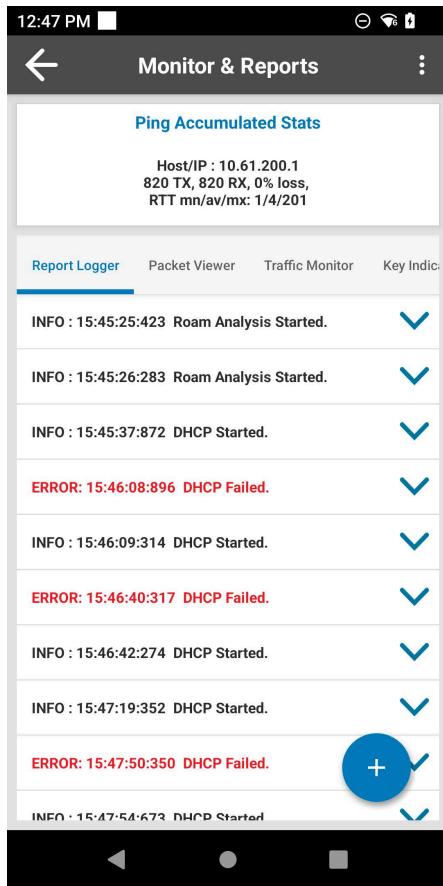
- **Enable/Disable pcap capture:** Enable to capture and store packets, per the Packet Capture Type selection.

Advanced 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.

Monitor and Reports

Tap  > **Roaming Analysis** > **Monitor & Reports** to view Roaming Analysis reports.

Figure 22 Monitor and Reports

- **Ping Accumulated Stats:** This view area is presenting data only in Active mode and remains empty in Passive mode. It displays ping data indicators of synthetic traffic of the Analysis, accumulated in real-time during capturing session, or a final summary of a loaded session.
- **Report Logger:** Displays connectivity and Roaming Analysis results. Tap a row to display detailed parameters and reasons of performance thresholds and issues. For more information, see [Report Logger Content](#).

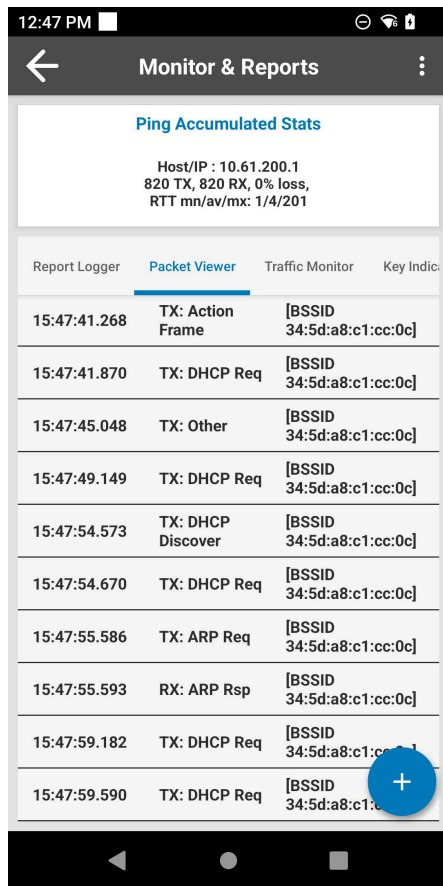
**NOTE:**

When in Active mode, this view shows real-time live events, as well as **logging & saving the entire data**. As long as SD card storage is available (see [SD Card Storage](#) settings), the view allows for interactive UI operations over the saved data, such as scrolling up and down, pause/resume live events, toggling between the other views/tabs and re-entry to the saved data, jumping to a specific position in the log, and more.

When in Passive mode, the view allows for interactive UI operations only if the SD Card Storage settings are changed from the default (see [SD Card Storage](#) settings). If it remains in default settings, the view shows only the real-time events as they happen, only while this specific tab is in the foreground, without the possibility to interact with the data, as it is not saved.

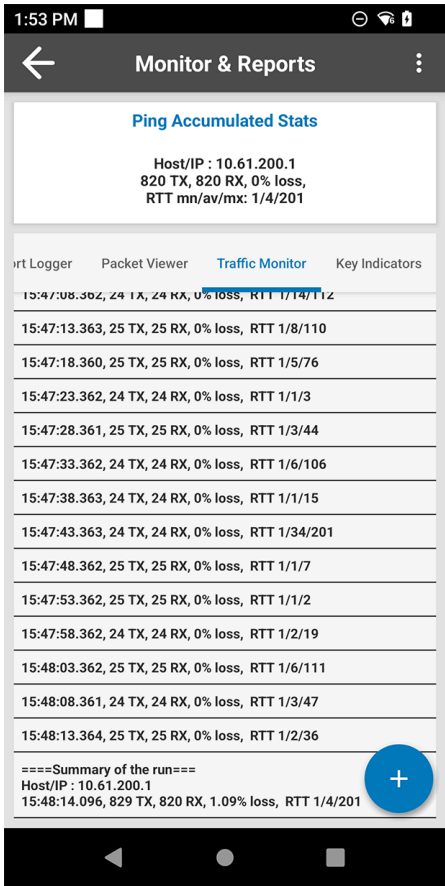
- **Packet Viewer:** This view area is presenting data only in Active mode and remains empty in Passive mode. It displays the time, direction, and type of select packets in a session. Tap a packet to view certain fields from its header content. Packet details include 802.11 management, EAP/EAPOL, ARP, DHCP, DNS, and ICMP.

Figure 23 Packet Viewer



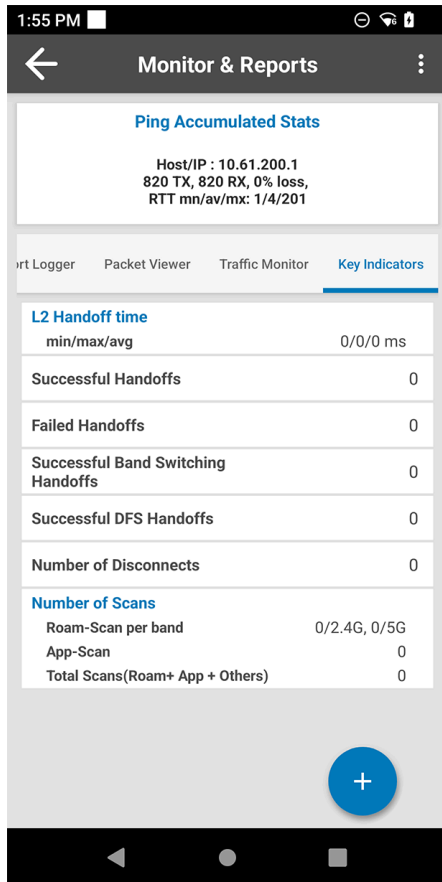
- **Traffic Monitor:** This view area presents data only in Active mode and remains empty in Passive mode. It displays detailed ping statistics. To change the ping refresh interval, see [Ping Refresh Settings](#).
- When specific ping errors are detected, such as 100 percent packet loss, or when there are many consecutive packets loss during ping, tap the information row to view the error report.

Figure 24 Traffic 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.

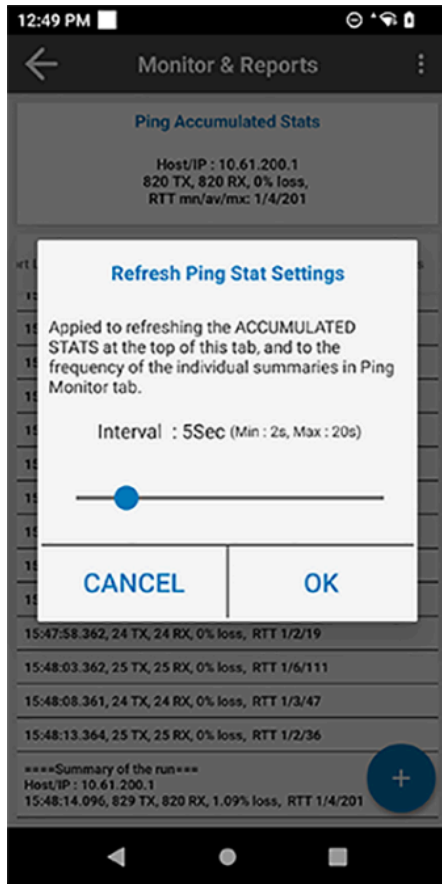
Figure 25 Key Indicators





Ping Refresh Settings

Use **Ping Refresh Settings** to change the time interval between each displayed line of accumulated statistics, where each contains multiple pings (range of displayed-statistics interval: 2 - 20 seconds, default: 5 seconds).

Figure 26 Ping Refresh Settings



To change the time interval between pings:

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

Voice Analysis

Use **Voice Analysis** to troubleshoot or monitor voice traffic performance and get deeper analysis in real-time for WLAN connectivity and link quality issues. The analysis data includes reports, packets, traffic statistics, and performance indicators.

Voice Analysis runs continuously and collects data when the Analyzer is running in the background, including when the app is closed. If the device is restarted, and if the Analysis mode of the session is Passive, the session resumes automatically after the restart. If the Analysis mode is Active, it will not resume automatically after the restart.



Use these best practices when running Voice Analysis:

- In Active mode, if a session of more than six hours is required, stop the live session and start another.
- It is not recommended to run high throughput applications while Analysis is in Active mode.
- It is not recommended to run any other feature in-parallel to Analysis, except Logging (packet capture), if needed, for short, selective periods. This is applicable to both Active and Passive modes.

Before starting Voice Analysis, it is important to making sure that the Settings of the Analysis is set appropriately to the Use Case and purpose. Use Cases can be reviewed in [Table 1](#).



NOTE: Please review the Voice Analysis Settings section before starting the Analysis session.

To start a Voice Analysis session, tap  > **Voice Analysis** > .


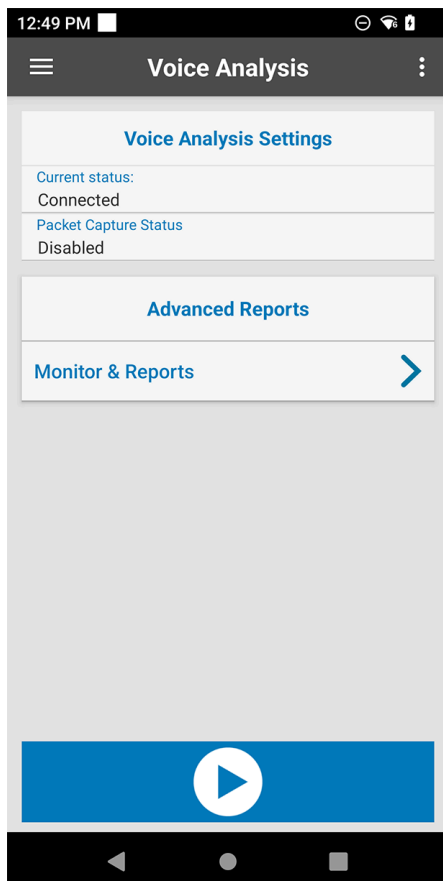
To stop a Voice Analysis session, tap .

Figure 27 Voice Analysis



Voice Analysis Settings


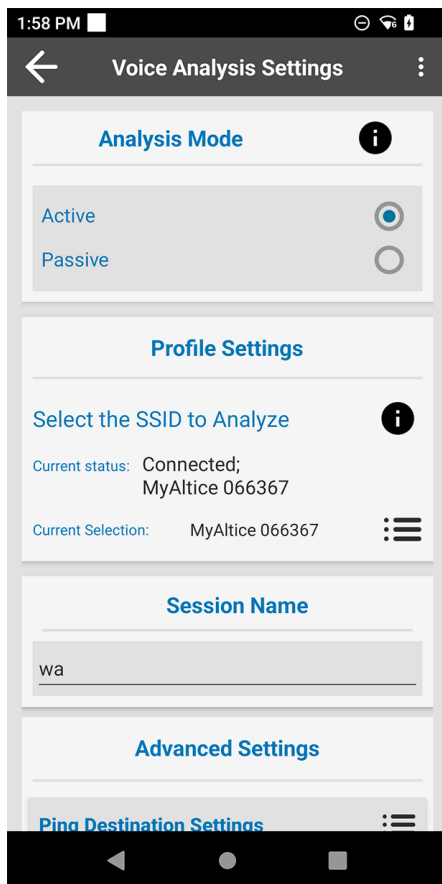
Tap  and select **Voice Analysis Settings**. The main screen displays the following settings:

Figure 28 Voice Analysis Settings



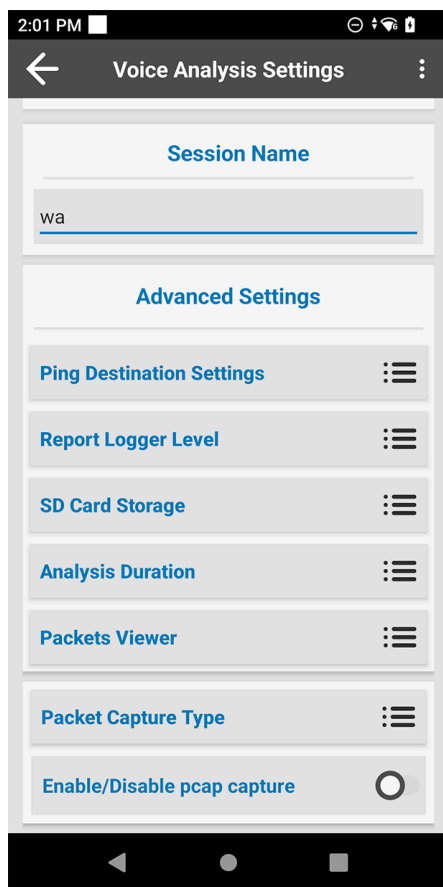
When in **Analysis Mode**, select the mode of the voice analysis to be performed by the Analyzer.

- When Passive mode is selected, the Analysis produces two categories of information:
 - A device's Roaming Events (hanging off between Access Points), which can cause issues and failures in roaming performance. This is the same level of data provided by the Roaming Analysis feature in Passive mode.
 - When the user is making VoIP calls with any standard SIP/RTP application, the SIP & RTP traffic of the application is automatically and passively measured, and additional Analysis data is reported approximately every 3 seconds, about the VoIP traffic metrics.

- When Active mode is selected, the Analysis produces two categories of information:
 - A device's Roaming Events (handing off between Access Points), can cause issues and failures in roaming performance. This is a similar, albeit slightly more detailed, level of data provided by the Roaming Analysis feature in Passive mode.
 - The feature facilitates continuous synthetic Ping traffic to a configurable destination. The synthetic traffic is automatically evaluated and produces an additional set of metrics data. The Ping traffic of this mode simulates VoIP traffic; packet-interval of VoIP codec, Type-of-Service (ToS) tag of VoIP, size of packets. In this mode the Analysis does not produce metrics about the application's non-synthetic SIP & RTP traffic if happening in parallel.

In Active mode of the Voice Analysis, the Profile Settings, Session Name, and all the settings of the Advanced Settings, are configured identically to the Roaming Analysis Settings of Active mode.

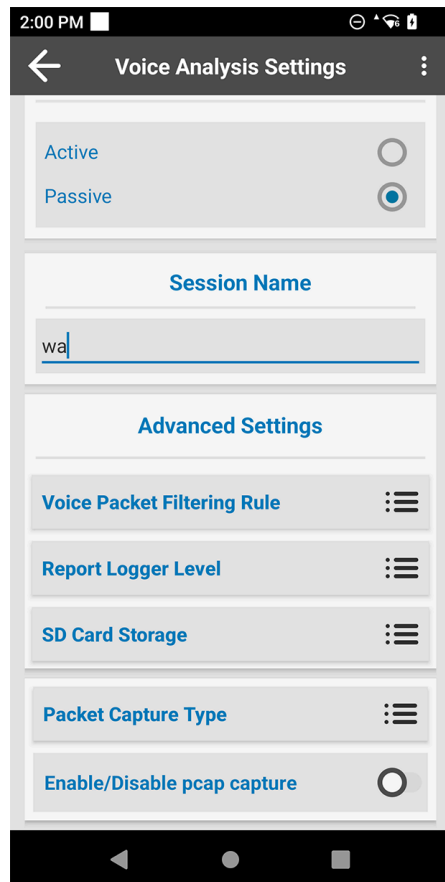
Figure 29 Voice Analysis Active Mode



In Passive mode of the Analysis, the Session Name and settings of the Advanced Settings are configured identically to the Roaming Analysis Settings of Passive mode, except for one unique Advanced Setting configuration named Voice Packet Filtering Rule.

Please follow Roaming Analysis Settings for handling settings which are identical.

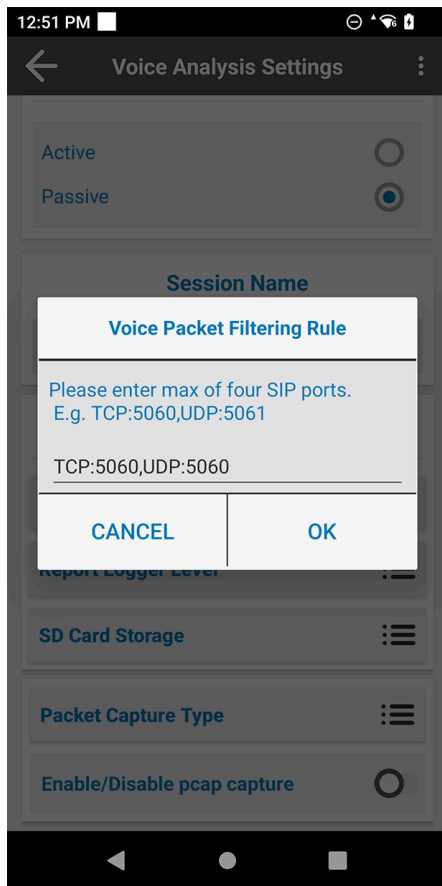
Figure 30 Voice Analysis Passive Mode



Voice Packet Filtering Rule

In the Passive mode of the Analysis, the feature measures application traffic of voice media ports (RTP), which is negotiated dynamically by the SIP signaling protocol. The Analysis is pre-configured to get that dynamic media information based on the default port deployment of SIP, which is 5060. However, it is possible that the SIP deployment is using a non-standard signaling port.

Ensure that this setting is configured to the SIP port of the deployment. Edit this field accordingly.

Figure 31 Voice Packet Filtering Rule

Advance Reports

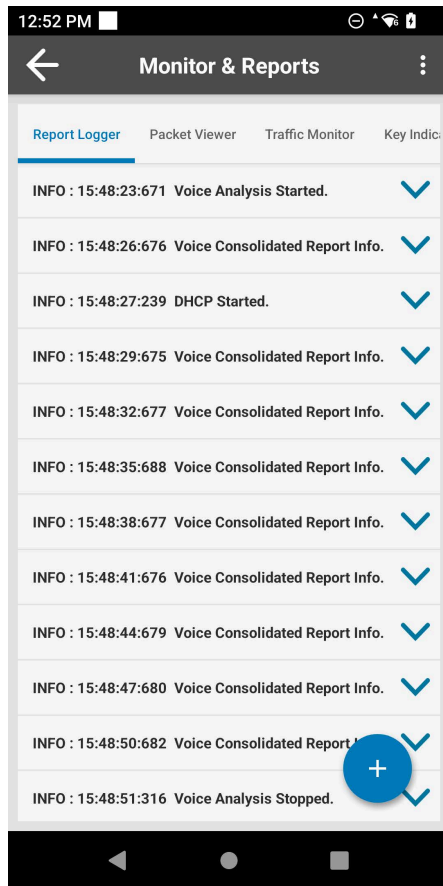
While Voice Analysis is running, session data displays in real-time. When Voice Analysis is not running, the most recent report displays.

To load a previous session while the live session runs in the background, or when Voice Analysis is not running, see **View Options** in Roaming Analysis.

View Options UI functionality of Voice Analysis is identical to View Options of Roaming Analysis.

Monitor and Reports

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

Figure 32 Monitor and Reports

- **Ping Accumulated Stats:** This view area presents data only in Active mode and remains empty in Passive mode. It displays ping indicators of synthetic traffic of the Analysis, accumulated in real-time during capturing session, or a final summary of a loaded session.
- **Report Logger:** Displays connectivity and Roaming Analysis results, as well as Voice traffic data. Tap a row to display detailed parameters and reasons of performance thresholds and issues. For more information, see [Report Logger Content](#).



NOTE: In Active mode, this view shows real-time live events, as well as **logging & saving the entire data**. As long as SD card storage is available (see SD Card Storage settings), the view allows for interactive UI operations over the saved data, such as scrolling up and down, pause/resume live events, toggling between the other views/tabs and re-entry to the saved data, jump to specific position in the log, and more. In Passive mode, the view allows for interactive UI operations only if the SD Card Storage settings are changed from the default (see SD Card Storage settings). If it remains in the default settings, the view shows only the real-time events as they happen, only while this specific tab is in the foreground, without possibility to interact with the data, as it is not saved.

The other tabs of the **Monitor & Reports** view; the **Packet Viewer**, **Traffic Monitor**, and the **Key Indicators**, present the same scope of data as the respective ones in the Roaming Analysis' Monitor & Report feature.

Networking Tools

To view available networking tools, tap  > **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.



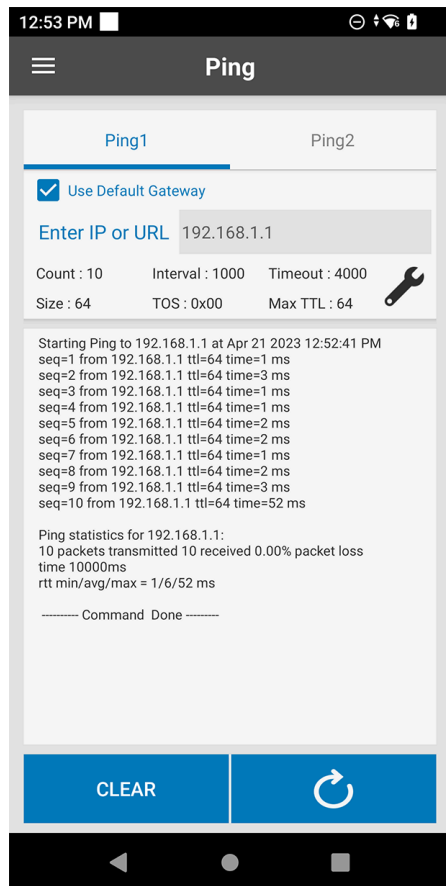
1. To use Ping, tap  > **Networking Tools** > **Ping**.
2. If connected to a Virtual Private Network (VPN), select **Use Default Gateway**.
3. To use a custom IP, URL, or FQDN, deselect **Use Default Gateway** and enter the IP, URL, or FQDN.
4. Tap .

Figure 33 Ping Screen



Ping Settings

Ping Settings provides options for configuring ping input settings.


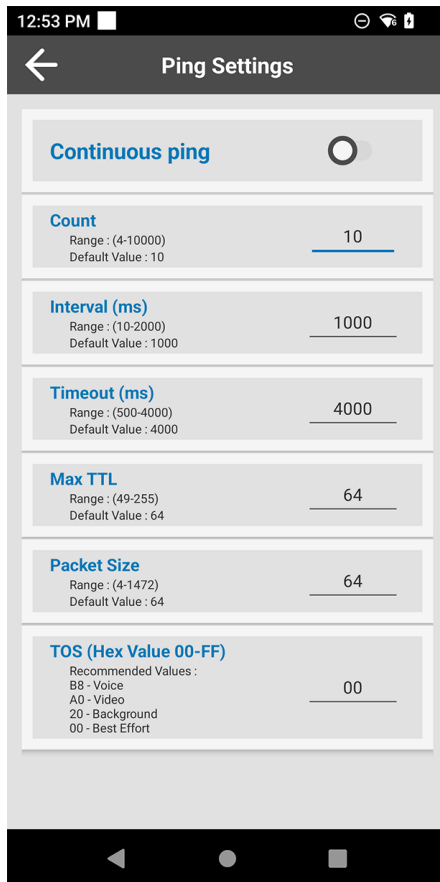
To configure ping input settings, tap .

Figure 34 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)
- **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:



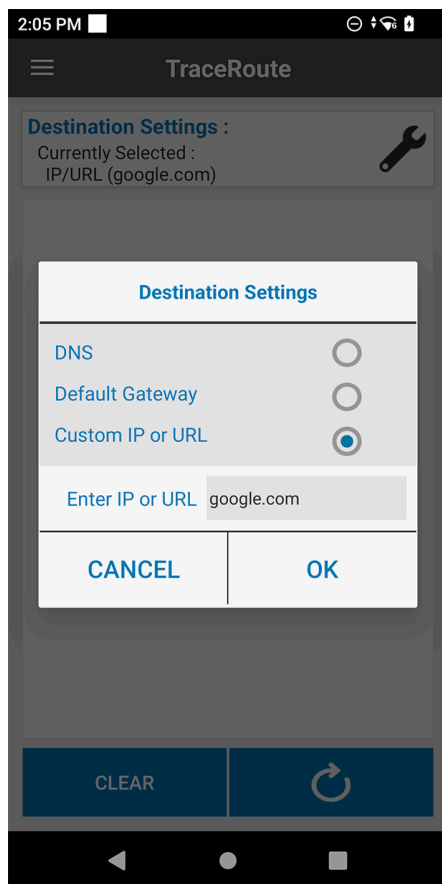
1. Tap  > **Networking Tools** > **TraceRoute**.
2. Tap . The **Destination Settings** dialog appears.
3. Select a Destination Type: **DNS**, **Default Gateway**, **Custom IP or URL**.
4. If setting a Custom IP or URL, tap the **Enter IP or URL** field and enter the IP or URL.

Figure 35 Destination Settings Dialog




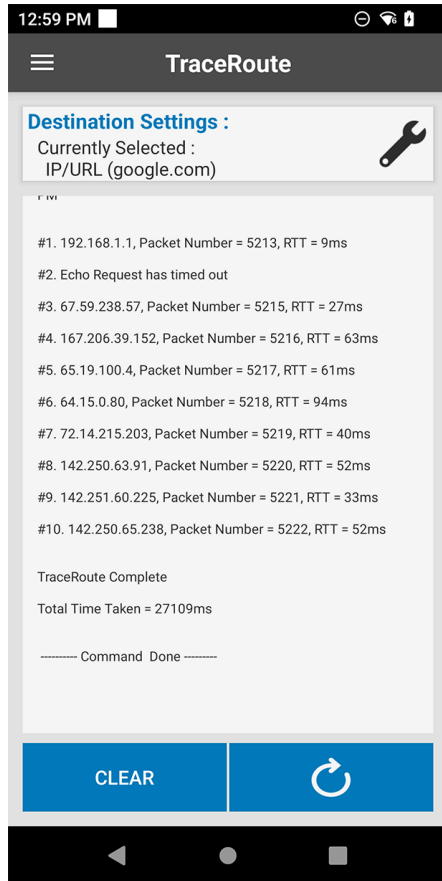
5. Tap **OK**.
6. Tap . TraceRoute runs using the currently selected destination.

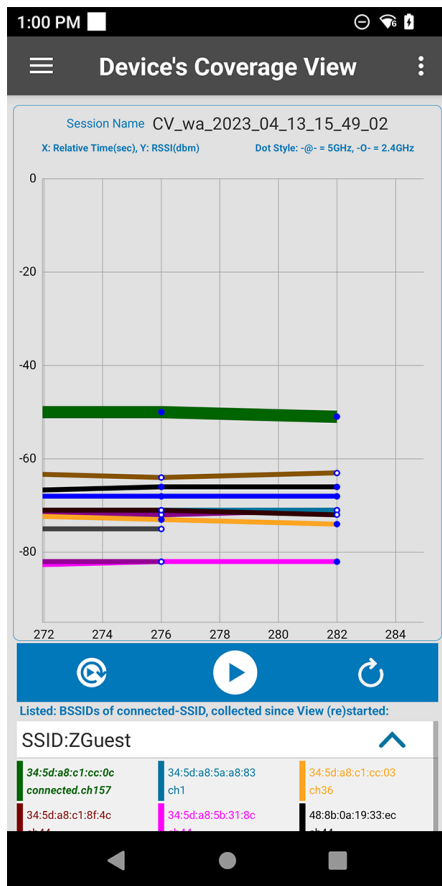
Figure 36 TraceRoute Screen



Device's Coverage View

Device's Coverage View displays the live and history of RSSI values (Y axis) of BSSIDs of the connected SSID over the relative time in seconds since the beginning of the capture (X axis), and depicts additional connectivity events in that timeline. If the device connects to a different SSID, or another Analyzer feature is accessed, Device's Coverage View resets.

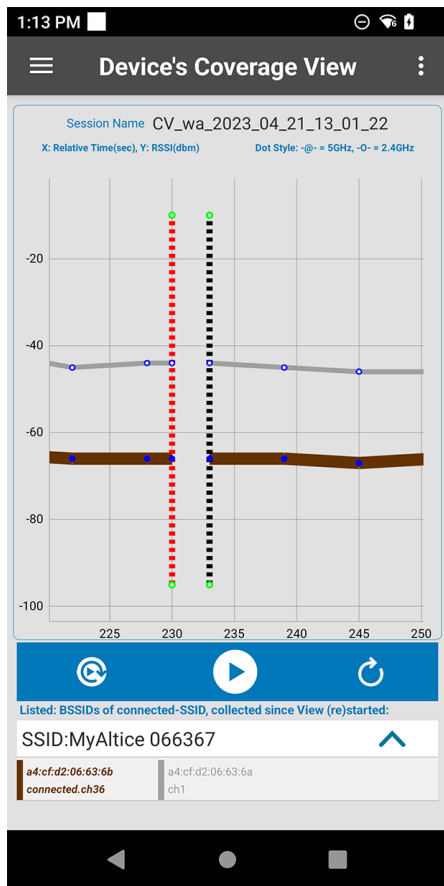
To display the **Device's Coverage View**, tap  > **Device's Coverage View**.

Figure 37 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 same BSSID colors also display as vertical bars on the **Scan List** screen.

Figure 38 Device's Coverage View Events



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

- **VIEW (RE)STARTED:** Purple vertical line = View started without a Connectivity or Roam event involved
- **ROAMED:** Green vertical line = AP hand-off event
- **DISCONN:** Red vertical line = Disconnection from SSID
- **NEW CONN:** Black vertical line = Connection to SSID

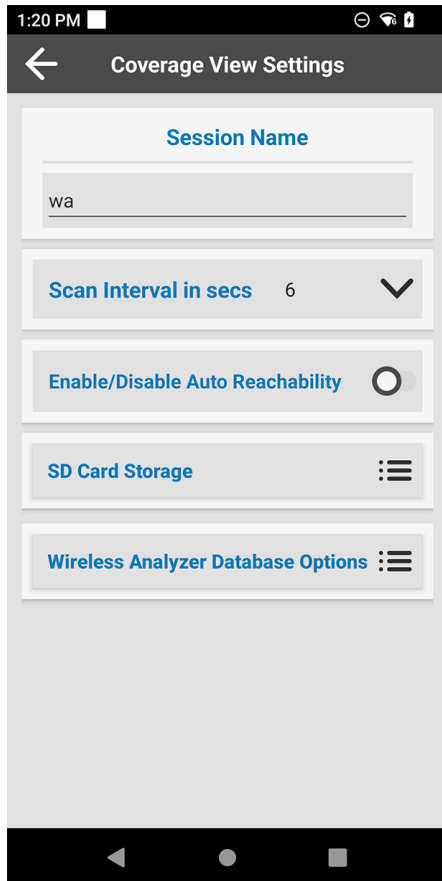
The grid view is interactive:

- Zoom in or Zoom out with two-finger pinching
- Pan with one finger in any direction to go backward and forward along the timeline
- Touch Scan samples (dots) or vertical events to expand the object with more related data

Coverage View Settings

Touch  and select the **Coverage View Settings**.

Figure 39 Coverage View Settings



- **Session Name:** Enter a custom session name. The final name is formatted with CV and appended with date and time. For example, CV_wa_2022 - 2 - 2_20 - 59 - 21.
- **Scan Interval:** Select to set the fixed interval between ongoing scans. Note that the interval options available in the drop-down box are not configurable, and they may vary in different device models.
- **Enable/Disable Auto Reachability:** use the **Auto Reachability Test** to have the feature 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.
- **SD Card Storage:** See **Roaming Analysis Settings > Advanced Settings** for description of this setting.
- **Wireless Analyzer Database Options:** See [Saved Data Options](#) for a description of this setting.

Logging

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


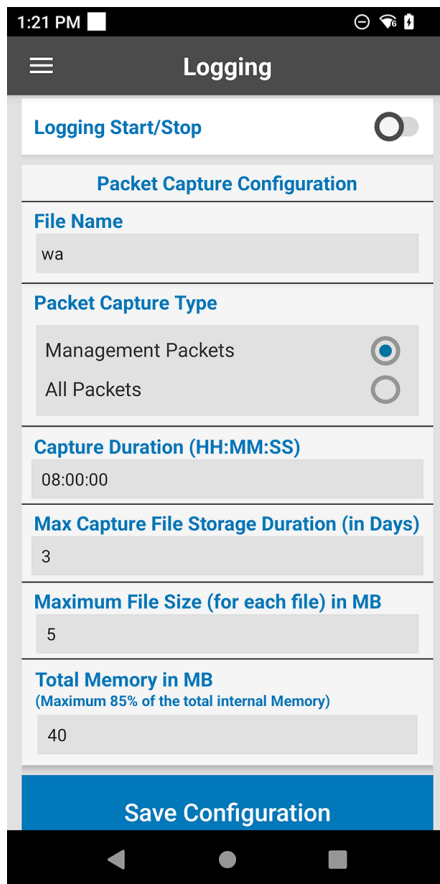
To display the **Logging** screen, tap  > **Logging**.

Figure 40 Logging Screen



The screenshot shows the 'Logging' screen on a mobile device. At the top, there's a status bar with the time '1:21 PM' and various icons. Below the status bar is a header with a menu icon and the title 'Logging'. The main content area has a toggle switch for 'Logging Start/Stop'. Below this is a section titled 'Packet Capture Configuration' which contains several settings: 'File Name' with the value 'wa', 'Packet Capture Type' with 'Management Packets' selected, 'Capture Duration (HH:MM:SS)' with the value '08:00:00', 'Max Capture File Storage Duration (in Days)' with the value '3', 'Maximum File Size (for each file) in MB' with the value '5', and 'Total Memory in MB' with the value '40'. At the bottom of the configuration section is a blue button labeled 'Save Configuration'.

- **Session Name:** Enter a custom session name. The name is appended with date and time. For example, wa_2022 - 2 - 2_20 - 59 - 21.
- **Packet Capture Type:** Select the category of Packet Types to be captured and stored in the sdcard. See Packet Capture for more details.
 - **Management Packets:** Select this option (default) to capture and save the device's transmitted and received 802.11 Mgmt, plus EAP/EAPOL, DHCP, ARP, ICMP, and DNS.
 - **All Packets:** Select this option to capture and save the Management Packets, as well as all the other device's transmitted and received 802.11-Data traffic. For example, all the device's operating system and applications transmitted & received IP-unicast traffic data, as well as all received IP-multicast/broadcast traffic



NOTE: The **All Packets** selection requires a pre-provisioned password. See [Configuration](#). In this setting, the stored packets are encrypted with the password in the sdcard.

- **Capture Duration:** Specify duration for the capture. The maximum and default is 8 hours.
- **Max Capture File Storage Duration (in days):** Specify the maximum number of days in which the storage will hold the captured file. After that, the files will be deleted. It can be set between minimum of 1 to maximum of 10 days. The default is 3.
- **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. The default is 5 MB.
- **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. The default is 40 MB.



NOTE: The Total Memory parameter can be configured to any value of up to 85% of the primary storage capacity.

- **Save Configuration:** Save the current configuration.



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

To Start the capture, toggle the switch next to **Logging Start/Stop** to the Start position.

To Stop the capture, toggle the switch next to **Logging Start/Stop** to the Stop position.

If the selected Packet Capture Type is **Management Packets**, when toggling to start, the capture will start per the settings.

If the selected Packet Capture Type is **All Packets**, when toggling to start, enter the pre-provisioned encryption password in the text box.

Advanced Configuration

Use the **Advanced Configuration** screen to view or edit Fusion Wi-Fi Stack parameters for Power Save Mode or Band Preference.

The purpose of interacting with power save and band preference configuration of the Wi-Fi in the Analyzer, is for rare cases of having to compare different values of those specific settings in same-device troubleshooting, and to collect Analysis data with the different values.

The default value is restored at the end of the troubleshooting. If the troubleshooting concludes that there is a reason to change the device configuration permanently, then that change happens with the officially incumbent device-management tools.

A password is required to edit the parameters. The Password needs to be pre-provisioned in the device. When attempting to Edit values, that Password needs to be entered. See [Configuration](#) for details.


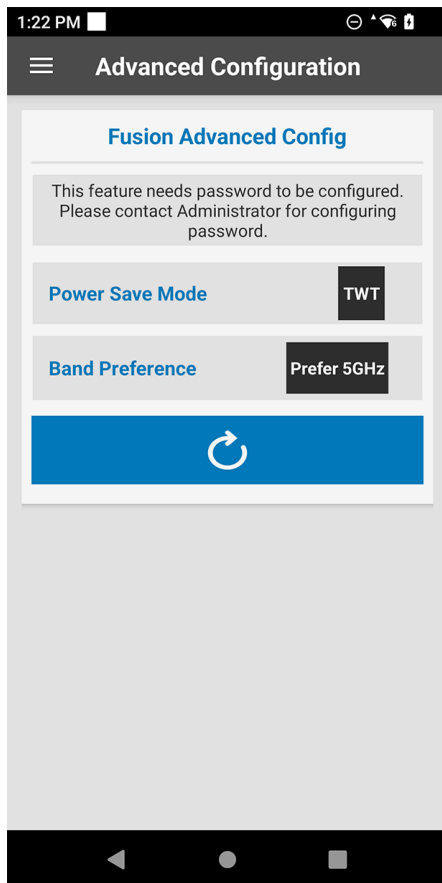
To display the **Advanced Configuration** screen, tap  > **Advanced Configuration**.

Figure 41 Advanced Configuration Screen



Appendix A: Configuration

Introduction

Zebra's Mobility Extensions (MX) allows configuration and certain features' actions of the Analyzer through device management and staging tools, with a compatible MX version that includes Wireless Analyzer manager package (formerly known as WorryFree Wi-Fi manager, or worryfreewifmgr).

Zebra's OEMConfig interfaces with Zebra's MX, thus capable tools using Android Managed Configurations framework can also access the Wireless Analyzer manager via the Zebra's OEMConfig.

For more information on using the Wireless Analyzer manager with MX, refer to: techdocs.zebra.com/mx/worryfreewifmgr/

Using the Configuration tool (powered by MS) for the Analyzer Application UI use cases is essential for features that require a password to be pre-provisioned in the device prior to the Analyzer respective feature operation. A password is required for:

- Packet Capture Type of **All Packets** mode, if set (non-default) inside **Roaming Analysis**, **Voice Analysis**, or **Logging** features.
- Editing values in **Advanced Configuration** feature

Using the Configuration tool is the only way to configure the password.

Apart from the Password configuration, the Analyzer Application UI is self-contained for all its operations and features settings, while Tools (powered by MX) can be used optionally for desired use cases of managing features in other ways than UI.

Using the Configuration tool for optional configuration and other Analyzer actions is essential in specific Wi-Fi troubleshooting cases such as:

- Admin's remote control of the device via the device management. For example, configure Settings of a feature, start it remotely to run in the background, then stop it remotely, and collect the saved data remotely.
- Admin's Local control of the device via local staging clients which can set MX configuration locally, such as Zebra's StageNow, when Analyzer UI happens to be inaccessible. For example, configure Settings of a feature with StageNow barcode, Start it with StageNow barcode to run in the background, then Stop it with StageNow barcode.

Please refer to techdocs.zebra.com/mx/worryfreewifmgr/ to find the full set of supported configuration and features actions.

Configuration of Password Using StageNow

This section provides instructions on how to use Zebra StageNow to provide a password for the Analyzer's required features noted in the [Introduction](#). As mentioned, that password can be provided with other MX compatible tools.

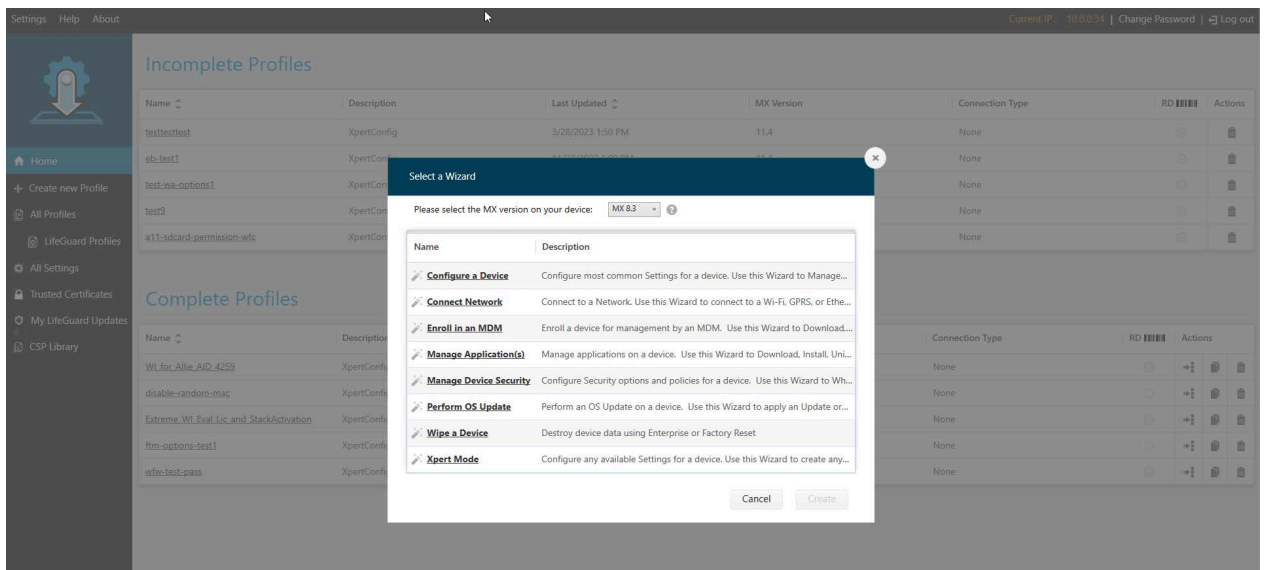
For more information on using StageNow, go to techdocs.zebra.com/stagenow.

Setting the Password

To provide a password for the Analyzer using StageNow:

1. Open the StageNow application on a host computer.
2. Select **Create New Profile** from the navigation bar on the left side.
3. In the **Select a Wizard** dialog, select an MX version that is less than or equal to the MX version supported by the target device.

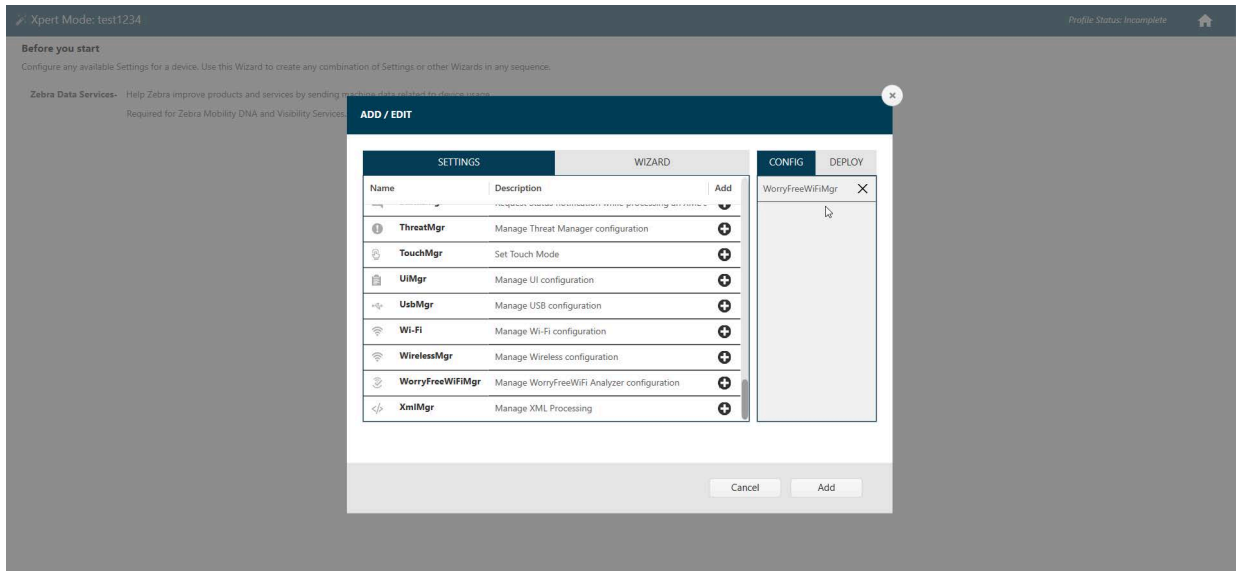
Figure 42 Select MX Version



4. Select **Xpert Mode**.
5. Select **Create**.
6. Enter a profile name in the **Enter Profile** name field.
7. Select **Start**. The **ADD/EDIT** dialog appears.

8. Scroll down and select **WorryFreeWiFMgr**.

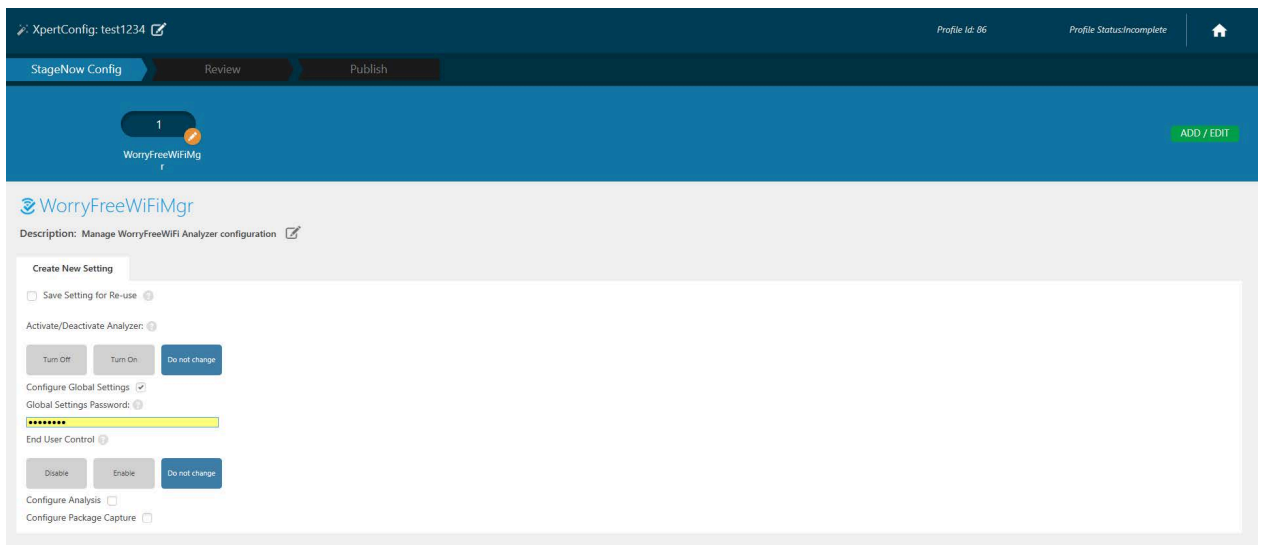
Figure 43 ADD/EDIT Dialog



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

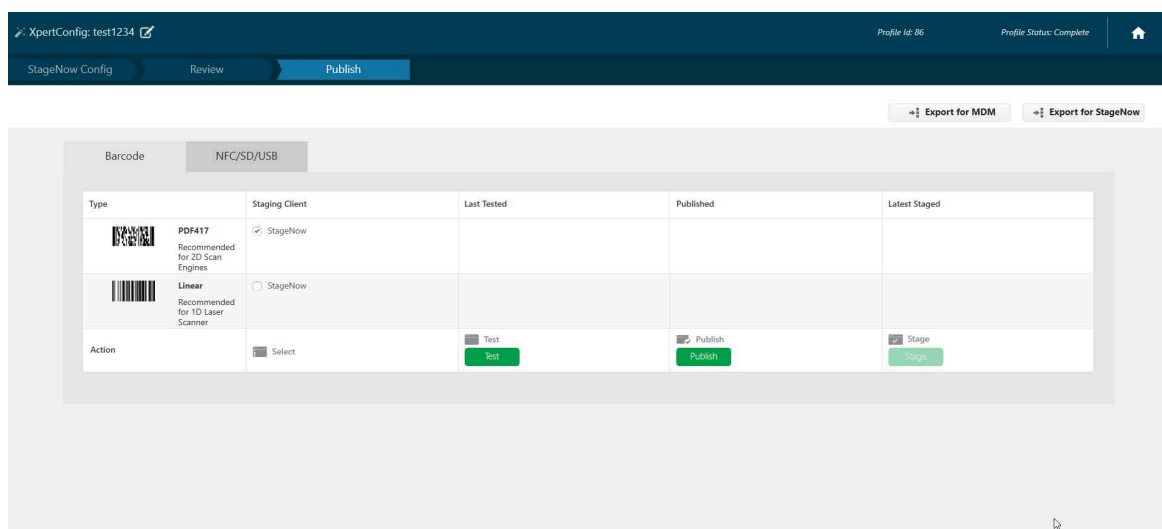
10. Select **Add**. The StageNow Config page appears.

Figure 44 StageNow Config



11. Select **Configure Global Settings** checkbox to enable it.
12. Enter a password in the **Global Settings Password** text field.
13. Select **Continue** and the **Review** tab appears.
14. Select **Complete Profiles** and the **Publish** tab appears.
15. In the Barcode tab, select the PDF417 option, choose another staging option such as NFC, or export the other file staging options (for example, XML or bin).

Figure 45 StageNow Config - Barcode Tab

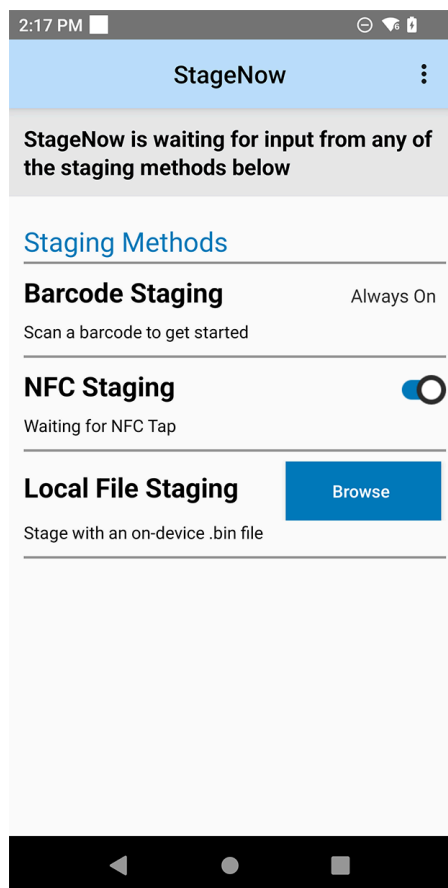


16. Select **Test** and StageNow generates a PDF file.
17. Open the PDF file which contains a StageNow barcode.

To set or reset the password in the device:

1. Open the StageNow app on the target device.

Figure 46 StageNow App



2. Use the target device to scan the StageNow barcode from the host computer.
3. After the **Stage Successful** dialog appears, select **Exit**.

Appendix B: Packet Capture

Introduction

Packet Capture automatically saves pcap files to local storage in the smu_pcap folder. When in All Packets mode, the pcap files are saved as password-protected ZIP files. Go to [Configuration](#) to set the password.

Use one of the following methods to enable Packet Capture:

- As part of the Roaming Analysis feature. See [Roam Analysis Settings](#).
- As part of the Voice Analysis feature. See [Voice Analysis Settings](#).
- As part of the Logging feature. See [Logging](#).

To view stored packets:

1. Ensure the previously mentioned features are stopped.
2. Collect the file(s) from the device, using any permitted access to the SD Card or sharing action, locally or remotely.
3. Unzip the files. If was captured in All Packets mode, then enter the same Analyzer password that was set when the pcap files were created when prompted.
4. Use packetizer PC tools such as Wireshark to analyze the pcap files.

Packet Capture Content

The packet capture feature saves incoming and outgoing traffic that is handled by the Wi-Fi stack in its 802.11-STATION role, a device that is connected (or attempting to connect) to a Network SSID profile.

- It includes Transmitted & Received Unicast traffic from/to the identity (MAC) of the 802.11-STATION. The traffic is captured inside the device, meaning the Transmitted traffic is captured before it is fully aired out to the AP. The Received traffic is captured after it is fully received successfully from the AP.
- It includes broadcast/multicast traffic sent from an AP to connected devices.
- It is 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 off-channels.
- It is always fully assembled in terms of 802.11: If different forms of Multiple Input Multiple Output (MIMO) and MSDU/MPDU Aggregation characteristics are applicable to WLAN over-the-air, it is not reflected in the capture.

- Traffic is not encrypted with respect to 802.11 and Wi-Fi Protected Access (WPA) encryption methods. For example, in the Transmit direction the traffic is captured before it is encrypted, and in the Receive direction it is captured after it is decrypted.

Supported Packet Types

The Analyzer can capture in two Packet Mode types:

- Management Packets: Includes the 802.11-STATION transmitted and received 802.11 Mgmt, plus EAP/EAPOL, DHCP, ARP, ICMP, and DNS.
- All Packets: Includes the Management Packets, plus all the other 802.11-STATION transmitted and received 802.11-Data traffic. For example, all the device's operating system and applications are transmitted and received Unicast traffic data, as well as all received IP-multicast/broadcast traffic.

As noted, the All Packets mode requires a password.

The exact 802.11 types and sub-types vary in different device models.

Supported Headers and Content

The Analyzer supports headers and content within the supported types and sub-types:

- Radiotap Header: The exact Radiotap header fields that have been captured vary in different device models.
- 802.11 Headers/Sub-Headers: The exact 802.11 header fields that have been captured vary in different device models.
- 802.11 Payload (all levels above the MAC level, also know as 802.11-Data type): Entire payload in an unencrypted format: w.r.t. WLAN-encryption.

Appendix C: Report Logger

Introduction

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

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

To view Voice Analysis reports, tap  > **Voice Analysis** > **Monitors & Reports** > **Report Logger**.

Content Format

Each item (event) in the Report Logger tab is structured in the following format:

- A one-line header with parameters; always viewable, depicting the main parameters of the event.
- If the item's view is touched and expanded: additional lines with parameters are shown for the same event.



NOTE: The verbiage of the additional parameters (expanded view) depends on multiple dynamic factors at the time of the event. Even for multiple events of same type, it does not necessarily mean that they will all include the same verbiage.

Header - Event Types

The header shows the severity class (INFO, WARNING, ERROR) of the event, the time that it occurred, and a short header string (event type).

Roaming and Voice Analysis Headers

Table 2 INFO Severity Class Headers

AUTH Started	AUTH Completed
ASSOC Started	ASSOC Completed
EAPOL STARTED	EAPOL Completed
DHCP Started	DHCP Completed

Table 2 INFO Severity Class Headers (Continued)

ARP Started	ARP Completed
Connection Started	Connection Completed
Roam Started	Roam Completed
Reassoc Started	Reassoc Completed
Scan Started	Scan Completed
Roam Analysis Started	Roam Analysis Stopped
Voice Consolidated Report	Voice Consolidated Report* (optional last-report at the end of the call)
Voice Analysis Started	Voice Analysis Stopped
Disconnect Suppression Triggered	Disconnect Suppression Completed
EAP Started	EAP Completed
SIP Call Started	SIP Call Stopped
SIP Call Media Paused	SIP Call Resumed
SIP Call Failed	SIP Call Restarted
Call summary report of RTP(RX) Stream	

Table 3 WARNING or ERROR Severity Class Headers

Connection Failed
Roam Failed. Retrying
Authentication Failed
Association Failed
EAPOL Failed
DHCP Failed
ARP Failed
Disconnected
Voice Consolidated Report
Deauth Seen
Disassoc Seen
EAP Failed
RTP measurements stopped for this SIP period
Voice Consolidated Report*

Table 3 WARNING or ERROR Severity Class Headers (Continued)

Voice Analysis Internal Limitation
Reassoc Failed

Voice Analysis Only Headers

Table 4 INFO or WARNING Severity Class Headers

Voice Consolidated Report	Voice Consolidated Report* (optional last-report at the end of the call)
Voice Analysis Started	Voice Analysis Stopped
SIP Call Started	SIP Call Stopped
SIP Call Media Paused	SIP Call Resumed
SIP Call Resumed	SIP Call Failed
SIP Call Restarted	Call summary report of RTP(RX) Stream
RTP measurements stopped for this SIP period	Voice Analysis Internal Limitation

Additional Parameters (when line item is expanded)

Roaming and Voice Analysis Reasons

Standard IEEE 802.11 Reason Codes for De-Authentication Packets: When the device receives a de-authentication packet from the AP, the analyzed strings may include an IEEE 802.11 standard Reason code. The reason code is retrieved directly from the 802.11 packet. 802.11 De-authentication Reason Codes have values in the range of 0 to 99.

Standard IEEE 802.11 Result Code for Authentication Response Packets: When the device receives an authentication response packet from the AP, the analyzed strings may include an IEEE 802.11 standard Result Code. The Result Code is retrieved directly from the 802.11 packet. The Result Code value is in the expanded view. 802.11 authentication Result Codes have values in the range of 250 to 255.

Standard IEEE 802.11 Status Codes for Association Packets: When the device receives association response packet from the AP, the analyzed strings may include an IEEE 802.11 standard Status Code. The status code is retrieved directly from the 802.11 packet. The status code value is in the expanded view. 802.11 Status Codes have values in the range of 0 to 107.

Analyzed Reasons for MAC Authentication and Association-related Events

- Unknown. Auth status code received is 255. Authentication has Timed out
- Association has Timed out
- Association not started
- Connection already completed
- Disconnect Reason - Deauth Packet from AP

- Deauth Packet from AP, Disconnect suppression may have triggered
- Deauth Packet sent from Device
- Disassoc Packet from AP, Disconnect suppression may have triggered
- Disassoc Packet sent from Device, Device is leaving BSS
- Disassoc Packet from AP, Disconnect suppression may have triggered
- Disconnect Reason - Disassoc Packet from AP

Analyzed Reasons for WLAN Security-related Events

- Analysis could not start due to EAPOL Analysis Failed
- Keynonce of eapol1 and eapol3 not equal
- ReplayCounter of eapol1 not equal to eapol2 or eapol3 is not equal to (eapol1 + 1)
- EAPOL four way handshake timeout
- Analysis is been done on an Open/WEP Profile. Hence EAPOL is not applicable
- EAPOL Key 1 not started
- EAPOL Key 2 not sent
- EAPOL Key 3 not received
- EAPOL Key 4 not sent
- EAP Identity Request not received
- EAP Identity Response not sent
- EAP Method mismatch
- EAP TLS Version mismatch
- EAP Failed
- Analysis is not being done on 802.1x profile, therefore EAP not applicable
- EAP exchange did not start
- EAP Method Request not received
- EAP Client Hello Timeout
- EAP Server Hello Timeout
- EAP Timeout
- Key Rotation due to Session Timeout Failed

Analyzed Reasons for DHCP Events

- Analysis could not start due to DHCP Analysis Failed
- DHCP_INVALID
- DHCP_NAK
- Device failed to start discover after NAK
- DHCP_INFORM

- NO DHCP server(s) found
- DHCP server didn't respond to the request
- Device failed to start discover after NAK
- DHCP not started
- DHCP Request not started

Analyzed Reasons for Reachability Events

- Analysis could not start due to ARP Analysis Failed
- WiFi is turned 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%
- Unable to reach gateway through arp
- Gateway IP is not available to test arp reachability
- ARP not started
- Ping test not started
- Host Could not be resolved
- Destination IP address is not valid
- Echo Request has timedout
- IP address not Reachable
- Ping Stopped due to disconnection
- Destination network unreachable
- Destination host unreachable
- Destination protocol unreachable
- Destination port unreachable
- Fragmentation required, and DF flag set
- Source route failed
- Destination network unknown
- Destination host unknown
- Source host isolated
- Network administratively prohibited
- Host administratively prohibited
- Network unreachable for ToS
- Host unreachable for ToS
- Communication administratively prohibited

- Host Precedence Violation
- Precedence cutoff in effect
- TTL expired in transit
- Fragment reassembly time exceeded
- Packets lost during ping

Analyzed Reasons for RF and Coverage-related Events

- Low Signal Strength
- Packet Loss during Low Signal Strength
- High Interference
- Packet Loss during High Interference
- High Channel Load
- Packet Loss during High Channel Load
- Poor Coverage Area
- Packet Loss in Poor Coverage Area
- Consecutive packet Loss
- Packet Loss Exceeded
- Packet Loss
- 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
- Tx Power and Data Rate Mismatch
- 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
- Disconnect Reason - Out of Coverage Area
- Disconnect Reason - Abrupt AP Loss

Other Miscellaneous Reasons

- Timeout happened between substate machines. 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
- AP of selected SSID to analyze is not in vicinity
- Wi-Fi is not the active network
- Undefined Error
- Auth Started
- Device storage space reached 90%
- Disconnect Reason - Wi-Fi Disabled
- Disconnect Reason - Profile Roam from Admin or User
- Disconnect Reason - Disconnect initiated by AP
- Analysis Timed Out

Voice Analysis Only Reasons

- 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 (in case of active analysis of synthetic voice traffic) or larger than 50ms (in case of passive analysis of SIP application traffic)

Inside the previously mentioned sub-headers, each of them may contain an additional Analyzed Reason string.

- Low Signal Strength
- High Interference
- High Channel Load
- Poor Coverage Area
- Packet Loss
- Tx Power and Data Rate Mismatch
- 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

