KEYW Engineering
BUSHIDO

09 APR 2015

BUSHIDO is a handheld, Wi-Fi direction finding solution capable of detecting and measuring the signal strength of any 802.11a/b/g/n device in both the 2.4 GHz and 5 GHz bands. This handheld receiver builds on the previous generations of related handheld receivers with over one thousand devices in service worldwide. The unit has been designed with a rugged, sealed, water-resistant composite housing for better performance and survivability.

Capabilities:

- Close-range **direction finding** tool using received signal strength indication (RSSI) bar graph and numerical value (dBm) with 90 dB of dynamic range.
- **Traffic generation** techniques may be selected to assist in direction finding.
- **Access Point Scan mode** scans all channels and displays Access Points (AP) without transmitting data – (Includes AD-HOC and hidden APs)
- **MAC Monitor mode** displays devices on a selectable channel or associated with a selectable AP (including AD-HOC and hidden APs)
- Device details including associated AP MAC/SSID, type, vendor, group cipher, pair cipher and authentication
- Expanded channel range covers unique European and Japanese standards
- Devices can be added to a **Watch list** using the handheld GUI or transferred as a file via USB.
- Packets can be collected in the industry standard **PCAP** file format for later upload to a PC and analyzed using tools such as Wireshark.
- **15 Gigabytes** of internal storage for PCAP files accessible via USB mass storage
- Audible feed back during direction finding. Audio tone based on the measured signal strength of the target device, increasing frequency as signal strength increases
- Audio is available using wired earphone or internal speaker.
- Vibration alert for indication of Watchlist list hit.
- Adjustable date/time – keeps time when powered off
- Selectable internal antenna or external antenna (SMA)
- Selectable backlight levels (off, low, mid or high)
- Sunlight readable and NVG compatible, trans-reflective LCD.
- Water resistant, glass reinforced polycarbonate housing with a sturdy lanyard point, recessed connections for Audio, USB and External Antenna with tethered caps.
- External power from a USB connection provides power and charges the internal battery.
- Internal rechargeable battery with battery level indicator
  - >6 hours of operation LCD backlight on, >7 hours backlight off.

KEYW Engineering
7740 Milestone Parkway, Hanover, MD, 21076
443-270-5295 www.keywcorp.com

For additional information, please contact:
EIGProducts@keywcorp.com

KEYW Engineering
BUSHIDO

09 APR 2015

Accessories include:

- RF cable for external antenna
- Universal AC wall power adapter
- 12/24VDC automotive power adapter
- USB cable for transferring files
- Wired ear bud headset (Motorola cell phone style)
- 2.5mm to 3.5mm adapter (for use with standard audio headphones)
- Adjustable Lanyard
- Pelican 1200 case with custom fitted foam insert

These materials are controlled by the International Traffic in Arms Regulations, 22 C.F.R. Parts 120 - 130, and require an export license from the U. S. Department of State prior to transfer to a foreign person or foreign destination. If these materials are exported or otherwise retransferred without the necessary license(s) or in violation of the terms or conditions of any export license, recipient shall indemnify and hold harmless KEYW, its employees and parents, its and their successors and assigns, from and against any and all liability or harms, including attorney fees, arising therefrom.

BUSHIDO Kit Price $8,000

(KEYW PN 200520-001)

KEYW Engineering
7740 Milestone Parkway, Hanover, MD, 21076
443-270-5295 www.keywcorp.com

For additional information, please contact:
EIGProducts@keywcorp.com

THE KEYW CORPORATION

BUSHIDO

User Guide

9/30/2015

BUSHIDO USER GUIDE (v2.1)

WELCOME

BUSHIDO is a handheld, Wi-Fi direction finding (DF) solution capable of detecting and measuring the signal strength of any 802.11 (a, g, and n) device in both the 2.4 GHz and 5 GHz bands. This handheld receiver builds on the previous generations of related handheld receivers with over one thousand devices in service worldwide. The unit has been designed with a rugged, sealed, water-resistant composite housing for better performance and survivability.

While scanning for networks and stations, BUSHIDO is a passive device that is virtually undetectable. When forcing a station to generate traffic for enhanced Direction Finding, the BUSHIDO maintains its stealth presence by spoofing the MAC address of the station's associated access point (AP). Several methods of generating traffic are implemented to minimize the signature of the device while performing its mission.

BUSHIDO USER GUIDE (v2.1)

Table of Contents

BUSHIDO USER GUIDE (v2.1)

BUSHIDO USER GUIDE (v2.1)

Revision History

12/15/2011 Initial Release for Software Version 1.0.0

3/27/2012 Beta test release t1.1.0 with the following features:

- DF from the Watchlist screen – allows navigation to DF screen without having to acquire packets first from the AP or MAC monitor screens.
- Auto-Hunt mode – From the DF Options screen, the user can enable or disable Hunt mode. If enabled, BUSHIDO will scan for APs and listen on each AP's channel until it finds the target. While in Hunt mode, "Hunting" will appear on the DF screen and the channels will change indicating the search pattern.
- Manual Hunt mode – if Auto-Hunt mode is disabled, the user can press the left/right buttons on the DF screen to manually change channels and search for the target.
- Stimulation (STIM) improvements – TIM has been improved to work with more devices.
- DF sensitivity –averaging and peak trimming has been added to improve direction finding.

9/12/2012 Release 1.1.0

- All the features in the above Beta release t1.1.0
- New STIM feature - rotates through RTS/CTS, TIM, TPC and ARPing at a configurable cycle (10, 25, 50, and 100 milliseconds)
- AP Scan and MAC Monitor aging - on/off with clear history
- Key repeat and paging
- Activity logging available through USB Mass Storage – logs watch list hits, etc.
- PCAP logging on/off in DF menu.
- Internal SD card verification - during boot and USB Mass Storage ejection/removal

1/8/2013 Release 1.1.1

- Customer request to improve editing new Watch list entry by automatically deleting the zeros.

9/30/2013 Added ITAR Restriction Information

12/19/14 Release 1.1.5

- Minor bug fixes
- Updated OUI table

6/30/2015 Release 2.0.0

- Remote Control via Bluetooth (aka Wi-Fi Remote Control - WRC)
- Friendly and Target Watch List Categories
- MAC and SSID Watch Lists
- Survey of APs, or APs and Stations
- Channel Map
- STIM Method Options
- Extended Color Coding by Station Type
- Updated Status Bar to Show Selected Channel
- Additional features only available with the WRC Android app

9/30/2015 Release 2.1

- Added Unassociated STIM method
- Improved performance
- Fixed bugs

Definition of Terms

AP – Access Point

CTS – Clear To Send

DF – Direction Finding

MAC – Media Access Control

OUI – Organizationally Unique Identifier

PCAP – Packet Capture

SD Card – Secure Digital Memory Card

Spoof – To impersonate or take on the identity of another Wi-Fi enabled device

SSID – Service Set Identifier

Station – A wireless device such as smartphone, laptop, etc.

STIM – Stimulate target by generating traffic to the target.

TIM – Traffic Indication Map

TPC – Transmit Power Control

RSSI – Received Signal Strength Indicator

RTS – Request To Send

Watch List (WL) – List of target and friendly names with MAC addresses and/or SSIDs

WDS – Wireless Distribution System

WRC – Wi-Fi Remote Control

BUSHIDO USER GUIDE (v2.1)

Get Started

Navigation and Controls

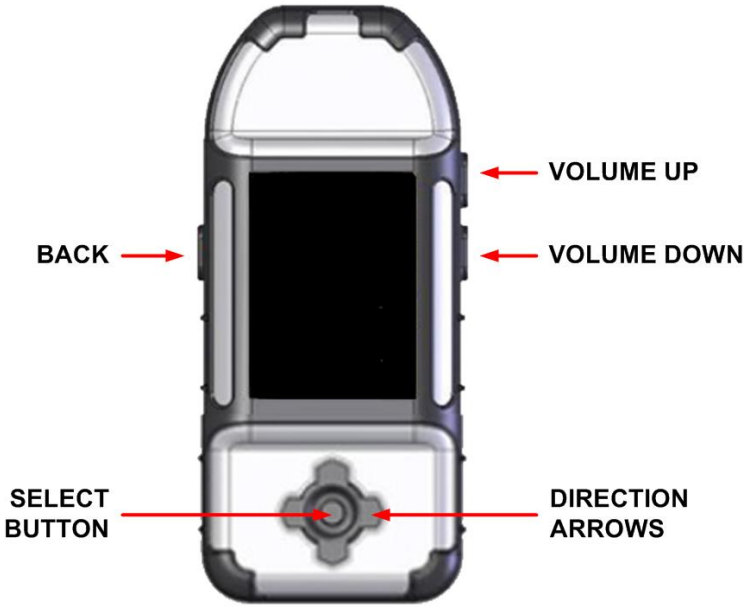


Figure 1

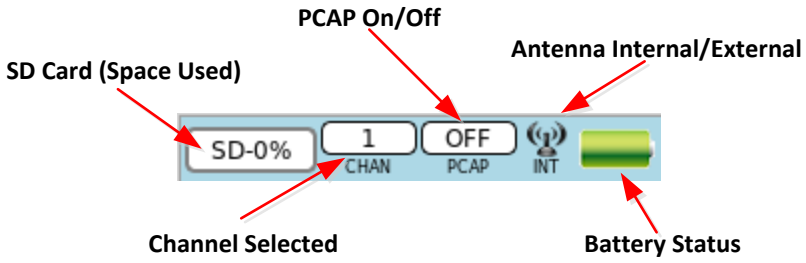
Volume – Controls (UP and DOWN) are on the right side as shown in Figure 1.

BACK Button – In addition to turning the device on and off, pressing the BACK button will return back to any previous menu.

Navigator – The surrounding arrows move the selector up, down, left, and right. The center (SELECT) button selects the option.

Note: holding down the SELECT button while pressing the UP or DOWN button will page through screens.

Main Screen Icons



BUSHIDO USER GUIDE (v2.1)

Turning the Device ON and OFF

Locate the BACK button on the left side of the device as shown in Figure 2.

Figure 2

Press the BACK button to turn the device ON. The device will display the logo as it boots up.

There are several ways to power the device OFF.

- From any screen, press and hold the BACK button until a 4-second countdown is displayed. Continue holding the BACK button until the countdown is finished, or release the BACK button and then press the SELECT button in the center to immediately confirm the shutdown (Figure 3). To cancel the shutdown, release the BACK button before the countdown is complete. The device will display Figure 4 when shutting down.

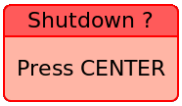


Figure 3

- If the unit is non-responsive a hard shutdown may be performed by holding the BACK button until the unit turns off (approx. 15-seconds).

Figure 4

Charging the Device

Plug the supplied charging adapter into the charging port (Figure 5).

If the BUSHIDO is powered on, the battery icon  will display a charging icon at the top of the screen if the device is charging properly.

The unit ships with an AC wall adapter and a DC car charger.

The expected battery life for normal usage is 4-6 hours.

Figure 5

External Audio Jack

A standard set of headphones are included in the kit.

Note: Any Motorola cell phone headset can be used.

Note: A 2.5mm to 3.5mm plug adapter is also included in the kit to allow any stereo headset to be used with the device.

Figure 6

Internal Antenna

The internal antenna is located at the top of the unit as shown in Figure 7.

The internal antenna is a pair of omni-directional antennas.

Note: Be sure to not have the tip of the device obstructed when in use (i.e. do not have your hand over the end of the device). Notice Figure 30 for proper way to hold the BUSHIDO for optimal performance.

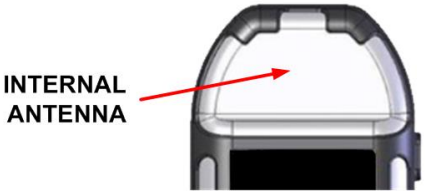


Figure 7

Locating the Serial Number

The unit serial number is etched into the back at the top of the device as shown in Figure 8.

The serial number can also be found at the bottom of the Settings menu.

Figure 8

External Antenna Connector

Attach optional SMA terminated antenna to the external connector supplied. The Wi-Fi HANDHELD ANTENNA: KEYW P/N: 201050-001 is recommended.

Note: This external connector is for the use of an optional external antenna. This connector is a normal polarity SMA. Many WLAN antennas use a reverse polarity SMA connector that will require an adapter to use with BUSHIDO. Use care when selecting and attaching an external antenna to this port.

Figure 9

Note: The external antenna will need to be activated on the Main Settings menu before the antenna has been attached.

To enable the external antenna, navigate to Settings from the main menu. Scroll down to External Antenna and press the SELECT button.

If the check box to the left of "External Antenna" is clear that means the external antenna port is NOT enabled (enabling the internal antenna).

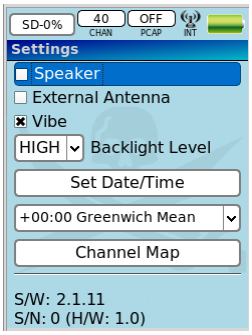


Figure 10

Accessing Internal Drives

If connected properly to a computer, the BUSHIDO will show up as two removable drives named “Bus-####” (where #### is the unit serial number) and “BUSHIDO”.

“Bus-####”: This drive contains two directories:

1. UpgradePackages – Used for field upgrades (see page 24).
2. Watchlists – Used to manually manage the watchlist file (watchlist.csv). Only one watchlist file is allowed in this directory. The watchlist file contains an explanation of the file format and includes examples.

“BUSHIDO”: This drive is the internal non-removable SD Card. Actual size of the internal SD Card depends on the BUSHIDO’s production date. Newer BUSHIDO units contain 32GB SD Cards (28GB available to operator). This drive contains two directories:

1. Pcaps – Contains standard PCAP files. The operator can delete/remove PCAP files when no longer needed. PCAP files will be split if they exceed 50MB.
2. MacCaps – Contains files recorded by the MAC Capture feature. This feature is accessible only via the WRC app. The operator can delete/remove MAC Capture files when no longer needed.

Note: Always “Remove Safely” both drives of the BUSHIDO properly before disconnecting the USB cable.

Using the BUSHIDO

Main Menu

When the BUSHIDO is first powered on, the top level Main Menu screen is shown (Figure 11). The operator can select any menu item by pressing the SELECT button.

Additional screens are displayed by selecting Survey, MAC Monitor, Watch List, and Settings menu items. Each screen is described in the following sections.

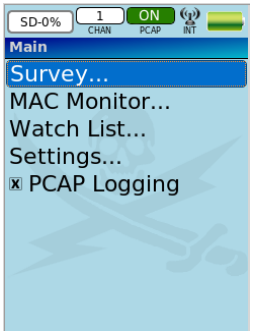


Figure 11

The data presented on the Survey and MAC Monitor screens have the following color definitions (Figure 12).

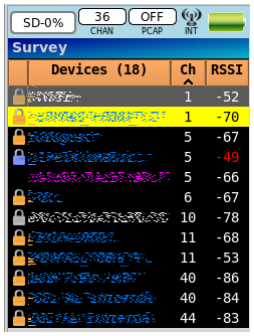


Figure 12

Text:

Green	Station with known associated AP
Blue	AP
Purple	Ad-hoc device
Orange	WDS device
White	Station with unknown associated AP
Red	RSSI value stronger than -50 dBm

Background:

Gray	Currently selected device
Yellow	Watch list target, yellow text if selected

Survey

Survey will perform a scan of all 802.11 APs, Ad-hocs, and Stations within range displaying SSID, Channel, and RSSI (Figure 13). To select whether or not Stations are displayed, press the SELECT button. A Select menu will be displayed (Figure 14). Check or uncheck the "AP/Adhoc Only" box to select what to display. The Select menu items are described further starting on page 18.

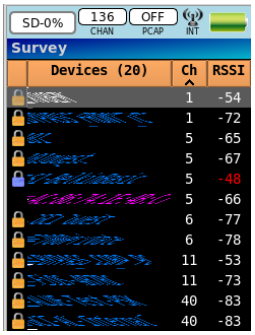


Figure 13

The current channel being scanned is shown at the top of the screen.

Note: Instead of transmitting probes, the BUSHIDO listens for APs/Ad-hocs/Stations making it invisible to the network.

The column sorting is changed by pressing the LEFT or RIGHT buttons. The current column being sorted will display a "^" symbol.

The security icons in the first column are:

- Encrypted WEP – Blue Lock
- Encrypted not WEP – Gold Lock
- Encrypted/Hidden – Gold Lock with 'H'
- Unknown – Grey Lock
- Hidden – 'H'
- Clear (no encryption) – No Icon

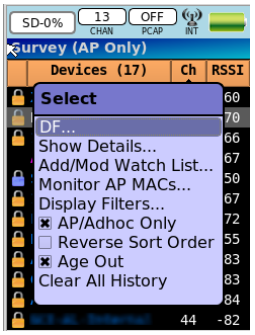


Figure 14

MAC Monitor

MAC Monitor will display all APs and Stations within range on a given channel displaying the Device name, RSSI, and Seconds since the last detected packet (Figure 15). The Device name will be the SSID for APs and Ad-hocs, if known, or the MAC address for Stations. If the device is in the Watch List (described on page 15), the Device name will be the operator assigned Alias.

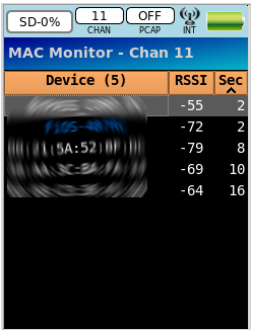


Figure 15

The current channel is shown at the top of the screen.

The column sorting is changed by pressing the LEFT or RIGHT buttons. The current column being sorted will display a "^" symbol.

Choose a device and press the Select button to be presented with a Select menu (Figure 16). The Select menu items are described starting on page 18.

Figure 16

Watch List

Watch List will display all saved WL entries on this device (Figure 17). Friendly entries are shown in white text. Target entries are shown in black text. The time since last WL hit is shown in the 's' (seconds) column. Friendly entries always have a hit time of '999'. Entries are only sorted by hit time, most recent first. Under the MAC/SSID column, MAC entries will show the MAC address and SSID entries will show the SSID.

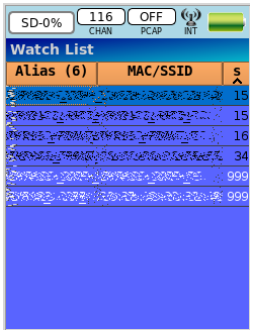


Figure 17

Figure 19

From the Watch List Select menu (press SELECT button – Figure 18):

- DF target: Navigates directly to DF screen. SSID WL entries cannot be DF'd (option grayed out).
- Add Target: Manually add target. Adds an empty MAC entry that can be edited using Edit Alias, Edit MAC, and Edit Type.
- Edit Alias: Allows user to add an easily identifiable name (Figure 19).
- Edit MAC: Allows user to edit the MAC address (Figure 20). SSID WL entries cannot have the MAC address edited (option grayed out).
- Edit Type: Allows the user to edit the Target or Friendly type (Figure 21). The MAC and SSID options can only be changed when adding an AP from either the Survey or MAC Monitor screens.
- Delete: Remove the selected WL entry.
  - ➢ Warning: there is no confirmation when deleting an entry.

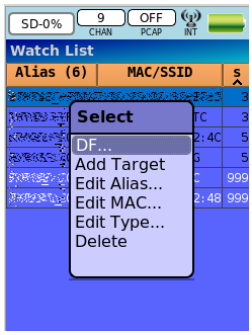


Figure 18

Figure 20

Figure 21

Watch List entries may be added via file transfer using the supplied USB cable and a computer. Navigate to the **WatchLists** folder and open the file **watchlist.csv** in a text editor. The format of each file entry is:

alias, type, address, category

alias – a descriptive name
type – the WL type ("mac" or "ssid")
address – if the type is "mac", this is the MAC address. If the type is "ssid", this is the SSID.
category – the category of the entry. 0 is target, 1 is friendly.

Example WL entries are included in the file and following. Note that SSIDs can contain non-printable characters. These are specified by an escape sequence of the form \xx, where the xx represents the hex value of the non-printable character. As an example, \62 is the letter 'b'. To include a backslash in an SSID, use \\. To include a comma in an SSID, use \2c.

TARGET-XX,mac,38:e7:d8:12:34:56,0
FRIENDLY_GUY,ssid,\00\00xyz,1

When/if a target in the Watch List is detected the BUSHIDO will give a chime and a vibe to the operator.

*NOTE: The Watch List can hold a maximum of **100** targets.*

Settings

Settings window will allow the operator to set multiple custom configuration settings.

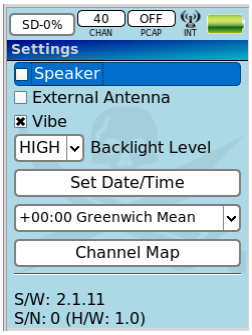


Figure 22

Note: X in the check box is Enabled

Speaker: Enable/Disable internal speaker.

External Antenna: Enable/Disable External Antenna. The antenna icon at the top of the screen will display “INT” or “EXT” to indicate the setting.

Vibe: Enable/Disable internal Vibe indicator.

Backlight Level: Choose from OFF, LOW, MID, and HIGH.

Set Date/Time: Date and time are saved on the BUSHIDO and will not need to be reset unless the battery is completely drained.

Time Zone: Select correct time zone.

Channel Map: Select the channels to be scanned (Figure 23).

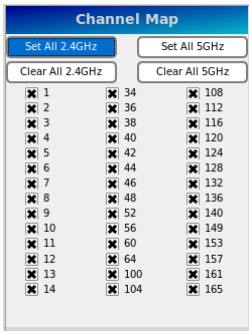


Figure 23

Versions: Software Version, Serial Number, and Hardware Version.

PCAP Logging

PCAP Logging will save all recorded traffic to an industry standard PCAP file format. Each time this option gets enabled (Figure 24), the “PCAP” icon at the top of the screen will turn green and display “ON” in the center. A new PCAP file is saved with a timestamp in its file name.

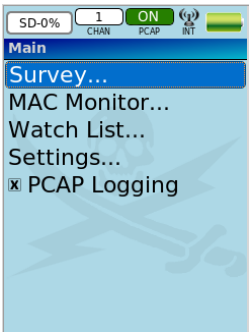


Figure 24

The PCAP file(s) are accessed by plugging the BUSHIDO into a computer via the supplied USB cable.

The BUSHIDO will appear as a USB drive labeled “BUSHIDO”. Navigate to the ‘Pcaps’ folder and copy the file(s) to the attached computer for further processing. Note that PCAP files cannot be created while the BUSHIDO is connected to the computer unless you eject the BUSHIDO.

Select Menu Options for Survey and MAC Monitor

Figure 25 and Figure 26 show the Select menus for the Survey and MAC Monitor screens, respectively. Each menu option is described below.

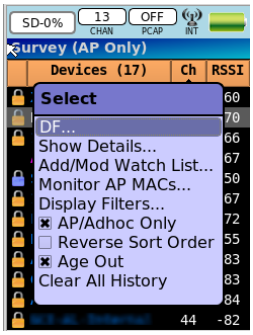


Figure 25

Figure 26

DF

Selecting DF allows the operator to target a specific device. Figure 27 shows the DF screen which provides the operator with the following information, depending on the device.

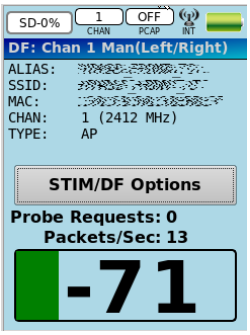


Figure 27

<u>AP</u>

- ALIAS: The user-defined name for the device if on the Watch List.
- SSID: The network name of the AP.
- MAC: The MAC address of the AP.
- CHAN: The current channel of the AP.
- TYPE: AP, AP (WDS), or AP (Hidden).

<u>Station</u>

- ALIAS: The user-defined name for the device if on the Watch List.
- MAC: The MAC address of the Station.
- SSID: The network name of the associated AP.
- AP MAC: The MAC address of the associated AP.
- AP CHAN: The current channel of the associated AP.
- TYPE: STATION or STATION (Disconnect).

Probe Requests shows a cumulative count of probe requests detected since entering the DF screen. Probe Requests are useful in the search for a target. Probe request may indicate that a target is in the area, but not necessarily on this channel.

Packets/Sec shows the current detected packet rate for this device. This number should increase when STIM'ing a device.

The signal strength detector shows the RSSI. There are three colors indicating the time since the last detected packet:

- Green: Less than 5 seconds
- Yellow: 5 to 9 seconds
- Red: Greater than 9 seconds

The STIM/DF Options button will allow the user to configure Stimulation (STIM) options, Auto Hunting and PCAP Logging (Figure 28).

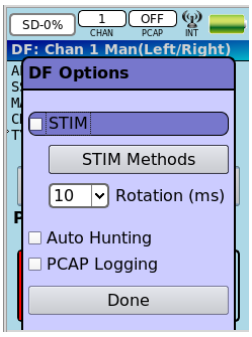


Figure 28

STIM – Check this box to turn on traffic stimulation. If enabled, it will rotate through the selected STIM Methods (RTS/CTS, TIM, TPC, ARPING, and/or UNASSOC) at a configurable rotation delay of 10, 25, 50 or 100 milliseconds.

NOTE: If the UNASSOC STIM method has been selected, a warning dialog will be shown to notify the user that the target device may alert its user. The UNASSOC STIM method will also temporarily disable the auto hunting option.

STIM Methods – Select the desired STIM Methods (Figure 29). A check in the box selects the method.

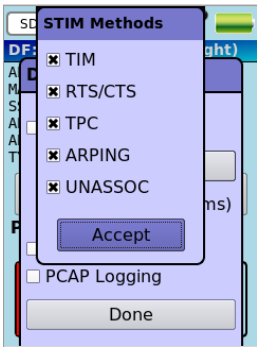


Figure 29

- **TIM** – Spoofed Traffic Indication packets are sent to the target causing it to request data from the AP.
- **RTS/CTS** – Request to send packets are sent to the target causing it to reply with a Clear to send packets.
- **TPC** – Transmit Power Control packets are sent to the target causing it to send power measurements.
- **ARPING** – Layer 2 ARP ping packets are sent to the target causing it to send ARP replies (open networks only).
- **UNASSOC** – Create multiple APs with SSID based on target's probe requests to initiate communication.

Auto Hunting – Check this box to enable the automatic search for targets. Auto Hunt mode will follow this process:

1. If no packets are seen and the RSSI bar graph goes red, about 15 seconds later Hunt mode begins. The title bar displays "Chan *NN* Hunting".
2. Initially, it will scan through channels quickly to determine available APs.
3. Using the list of available APs, it will camp on each AP's channel for a few seconds searching for the target. If STIM options are enabled, and the channel has multiple APs, it will stay on the channel longer.
4. If the target is found, the title bar will change to "Chan *NN* Hunt (Auto)" and it will repeat from step 1.
5. If the target isn't found, it will repeat the process from step 3. Periodically, it will repeat the process from step 2 in order to refresh the AP list.

If Auto Hunt mode is disabled, then the title bar will display "Chan *NN* Man(Left/Right)". The user can manually change channels by pressing the left/right buttons.

NOTE: Auto Hunt mode will be temporarily disabled while UNASSOC STIM is in progress.

PCAP Logging – Check this box to turn on PCAP logging.

Proper Usage when Direction Finding

- Be sure to hold the BUSHIDO up against chest and pointing straight in front (Figure 30).
- Tilting the nose of the BUSHIDO up slightly will increase performance.
- Slowly point the BUSHIDO in all directions. Proceed in the direction that displays the highest RSSI reading (closest to 10 dBm).

Figure 30

Show Details

Alias, MAC, SSID, Type, Vendor, Channel, and Encryption status will be displayed (Figure 31).

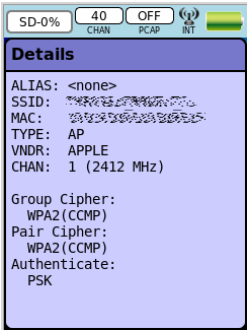


Figure 31

Add/Mod Watch List

The operator can select the Friendly or Target type. Friendly entries will not show up on Survey or MAC Monitor screens, nor will be recorded in PCAP files.

For APs, select MAC, SSID or both. For Stations, only MAC is selectable.

After selecting the Done button, the WL Alias will be created from either an AP's SSID or default to "TGT-xx:xx:xx" where xx:xx:xx is the last three bytes of the MAC address.

Figure 32

Monitor AP MACs

Monitor AP MACs will perform a survey of the associated Stations for a specific AP. When selecting Monitor AP MACs for an AP from either the Survey or MAC Monitor screens, the associated Stations for that AP will be displayed. When selecting Monitor AP MACs for an associated Station, the associated AP will be determined and that AP's associated Stations will be displayed. For unassociated Stations, the Monitor AP MACs menu options will not be available.

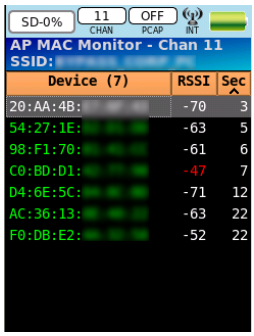


Figure 33

The Monitor AP MACs screen is a slightly modified version of the MAC Monitor screen displaying the same MAC, RSSI, and Seconds (Figure 33) and the same menu options (Figure 34). The SSID for the AP is shown in the title bar above the table.

Figure 34

To go to the MAC Monitor screen from the Monitor AP MACs screen, press the SELECT button and uncheck Monitor AP MACs.

Select Channel (MAC Monitor only)

Select Channel will allow the operator to change the channel within the current channel map (Figure 35). The channel map is editable from the Settings screen (Figure 23).

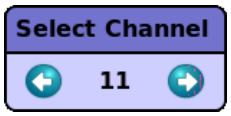


Figure 35

Regions Supported: USA, JAPAN, and EUROPE

Channels Supported:
1,2,3,4,5,6,7,8,9,10,11,12,13,14
34,36,38,40,42,44,46,48,52,56,60,64
100,104,108,112,116,120,124,128,132,136,140
149,153,157,161,165

Display Filters (Survey)

The filters shown on Figure 36 will allow the operator to filter out information from displaying on the screen that may not be important to them. Stations and watch list targets cannot be filtered and will always be displayed.

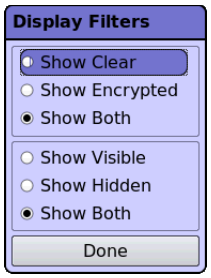


Figure 36

Radio button group for Show Clear, Encrypted, or Both

- Show Clear: Show only Clear (non-encrypted) APs
- Show Encrypted: Show only Encrypted APs
- Show Both: Show Clear and Encrypted APs

Radio button group for Show Visible, Hidden, or Both

- Show Visible: Show only Visible APs
- Show Hidden: Show only Hidden APs
- Show Both: Show both Visible and Hidden APs

Display Filters (MAC Monitor)

The filters shown on Figure 37 will allow the operator to filter out information from displaying on the screen that may not be important to them. Watch list targets cannot be filtered and will always be displayed.

Figure 37

Check box to show device type

- Show Stations: Uncheck box to hide stations
- Show APs: Uncheck box to hide APs
- Show Hidden APs: Uncheck box to hide hidden APs
- Show Ad-hoc: Uncheck box to hide Ad-hoc devices

AP/Adhoc Only (Survey only)

Selecting AP/Adhoc Only will allow the operator to not show Stations on the screen.

Reverse Sort Order

Reverse Sort Order when selected will reverse all displayed data. The "^" marker will switch to "v" (Figure 38).

Text data will switch from ascending-descending to descending-ascending order.

Numeric data will switch from lowest-highest to highest-lowest order.

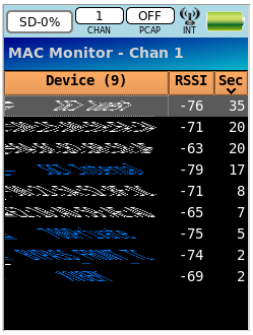


Figure 38

Age Out

Check this box to Age Out entries (Figure 39). If selected, devices that don't transmit data within 40 seconds will disappear from the screen. Unselecting Age Out will display all devices in its history.

Figure 39

Clear All History

Selecting Clear All History will clear all internal history for both the Survey and MAC Monitor screens.

Field Upgrade Instructions

Figure 40

1. Determine the current software version on the Settings screen (see page 17).

2. Connect BUSHIDO to computer via USB cable.

   The BUSHIDO will display a black screen indicating that it is in "Mass Storage Mode" (Figure 40).

   Upgrading from software version 1.x:
   If connected properly, the BUSHIDO will show up as a removable drive named "BUSHIDO". Copy the BUSHIDO upgrade package file to the "UpgradePackages" folder on the "BUSHIDO" drive.

   Upgrading from software version 2.x:
   If connected properly, the BUSHIDO will show up as two removable drives named "Bus-####" (where #### is the unit serial number) and "BUSHIDO". Copy the BUSHIDO upgrade package file to the "UpgradePackages" folder on the "Bus-####" drive.

3. Verify or rename the file in the "UpgradePackages" folder to **bushido.upgrade.pkg.**

4. Once the file copy/rename has completed, SAFELY REMOVE the drive(s) from the computer.

   - Windows - right click and select EJECT
   - Mac - drag the drive to the trash bin to eject the drive

5. Once safely ejected, the upgrade process will begin automatically. The USB cable can now be disconnected.

   This process can take a few minutes. The BUSHIDO will display upgrade status as it upgrades.

6. Upgrading from software version 1.x:
   When the upgrade has completed, the BUSHIDO will indicate that the upgrade was successful. The BACK key can be pressed to shut down the device.

   Upgrading from software version 2.x:
   When the upgrade has completed, the BUSHIDO will indicate that the upgrade was successful and will reboot. If the USB cable is still connected, the BUSHIDO will return to "Mass Storage Mode".

Remote Control

The BUSHIDO can be remotely controlled using the WRC app on an Android phone. When the BUSHIDO is being remotely controlled, local control is locked out and the display will show Figure 41.

Figure 41

Additional features are provided through WRC that are not directly available via the BUSHIDO user interface. Refer to the WRC User Guide for details on these features:

- MAC Capture
- MAC Compare
- View Probe Requests
- View SSID watch list history

If the WRC app is terminated, or disconnected from the BUSHIDO, local control is restored and the BUSHIDO GUI will be at the main window (Figure 42).

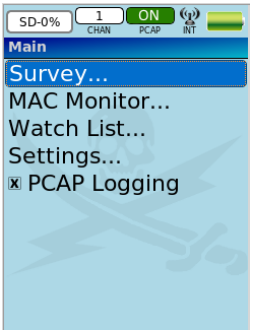


Figure 42

Warranty Statement

The KEYW Corporation warrants each new product manufactured to be free from defects in material and workmanship under normal use and service for the warranty period. This warranty is provided to the original end user and is not assignable or transferable. The KEYW Corporation will repair, without charge, any KEYW product which fails due to a defect in material or workmanship within the warranty period. This warranty excludes damage caused by improper operation, testing, repair, modification, alteration, adjustment, installation, or maintenance of the KEYW product. Damage resulting from either accident or neglect is also excluded. The preceding warranty is The KEYW Corporation's only warranty concerning the products, services and any deliverables resulting under this order, and is made expressly in lieu of all other warranties and representations, express or implied, including any implied warranties of fitness for a particular purpose, merchantability, non-infringement or otherwise.

NOTWITHSTANDING ANY OTHER PROVISION OF THIS WARRANTY AND EXCEPT AS OTHERWISE PROVIDED UNDER APPLICABLE LAW, IN NO EVENT SHALL KEYW BE LIABLE FOR INDIRECT, SPECIAL, CONSEQUENTIAL, MULTIPLE OR PUNITIVE DAMAGES, OR ANY DAMAGE DEEMED TO BE OF AN INDIRECT OR CONSEQUENTIAL NATURE ARISING OUT OF OR RELATED TO ITS PERFORMANCE UNDER THE WARRANTY, WHETHER BASED UPON BREACH OF CONTRACT, WARRANTY, NEGLIGENCE AND WHETHER GROUNDED IN TORT, CONTRACT, CIVIL LAW OR OTHER THEORIES OF LIABILITY, INCLUDING STRICT LIABILITY. THE KEYW CORPORATION SHALL NOT BE LIABLE FOR THE LOSS OF ANTICIPATORY PROFITS.

ITAR Restriction

These materials are controlled by the International Traffic in Arms Regulations, 22 C.F.R. Parts 120 - 130, and require an export license from the U. S. Department of State prior to transfer to a foreign person or foreign destination. If these materials are exported or otherwise retransferred without the necessary license(s) or in violation of the terms or conditions of any export license, recipient shall indemnify and hold harmless KEYW, its employees and parents, its and their successors and assigns, from and against any and all liability or harms, including attorney fees, arising therefrom.

BUSHIDO USER GUIDE (v2.1)

BUSHIDO Kit Contents

- Pelican 1200 case with custom fitted foam insert
- BUSHIDO Wi-Fi detector
- Adjustable lanyard
- Wired ear bud headset (Motorola cell phone style)
- 12/24 VDC automotive power adapter
- USB cable for charging and PC interface
- 2.5mm to 3.5mm adapter (for use with standard audio headphones)
- Universal AC wall power adapter
- RF Cable for external antenna (external antenna not included)

CDW·G

CDWG.com | 800.594.4239

OE400SPS

SALES QUOTATION

QUOTE NO.	ACCOUNT NO.	DATE
HCBC444	5218279	5/17/2016

BILL TO:
CITY OF FT WORTH- IT SOLUTIONS
1000 THROCKMORTON ST

Accounts Payable
FORT WORTH , TX 76102-6311

Customer Phone #817.871.6640

SHIP TO:
CITY OF FT WORTH- IT SOLUTIONS
Attention To: FINANCE DIVISION
1000 THROCKMORTON ST

FORT WORTH , TX 76102-6311
Contact: JULIE RIOS 817.392.7805

Customer P.O. # HCBC444 QUOTE

ACCOUNT MANAGER	SHIPPING METHOD	TERMS	EXEMPTION CERTIFICATE
DAVE EDWARDS 877.274.3443	FEDEX Ground	Net 30 Days-Govt State/Local	STATE

QTY	ITEM NO.	DESCRIPTION	UNIT PRICE	EXTENDED PRICE
25	3604020	CANON 2.1MP PTZ 1080P UP TO 30FPS Mfg#: VB-H43 Contract: National IPA Technology Solutions 130733	1,651.29	41,282.25
25	4134986	CANON 1.3MP LOW LIGHT PTZ 30 FPS Mfg#: VB-M50B Contract: National IPA Technology Solutions 130733	2,379.40	59,485.00
		SUBTOTAL		100,767.25
		FREIGHT		0.00
		TAX		0.00

US Currency

TOTAL 100,767.25

Please remit payment to:
CDW Government
75 Remittance Drive
Suite 1515
Chicago, IL 60675-1515

CDW Government
230 North Milwaukee Ave.
Vernon Hills, IL 60061

Fax: 312.752.3902

This quote is subject to CDW's Terms and Conditions of Sales and Service Projects at
http://www.cdwg.com/content/terms-conditions/product-sales.aspx
For more information, contact a CDW account manager.

Interpreting Call Detail Records

Your response includes Call Detail Records (CDR) either with or without location. Our query results in an Excel file with multiple columns. Each row represents one call on the T-Mobile network. Some fields only appear in reports with location information.

Multimedia Messages (MMS) and text messages sent as MMS **do not** appear as part of a call record. Standard text messages **do** appear on this report. Calls made while roaming also **do not** appear on this report.

Entries with outgoing calls to 8056377249 indicate incoming calls that are forwarded (out) to the voicemail system. Entries with outgoing calls to 8056377243 = 805-MESSAGE indicate voicemail retrieval.

Please remember that T-Mobile CDR systems natively use Coordinated Universal Time (UTC). By default, that means a day of call detail records are taken from 00:00:01 to 23:59:59 UTC which may differ from your intended time range due to your time zone. If specific times other than our default are important to your inquiry, please submit legal demands with the date range/time frame adjusted for UTC to avoid delay or confusion. We are unable to convert the time displayed in the records to the local time of the handset.

The columns present on your CDR may be:

COLUMN NAME	DESCRIPTION	LOCATION RPT ONLY?	NOTES
Date	Date format mm/dd/yyyy	NO	
(UTC) Time	24 hour time format - hh:mm:ss in UTC	NO	In UTC time
Duration	Duration hh:mm:ss	NO	
Call Type	Type of call: callForwarding = Forwarded Call; mSOriginating = Outgoing Voice Call; mSTerminating = Incoming Voice; mSOriginatingSMSinMSC = Outgoing SMS; mSTerminatingSMSinMSC = Incoming SMS; moc=Mobile Originating Call; mtc= Mobile Terminating Call	NO	
Direction	Outgoing or Incoming to the target telephone number	NO	
Calling Number	Phone number that initiated the call	NO	
Dialed Number	Dialed digits	NO	
Called Number	Phone number that received the call	NO	
Destination Number	The final destination number to which the network has connected the call (might be different from the one dialed by subscriber if network translation was applied)	NO	
IMSI	International Mobile Subscriber Identity of the target number, if present	NO	
IMEI	International Mobile Equipment Identity of the target number, if present	NO	
Completion Code	Completed successfully or Abnormal Completion (network interruption). Abnormal completion calls display on this report but may or may not show on a customer's bill.	NO	
Answered?	Answered or Unanswered. Unanswered calls display on this report but may or may not show on a customer's bill.	NO	
Service Code	11 Calling line identification presentation 12 Calling line identification restriction 13 Connected Line ID Presentation 20 All Call Forwarding Services 21 Call Forwarding Unconditional (CFU) 28 All Cond Call Forwarding Services 29 Call Forwarding on Mobile Subscriber Busy (CFB) 2A Call Forwarding on No Reply (CFNRy) 2B Call Forwarding on Not Reachable (CFNRc) 31 Explicit Call Transfer (ECT) 42 Call Hold 41 Call waiting 51 Multi-Party (MPTY)	NO	
Disconnecting Party	Calling Party; Called Party or Network	NO	

Service Indicator	If populated, then the call was originated on WIFI/VoLTE, and has continued on GSM (expect 2 CDRs for same call leg)	NO	
SMS Deliv Status	SMS delivery result	NO	
Switch Name	Name of the switch which was used to deliver the call to the target number.	NO	This is NOT an indication of the location of the device.
1st LTE Site ID	EnodeBid value in decimal	YES	Only present if the call was over LTE
1st LAC	1st LAC value in decimal	YES	Not present if the call was over LTE
1st Cell ID	1st Cell Site ID value in decimal	YES	Not present if the call was over LTE
1st Tower Azimuth	Location: Azimuth orientation of antenna serving user if available (see note below)	YES	
1st Tower LAT	Latitude of 1st cell tower used.	YES	
1st Tower LONG	Longitude of 1st cell tower used.	YES	
1st Tower Address	Street Address of the 1st serving tower if available	YES	
1st Tower City	City of the 1st serving tower if available	YES	
1st Tower State	State of the 1st serving tower if available	YES	
1st Tower Zip	ZIP of the 1st serving tower if available	YES	
Last LTE Site ID	EnodeBid value in decimal	YES	Only present if the call was over LTE
Last LAC ID	Last LAC value in decimal	YES	Not present if the call was over LTE
Last Cell ID	Last Cell Site ID value in decimal	YES	Not present if the call was over LTE
Last Tower Azimuth	Azimuth orientation of antenna serving user if available (see note below)	YES	
Last Tower LAT	Latitude of last cell tower used.	YES	
Last Tower LONG	Longitude of last cell tower used.	YES	
Last Tower Address	Street Address of the last serving tower if available	YES	
Last Tower City	City of the last serving tower if available	YES	
Last Tower State	State of the last serving tower if available	YES	
Last Tower Zip	ZIP of the last serving tower if available	YES	

A NOTE ON AZIMUTH: The azimuth listed is the center compass degree facing of the identified sector of the tower. Generally, the coverage of a tower is circular and divided in three equal pieces (each 120 degrees wide). Due north is 0, due south is 180. However, not every tower is aligned with the first sector starting at 0. Using the listed azimuth, rough direction from the tower can be calculated for a call. The center degree of the sector's facing is indicated in this field. For example, if a facing has a listed orientation of 90, the center of the coverage is pointed at 90 degrees but the sector will cover traffic from roughly 60 degrees on either side (thus 30 to 150 degrees in this example).

For more information on UTC, please visit: http://www.timeanddate.com/time/aboututc.html. To convert records to your local time, you will need to use a converter such as http://www.worldtimeserver.com/convert_time_in_UTC.aspx.

Interpreting Subscriber Information

Your response includes subscriber information. Our query results in an Excel file with multiple rows. Not all rows appear on every report depending on the type of subscriber, their dates of service and the nature of your request.

The rows present **may** be:

Subscriber Details:	
Subscriber Name	Name associated with billing for this phone number
Subscriber Address	Address associated with this phone number
Subscriber Status	Status of the account
Subscriber Name Effective Date	Date this name became associated with this phone number

Account Details:	
Activation Date	Account Activation Date
Termination Date	Cancellation/Termination Date, if it has been terminated
Account Name	Primary Accountholder's Name
Account No	Billing Account Number (BAN)
Account Effective Date	Current Account Status Effective Date
Account Expiration Date	Account Expiration Date, if it has been terminated

Device Details:	
Phone Model	Phone Model
ICCID	Integrated Circuit Card Identifier for the SIM card
IMSI	International Mobile Subscriber Identity
MDN Effective Date	Phone number begin date
MDN Expiration Date	Phone number end date
MSISDN No	Target number
MSISDN Status	Current status of this telephone number
MSISDN Market	Home market of this telephone number
MSISDN Name	Name associated with this telephone number
SIM	Subscriber Identity Module number associated with this phone number
IMEI	International Mobile Equipment Identity
Begin Service Date	N/A
Device Network Type	GSM or CDMA (only displays for legacy MetroPCS customers

Billing Details:	
Bill Name	Name associated with billing for this phone number
Bill Birth Date	Subscriber birth date
Bill SSN	Subscriber Social Security Number
Bill Cycle	Bill cycle for postpaid subscribers
Bill Address	Subscriber address
Company Name	Business Name
Rate Plan	Subscriber Plan
Rate Plan Desc	Description of major features under the plan
Contact 1	Primary contact phone number

Contact 2	Secondary contact phone number
Brand	TMUS brand or MVNO providing service
Coupon	Prepaid Coupon Serial Number
Last Refilled	Last Prepaid Refill Date

Ported Details:

Ported Carrier	Company to which the number has been ported, if known

PLEASE NOTE: You may receive multiple subscriber information files if the target has used their SIM card with multiple devices or if the subscriber's line has been suspended multiple times within your target timeframe.

	Vigilant Solutions **2021 Las Positas Court** **Suite # 101** **Livermore, CA 94551** **(P) 845-797-3092 (F) 925-398-2113**	**Be smart. Be safe.** **Be Vigilant.**

Attention:	Fort Worth Police Department	Date	9/1/2016
Project Name:	Data Renewal	Quote Number:	KJS-0700-01

PROJECT QUOTATION

We at Vigilant Solutions are pleased to quote the following systems for the above referenced project:

Qty	Item #	Description
(1)	VS-LDS-3	**Vigilant 'Commercial Data' Access via LEARN** • Local/State LEA Tier 3 Commercial LPR Data access • Access to all Vigilant commercially acquired national vehicle location data • Unlimited access for agency wide unlimited users of all commercial LPR data and LEARN components • Includes full use of hosted/managed LPR server account via LEARN • Includes Vigilant's complete suite of LEARN data analytics • As per the Vigilant Solutions Software Service Agreement
(1)	VS-FSHSL-3	**FaceSearch with Vigilant Image Gallery Access** • Hosted access to agency/shared images and Vigilant Image Gallery • Agency wide
Subtotal Price (Excluding sales tax)		**$49,500.00**

Quote Notes:

1. All prices are quoted in USD and will remain firm and in effect for 60 days.
2. LEARN Data Subscription for period 11/1/16 - 10/30/17
3. Face Search Account Included at no additional cost

Quoted by: Kevin Schneider - 845-797-3092 - kevin.schneider@vigilantsolutions.com

Total Price (Excluding sales tax)	**$49,500.00**	
Accepted By:	Date:	P.O#

Milestone Systems

Milestone Mobile 2014 (Server)

The Open Platform Company

Contents

Introduction

About Milestone Mobile

Milestone Mobile includes:

- **Milestone Mobile client**
- **Milestone Mobile server**
- **Milestone Mobile plug-in**

The Milestone Mobile client is a mobile surveillance application that you download and install on your Android smartphone/tablet, Apple® device or Windows 8 Phone device. You can install as many instances of Milestone Mobile clients as you need. See the **Milestone Mobile User's Manual** at http://www.milestonesys.com/mobilehelp (http://www.milestonesys.com/mobilehelp) for further information.

The Milestone Mobile server and Milestone Mobile plug-in are covered in this Administrator's Manual.

Prerequisites for using Milestone Mobile

The following items must be in place before you can start using Milestone Mobile:

- An XProtect system installed and configured with at least one user.
- Cameras and views set up in XProtect® Smart Client.
- A mobile device running Android, iOS or Windows 8 and access to Google Play, App Store℠ or Windows Phone Store from which you can download the Milestone Mobile application.
- If you run XProtect Go, install the Milestone Mobile server on the same physical computer as XProtect Go.

Milestone Mobile is only compatible with some versions of XProtect. See System requirements for Milestone Mobile server (see "XProtect Mobile server" on page 6) for more information.

Access XProtect Web Client

If you have a Milestone Mobile server installed on your computer, you can use the XProtect® Web Client to access your cameras and views. Since you do not need to install XProtect Web Client, you can access it from the local computer on which you installed the Milestone Mobile server or any other computer you want to use for this purpose.

To access the XProtect Web Client:

1. Set up the Milestone Mobile server in the Management Application.
2. Open an Internet browser (Internet Explorer, Mozilla Firefox, Google Chrome or Safari) or click **Open XProtect Web Client** in the Mobile Server Manager (see "About Mobile Server Manager" on page 18).

3. Type in the IP address (that is, the external address and port of the server on which the Milestone Mobile server is running.

   Example: The Milestone Mobile server is installed on a server with the IP address 127.2.3.4 and is configured to accept HTTP connections on port 8081 and HTTPS connections on port 8082 (default settings of the installer).

   In the address bar of your browser, type: http://127.2.3.4:8081 or https://127.2.3.4:8082, depending on whether you want to use a standard HTTP connection or a secure HTTPS connection. You can now begin using XProtect Web Client.

4. Add the address as a bookmark in your browser for easy future access to XProtect Web Client. If you use XProtect Web Client on the local computer on which you installed the Milestone Mobile server, you can also use the desktop shortcut created by the installer. Click the shortcut to launch your default browser and open XProtect Web Client.

You must clear the chase of Internet browsers running the XProtect Web Client before you can use a new version of the XProtect Web Client. System administrators must ask their XProtect Web Client users to clear out their browser's cache upon upgrade or force this action remotely (you can do this action only in Internet Explorer in a domain).

System requirements

XProtect Mobile client

Smartphones or tablets running Android 2.2+, iOS5+ or Windows 8 Phone or portable music players using iOS5+.

XProtect Mobile server

Name	Description
Operating system	▸ Windows 7 Professional (32-bit or 64-bit*) ▸ Windows 7 Enterprise (32-bit or 64-bit*) ▸ Windows 7 Ultimate (32-bit or 64-bit*) ▸ Windows 8 ▸ Windows 8.1 ▸ Windows 2012 Server ▸ Windows 2012 Server R2
CPU	Minimum Intel® Pentium® 4, 2.4 GHz or higher (CoreTM 2 recommended).
RAM	Minimum 2 GB (4 GB or more recommended).
Network	Ethernet (1 Gbit recommended).
Graphics	Adapter AGP or PCI-Express, minimum 1024 x 768, 16-bit colors.
Hard disk type	E-IDE, PATA, SATA, SCSI, SAS (7200 RPM or faster).
Hard disk space	Minimum 1 GB free hard disk space available, excluding space needed for recordings.
Software	▸ Microsoft .NET 3.5 and 4. ▸ DirectX 9.0 or newer. ▸ Windows Help (WinHlp32.exe). Download all from http://www.microsoft.com/downloads (http://www.microsoft.com/downloads).

Name	Description
Milestone XProtect® video management software	▸ XProtect® Corporate 5.0+ ▸ XProtect® Expert 2013+ ▸ XProtect® Enterprise 8.1+ ▸ XProtect® Professional 8.1+ ▸ XProtect® Express 1.1+ ▸ XProtect® Essential 2.1+ ▸ XProtect® Go 2.1+

* Running as a 32-bit service/application.

XProtect Mobile plug-in

See the **System requirements** section in your system documentation.

Configuration

About Mobile server

A Mobile server handles log-ins to the system from Milestone Mobile client from a mobile device or XProtect Web Client.

Upon correct login, the Mobile server distributes video streams from relevant recording servers to Milestone Mobile client. This offers an extremely secure setup, where recording servers are never connected to the Internet. When a Mobile server receives video streams from recording servers, it also handles the complex conversion of codecs and formats allowing streaming of video on the mobile device.

You must install the Mobile server on any computer from which you want to access recording servers. Before you begin the installation of the Mobile server, make sure you are logged in with an account that has administrator rights. Installation cannot be successful if you use a standard user account.

About Video push

Video push is feature in your Milestone Mobile client that allows you to use your mobile device's camera to, for example, collect evidence when you investigate an alarm or event. You do this by sending a video stream from your mobile device to your system. In the Mobile server settings, you can set up how many users should be able to use the Video push feature in the system.

About Milestone Federated Architecture and master/slave servers

If your system supports Milestone Federated Architecture and/or master/slave servers, you can access such servers with your Milestone client. Use this functionality to gain access to all cameras on all slave servers by logging in to the master server.

This means that when users of the Milestone client log in to a server to see cameras from all servers in your system, they must connect to the IP address of the master server. Users must have administrator rights on all servers in the system in order for the cameras to show up in the Milestone client.

If you use XProtect Enterprise or any other streamlined software version (that is XProtect Professional, XProtect Express, XProtect Essential or XProtect Go), you should only install the Milestone server on the master server and not on any slave servers. System administrators must make sure that client users only connect to a master server.

About actions

You can manage the availability of the **Actions** tab in the Milestone Mobile client by enabling or disabling this on the Mobile server tab. **Actions** are by default enabled, and all available actions for the connected devices are shown here.

About naming an output for use in Milestone Mobile

In order to get actions shown correctly together with current camera, it is important that the output uses the exact same name as the camera.

Example:

If you have a camera named "AXIS P3301,P3304 - 10.100.50.110 - Camera 1", you must also name the action "AXIS P3301,P3304 - 10.100.50.110 - Camera 1".

You can add a further description to the title afterwards, for example "AXIS P3301,P3304 - 10.100.50.110 - Camera 1 - Light switch".

Important: If you do not follow these naming conventions, actions are not available in the action list for the associated camera's view. Instead, actions appear in the list of other actions on the **Actions** tab.

About saving configuration changes in XProtect Enterprise 8.1 and streamlined software versions

The following applies to XProtect Enterprise 8.1, XProtect Professional 8.1, XProtect Express 1.1, XProtect Essential 2.1 and XProtect Go 2.1 software versions only.

If you are logged into the Milestone Mobile client and are watching one or more cameras views while at the same time changing configuration in the Management Application, the live video from the camera may freeze in the Milestone Mobile client if you click **File > Save** in the Management Application**.**

To avoid this scenario, you must restart the Milestone Mobile service manually. See the Windows Help for information about how to do this.

If you are using newer versions of XProtect, the Milestone Mobile service restarts with the other services and no user action is required.

Add/edit a Mobile server

1. Go to **Servers** > **Mobile Servers.** From the menu that appears, select **Create New**. Fill in/edit the needed properties.

IMPORTANT: If you edit settings for **Login method, All cameras view** and **Outputs and events**, while you are connected to the Milestone Mobile client, you must restart the Milestone Mobile client for the new settings to take effect.

Add a Video push channel

Each Video push channel requires a separate camera license.

To add a Video push channel (see "About Video push" on page 8), do the following:

1. On the **Video Push** tab, select the **Video push** checkbox to enable the functionality.

2. In the bottom right corner, click **Add** to add a video push channel to the **Channels** mapping.
3. Channels are mapped to devices through user names. Select a user name from a user account already set up in your system to associate with the relevant Video push channel. If you do not associate the Video push channel with an already created user, you cannot use Video push in your Milestone Mobile client when you log in.
4. Add the Video push driver as a hardware device (see "Add a Video push driver as a hardware device" on page 10) to the system. You must choose the **Manual** hardware device detection method as the Video push driver does not show up in automatic hardware searches.
5. On the **Video Push** tab, click **Find Cameras**. If successful, the newly added Video push driver appears in this list. Save your configuration to make the Video push driver ready for use.

You can remove video push channels you do not require. To do so, select the relevant channel and click **Remove** in the bottom right corner.

Add a Video push driver as a hardware device

If you add a Video push channel, you must add the Video push driver to your Management Application/Management Client. To do so:

1. Open the **Add New Hardware Wizard** in your Management Application/Management Client.
2. Choose the **Manual** option. The Video push driver will not be detected in automatic hardware searches.
3. Specify hardware device settings (see "Add hardware devices settings" on page 10) and select the hardware driver manually.
4. Once finished, your Video push driver must be associated with your Video push channel. To do so, return to your Mobile server > **Video Push** tab and click **Find Cameras**.

Add hardware devices settings

Specify the following settings when you add a Video Push driver in the **Add Hardware Devices** wizard:

Name	Description
Use:	Select if the Video push driver should added to the XProtect video management system.
Address:	Type in the Milestone Mobile server IP address.
Port:	Type in the port number for your Video push driver. The default port is 80. The port is for communication between the Milestone Mobile server and your XProtect server. **Important:** The port number you set must be identical with the port number you set when you specify your Video push settings (see "Video Push" on page 13). If the port numbers are not identical, your Video push channel will not work.

Name	Description
User name:	Select the same user name as associated with the Video push channel when you added (see "Add a Video push channel" on page 9) this.
Password:	Type in the password for the Video push driver. The password for your Video push driver is **Milestone** (this cannot be changed).
Hardware Driver:	Select the **Video push driver**.
Verified:	Select if the Video push driver runs on a secured HTTPS connection.

Once finished, go back to your Milestone Mobile server > **Video Push** tab and click **Find Cameras** to finish setting up the Video push channel.

Add an automatic export rule

1. In the Management Application/Management Client, click the relevant Mobile server > **Export** Tab.
2. Under **Automatic Exports**, click **Add...** to open the **Auto Export Rule** window**.**
3. Set the relevant Auto Export Rule window settings (on page 15).
4. When finished, click **OK**.

Mobile server settings

General

Fill in and specify general settings for the Milestone Mobile server:

Name	Description
Server name:	Enter a name of the Milestone Mobile server.
Description:	Enter an optional description of the Milestone Mobile server.
Mobile server:	Choose between all Milestone Mobile servers currently installed to the specific XProtect system. Only Milestone Mobile servers that are running are shown in the list.
Connection type:	Choose how clients should connect to the Milestone Mobile server. You can choose between the following options: **HTTP only**, **HTTP and HTTPS** or **HTTPS Only**.
Client timeout (HTTP):	Set a time frame for how often the Milestone Mobile client must indicate to the Mobile server that it is up and running. The default value is 30 seconds. Milestone recommends that you do **not** increase the time frame.

Name	Description
Login method:	Select how you want to log in to the Mobile server server should take place. You can choose between the following options: **Automatic, Windows Only** or **Basic Only.**
Enable XProtect Web Client:	Enable the use of XProtect Web Client.
Enable all cameras view:	Enable/disable viewing of **All Cameras** view. This view contains all cameras on a recording server (user rights permitting).
Enable actions (events and outputs):	Enable/disable actions in Milestone Mobile clients.
Enable keyframes:	Enable/disable video stream to stream key frames only. Enabling key frames only reduces bandwidth usage.
Enable full-size images:	Enable the Milestone Mobile server to send full-size images to the MilestoneMobile client or XProtect Web Client. Note that enabling full-size images increases your bandwidth usage and that enabling this option disables all rules set up in the **Performance** settings.
Direct streaming:	Choose how to handle direct streaming in XProtect Web Client. Choose between enforcing the use of direct streaming, enforcing the use when possible or never enforcing its use.
Configuration backup:	Import or export your Milestone Mobile server configuration. Your system stores the configuration in an XML file.

Server Status

See the status details for your Mobile server. The details are read-only:

Name	Description
Server active since	Shows how long the Mobile server has been running since it was last stopped.
CPU usage	Shows current CPU usage on the Mobile server.
Internal bandwidth	Shows the current bandwidth in use between the Mobile server and the relevant recording server.
External bandwidth	Shows the current bandwidth in use between the mobile device and Mobile server.
User Name column	Shows user name(s) of the Mobile server user(s) connected to the Mobile server.
State column	Shows the current relation between the Mobile server and the Milestone Mobile client user in question. Is the user connected (a state preliminary to servers exchanging keys and encrypting credentials) or is he/she actually logged in? Possible states are: **Connected** and **Logged** In XProtect.

Name	Description
Bandwidth Usage column	Shows the level of bandwidth used by the Mobile server client user in question.
Live Streams column	Shows the number of live video streams currently open for the Milestone Mobile client user in question.
Playback Streams column	Shows the number of playback video streams currently open for the relevant Mobile client user.
Video Push streams	Shows the number of Video Push stream currently open for the relevant Mobile client user.
Direct Streams	Shows the number of live video streams using Direct Streaming that are currently open for the relevant Mobile user.

Video Push

If you enable Video push, specify the following settings:

Name	Description
Video push	Enable Video push on the Mobile server.
Number of channels	Specify the number of enabled Video push channels in your XProtect system.
Channel column	Shows the channel number for the relevant channel. Non-editable.
Port	Port number for the relevant Video push channel.
MAC	MAC address for the relevant Video push channel.
User Name	Enter the user name associated with the relevant video push channel.
Camera Name	Shows the name of the camera if the camera has been identified.

Once you have completed all necessary steps (see "Add a Video push channel" on page 9), click **Find Cameras** to search for the relevant camera.

Export

Specify the following settings for exported recordings:

Name	Description
Export	Select to enable export in clients.
Include timestamps	Select to add timestamps to exported video.
Used codec for AVI files	Choose a codec to use to encode your exported AVI video files.
Export to	Specify the location to which recordings should be exported.

Name	Description
Delete exported recordings older than	Enter the number of days to pass before recordings are deleted. Note that if the value is set to 1 day, exported files are deleted up to 10 minutes from the applied change, not immediately. Users can restart the Mobile server manually to make the changes take effect immediately.
Limit size of exports folder to	Enter a number to set a maximum limit for the folder to which the recordings are exported.
View exports of other users	Select this check box to enable users to be able to view exports made by other users.

Automatic exports

If you want to set up your system to automatically export video when a certain event occurs, you must set up rules to instruct the system about when to carry out automatic exports:

Enabled	Select this check box to enable automatic exports.

In the columns below the **Enabled** check box is a list of all automatically exported video. See the following details for individual automatic exports:

Name column	Name of the rule.
Item column	Item that triggers the automatic export.
Event column	Shows event that triggers the automatic export.
Camera column	Camera from which the video is recorded.
Duration column	Length of the exported video file.
Export type column	Indicates whether the export file format is database format or AVI format.

Exported recordings

In the columns, see the following details for every individual exported recording:

Name column	Name of the exported recording.
State column	State of the exported recording.
Camera column	The camera that provided the exported recording.
Timestamp column	The point of time when the export took place.
Duration column	The length of the exported recording.
User column	The name of the user who provided the exported recording.
MB column	The size of the exported recording.
Type	The type of export. This can be **Manual** or **Automatic**.

Note: Click Refresh to update the list of exported recordings shown.

Auto Export Rule window settings

When you add a new rule for automatic export to take place, specify the following:

Name	Description
Name:	Provide a name for the rule you want to create, for example **Door opened** or **Motion detected**.
Item:	Choose the item to trigger the automatic export. This can be cameras, inputs, outputs and events. If you select a camera, this will automatically be selected as the camera to record video from.
Item type:	Displays the type of selected item.
Event:	Shows event that is used to trigger the automatic export. Type of available events depends on selected item.
Camera:	Select the camera from where the video will be recorded.
Duration:	Type the amount of time the video clip should export (in seconds).
Export type:	Choose whether the exported video clip should be in the XProtect database format or if it should be exported as an AVI file.

Performance

On the **Performance** tab, you can set the following limitations on the Milestone Mobile server's performance:

Level 1

Level 1 is the default limitation placed on the Milestone Mobile server. Any limitations you set here are always applied to the Milestone Mobile's video stream.

Name	Description
Level 1	Select the check box to enable the first level of limitations to Milestone Mobile server performance.
Max FPS	Set a limit for the maximum number of frames per second (FPS) to send from the Milestone Mobile server to clients.
Max image resolution	Set a limit for the image resolution to send from the Milestone Mobile server to clients.

Level 2

If you would rather like to enforce a different level of limitations that the default one in **Level 1**, you can select the **Level 2** check box instead. You cannot set any settings higher than what you have set them to in the first level. If you, for example, set the Max FPS to 45 on **Level 1**, you can set the Max FPS on **Level 2** only to 44 or below.

Name	Description
Level 2	Select the check box to enable the second level of limitations to Milestone Mobile server performance.
CPU threshold	Set a threshold for the CPU load on the Milestone Mobile server before the system enforces video stream limitations.
Bandwidth threshold	Set a threshold for bandwidth load on the Milestone Mobile server before the system enforces video stream limitations.
Max FPS	Set a limit for the maximum number of frames per second (FPS) to send from the Milestone Mobile server to clients.
Max image resolution	Set a limit for the image resolution to send from the Milestone Mobile server to clients.

Level 3

You can also select a **Level 3** check box to create a third level for limitations. You cannot set any settings higher than what you have set them to in **Level 1** and **Level 2**. If you, for example, set the **Max FPS** to 45 on **Level 1** and to level 32 on **Level 2**, you can set the **Max FPS** on **Level 3** only to 31 or below.

Name	Description
Level 3	Select the check box to enable the second level of limitations to Milestone Mobile server performance.
CPU threshold	Set a threshold for the CPU load on the Milestone Mobile server before the system enforces video stream limitations.
Bandwidth threshold	Set a threshold for bandwidth load on the Milestone Mobile server before the system enforces video stream limitations.
Max FPS	Set a limit for the frames per second (FPS) to send from the Milestone Mobile server to clients.
Max image resolution	Set a limit for the image resolution to send from the Milestone Mobile server to clients.

Note: The system does not instantly switch from one level to another level. If your CPU or bandwidth threshold goes less than five percent above or below the indicated levels, the current level stays in use.

Note that if you enable **Enable full-size images** on the **General** tab, none of the **Performance** levels are applied.

Log Settings

Fill in and specify the following log settings:

Name	Description
Enabled	Enable/disable logging of Milestone Mobile client's actions in a separate log file.
Log file location:	Path to where log files are saved.
Keep logs for:	Number of days to keep logs for (default 3 days).
CPU usage:	Default level of CPU usage which will trigger a warning in the log.
Internal bandwidth:	Default internal bandwidth usage which will trigger a warning in the log.
External bandwidth:	Default external bandwidth usage which will trigger a warning in the log.
Check every:	Default time frame (30 sec.) for checking warning levels.

Mobile Server Manager

About Mobile Server Manager

The Mobile Server Manager is a tray-controlled feature connected to Mobile server. Right-clicking the Mobile Server Manager icon in the system tray opens a menu from which you can easily access Mobile server functionality. You can:

- Open XProtect Web Client (see "Access XProtect Web Client" on page 4)
- Start, stop and restart the Mobile service (see "Start, stop and restart Mobile service" on page 20)
- Fill in or change surveillance server credentials (see "Fill in/edit surveillance server credentials" on page 20)
- Show/edit port numbers (on page 20)
- Edit certificate (on page 19)
- Open today's log file (see "About accessing logs and exports" on page 19)
- Open log folder (see "About accessing logs and exports" on page 19)
- Open export folder (see "About accessing logs and exports" on page 19)
- Show Mobile server status (see "About show status" on page 18)
- Access the Milestone Mobile Help website (where you find manuals, frequently asked questions (FAQs) and product demonstration videos.)

About show status

If you right-click the Mobile Server Manager and select **Show Status...** (or double-click the Mobile Server Manager icon), a window opens, showing the status of the Mobile server. You can see the following:

Name	Description
Server running since:	Time and date of the time when the Mobile server was last started.
Connected users:	Number of users currently connected to the Mobile server.
CPU usage:	How many % of the CPU is currently being used by the Mobile server.
CPU usage history:	A graph detailing the history of CPU usage by the Mobile server.

About accessing logs and exports

The Mobile Server Manager lets you quickly access the log file of the day, open the folder to which logs files are saved, and open the folder to which exports are saved.

To open any one of these, right-click the Mobile Server Manager and select **Open Today's Log File**, **Open Log Folder** or **Open Export Folder** respectively**.**

Important: If you uninstall Milestone Mobile from your system, its log files are not deleted. Administrators with proper rights can access these log files at a later timer, or decide to delete them if they are not needed any longer. The default location of the log files is in the ProgramData folder. If you change the default location of log files, existing logs are not copied to the new location nor are they deleted.

Edit certificate

If you want to use a secure HTTPS protocol to establish connection between your mobile device or the XProtect Web Client and the Mobile server, you must have a valid certificate for the device or web browser to accept it without warning. The certificate confirms that the certificate holder is authorized to establish the connection.

When you install the Mobile server, you generate a self-signed certificate if you run a **Typical** installation. If you run a **Custom** installation, you get the choice between generating a self-signed certificate or loading a file containing a certificate issued by another trusted site. If you, at a later point, want change the certificate you use, you can do this from the Mobile Server Manager.

1. Right-click the Mobile Server Manager and select **Edit Certificate...**
2. Choose whether you want to either:
   - Generate a self-signed certificate or
   - Load a certificate file.

Generate a self-signed certificate

1. Choose the **Generate a self-signed certificate** option and click **OK**.
2. Wait for a few seconds while the system installs the certificate.
3. Once finished, a window opens and informs you that the certificate was installed successfully. The Mobile service is restarted for the changes to take effect.

Locate a certificate file

1. Choose the **Load a certificate file** option.
2. Fill in the path for the certificate file or click the ... box to open a window where you can browse for the file.
3. Fill in the password connected to the certificate file.
4. When finished, click **OK**.

Note that HTTPS is not supported on Windows XP and Windows 2003 operating systems and works on Windows Vista or newer Windows OS only.

Fill in/edit surveillance server credentials

1. Right-click the Mobile Server Manager and select **Surveillance Server Credentials...**
2. Fill in the **Server URL**
3. Select what user you want to log in as:
   - Local system administrator (no credentials needed) or
   - A specified user account (credentials needed)
4. If you have chosen a specified user account, fill in **User Name** and **Password**.
5. When finished, click **OK**.

Show/edit port numbers

1. Right-click the Mobile Server Manager and select **Show/Edit Port Numbers...**
2. To edit the port numbers, fill in the relevant port number. You can indicate a standard port number (for HTTP connections) and/or a secured port number (for HTTPS connections).
3. When finished, click **OK**.

Start, stop and restart Mobile service

If needed, you can start, stop and restart the Mobile service from the Mobile Server Manager.

To perform any of these tasks, right-click the Mobile Server Manager and select **Start Mobile service**, **Stop Mobile service** or **Restart Mobile service** respectively**.**

Frequently asked questions (FAQs)

1. **Why can't I connect from my Milestone Mobile client to my recordings/Milestone Mobile server?**

   In order to connect to your recordings, the Milestone Mobile server must be installed on the server that runs your XProtect video management system or alternatively on a dedicated server. Furthermore, the relevant Milestone Mobile settings are needed in your XProtect video management setup. These are installed as either plug-ins or as part of a product installation or upgrade. For details on how to get the Milestone Mobile server and how to integrate the Milestone Mobile client-related settings in your XProtect video management system, see **What is Milestone Mobile** (see "**About Milestone Mobile**" on page 4). For relevant documentation of the Milestone Mobile server and the related Milestone Mobile client settings in your XProtect video management system, see **Manage Mobile Servers**.

2. **I installed the Milestone Mobile server to XProtect Corporate, but I can't connect to the server from my device. What is the problem?**

   After you have installed the Milestone Mobile server to your XProtect Corporate (4.0+), you must install the Milestone Mobile plug-in to see the Milestone Mobile server in your XProtect Corporate setup (Milestone Mobile Administrator's Manual which can be downloaded from http://www.milestonesys.com/downloads). When you have installed the Milestone Mobile plug-in, locate the plug-in under MIP Plugins in the navigation tree in the XProtect Corporate management client, expand it, choose Mobile Settings > Mobile Servers > Add New. Here, you add the details about your Milestone Mobile server (Server name, Description (optional), Server Address, Port and more). Once you finish, restart the Milestone Milestone Mobile Service (done from Windows Services) and try to reconnect with your device.

3. **How do I add a Milestone Mobile server/location/site to my Milestone Mobile client?**

   This is done from the Milestone Mobile client. When you open it for the first time, you must add one or more mobile servers in order to retrieve video from your cameras. Your added Milestone Mobile servers will be listed alphabetically. You can add as many Milestone Mobile servers as needed, as long as you have the needed log-in credentials.

4. **Why is the image quality sometimes poor when I view video in the Milestone Mobile client?**

   The Milestone Mobile server automatically adjusts image quality according to the available bandwidth between the server and client. If you experience lower image quality than in the XProtect® Smart Client, you might have too little bandwidth to get full resolution images through the Milestone Mobile client. The reason for this can either be too little upstream bandwidth from the server or too little downstream bandwidth on the client. See the **XProtect Smart Client User's Manual** which can be downloaded from http://www.milestonesys.com/downloads (http://www.milestonesys.com/downloads).

   If you are in an area with mixed wireless bandwidth, you may notice that the image quality improves when you enter an area with better bandwidth.

5. **How do I create views?**

   You cannot create or configure views in the Milestone Mobile client. It uses views and related names already created in the XProtect Smart Client. If you do not have any views set up, you

can use the **All cameras** view to see all the cameras in your system. You can always add more views to the XProtect Smart Client at a later time.

6. **How do I add a new Milestone Mobile user?**

   A Milestone Mobile user is just like any other XProtect user. You add a new Milestone Mobile user the same way you normally add a new user in your Management Client/Management Application: right-click on **Users** in the Navigation Pane and select **Add new basic user** or **Add new Windows user**. If you select new basic user, you must change the server login method to **Automatic** or **Basic Only** depending on your system. You change your server login method from the **Login method** drop-down menu on the **General** tab of the Mobile Server entry under **Servers** > **Mobile Servers** in the Management Application/Client.

7. **Can I control my pant-tilt-zoom (PTZ) cameras and use presets from Milestone Mobile client?**

   Yes, in the Milestone Mobile client, you can control your connected PTZ cameras and use presets in live mode.

8. **How can I navigate my recordings?**

   Android: You can navigate through your recordings in playback mode. Select the camera you wish to view in playback mode and choose **Menu** > **Playback**. Once you are in playback mode you can search through your recordings using the control buttons. You also have the option to go to a specific time by choosing **Menu** > **Go to time**. Once you have chosen **Go To time**, select the date and time you want to view.

   iOS: You can navigate through your recordings in playback mode. Select the camera you wish to view in playback mode and tap **Playback**. Once you are in playback mode, you can search through your recordings using the control buttons. You also have the option to go to a specific time by choosing **Menu > Go to time**. Once you have chosen **Go to time**, select the date and time you want to view and click **Confirm**.

9. **Can I view live and recorded video at the same time?**

   Yes, in playback mode, you get a small picture-in-picture (PiP) view live from the same camera.

10. **Can I use the Milestone Mobile client without a 3G data plan?**

    Yes, you can use Milestone Mobile through Wi-Fi. Either locally on the same network as your XProtect video management system or at a different location, such as a public network in a café or a home network. Note that bandwidth on public networks vary and may affect the image quality of the video streams.

11. **Can I use the Milestone Mobile client with a 4G/LTE data plan?**

    Yes, you can use any data connection on your mobile device that allows you to access the internet to connect to your XProtect video management system.

12. **Can I add multiple servers to the Milestone Mobile client?**

    When you open the Milestone Mobile client for the first time, you must add one or more mobile servers in order to retrieve video from your cameras. These Milestone Mobile servers are listed alphabetically. If you want to retrieve video from additional servers, repeat this process. You

can add as many Milestone Mobile servers as needed, as long as you have the relevant log-in credentials.

13. **Why is the image quality poor when I connect to my XProtect video management system at home through Wi-Fi at my office?**

    Check your home internet bandwidth. Many private internet connections have different download and upload bandwidths often described as, for example, 20 Mbit/2 Mbit. This is because home users rarely need to upload large amounts of data to the internet, but consume a lot of data instead. The XProtect video management system needs to send video to the Milestone Mobile client and is limited by your connection's upload speed. If low image quality is consistent on multiple locations where the download speed of the Milestone Mobile client's network is good, the problem might be solved by upgrading the upload speed of your home internet connection.

14. **Where are my screenshots saved?**

    Android: Snapshots are saved to your device's SD card at: **/mnt/sdcard/XProtect**.

    iOS: Snapshots are saved to your device and can be accessed from **Photos** on your device.

    You cannot change the default settings on neither Android nor iOS.

15. **How do I avoid the security warning when I run XProtect Web Client through an HTTPS connection?**

    The warning appears because the server address information in the certificate is incorrect. The connection will still be encrypted.
    The self-signed certificate in the Milestone Mobile server needs to be replaced with your own certificate matching the server address used to connect to the Milestone Mobile server. These certificates are obtained through official certificate signing authorities such as Verisign. Consult the chosen signing authority for more details.
    Milestone Mobile server does not use Microsoft IIS, even in XProtect Corporate installations. This means that instructions provided for generating certificate signing request (CSR) files by the signing authority using the IIS is not applicable for theMilestone Mobile server. You must manually create CSR-file using command line certificate tools or other similar third-party application. Please note that this process should be performed by system administrators and advanced users only.

Index

Copyright, trademarks and disclaimer

Trademarks

XProtect is a registered trademark of Milestone Systems A/S.

Microsoft and Windows are registered trademarks of Microsoft Corporation. App Store is a service mark of Apple Inc. Android is a trademark of Google Inc.

All other trademarks mentioned in this document are trademarks of their respective owners.

Disclaimer

This text is intended for general information purposes only, and due care has been taken in its preparation.

Any risk arising from the use of this information rests with the recipient, and nothing herein should be construed as constituting any kind of warranty.

Milestone Systems A/S reserve the right to make adjustments without prior notification.

All names of people and organizations used in the examples in this text are fictitious. Any resemblance to any actual organization or person, living or dead, is purely coincidental and unintended.

This product may make use of third party software for which specific terms and conditions may apply. When that is the case, you can find more information in the file **3rd_party_software_terms_and_conditions.txt** located in your Milestone surveillance system installation folder.

About Milestone Systems

Founded in 1998, Milestone Systems is the global industry leader in open platform IP video management software. The XProtect platform delivers powerful surveillance that is easy to manage, reliable and proven in thousands of customer installations around the world. With support for the widest choice in network hardware and integration with other systems, XProtect provides best-in-class solutions to video enable organizations – managing risks, protecting people and assets, optimizing processes and reducing costs. Milestone software is sold through authorized and certified partners. For more information, visit:

www.milestonesys.com.

Sandoval Custom Creations, Inc
2094 Quartz Mountain Drive/
PO Box 155
Larkspur, CO 80118 US
303-918-3878
Shaun@sccicovert.com
www.sccicovert.com

QUOTE

QUOTE # 2030
DATE 04/25/2016

ADDRESS
Fort Worth, TX PD
Attn: Joe Shipp

SHIP TO
Fort Worth, TX PD
Attn: Joe Shipp

Please detach top portion and return with your payment.

ACTIVITY	QTY	RATE	AMOUNT
Canon VB-H43 Canon VB-H43 IP PTZ network camera [THIS QUOTE IS FOR A QUANTITY OF 25 OR MORE UNITS]	1	1,925.00	1,925.00
Canon VB-M50B Canon VB-M50 [THIS QUOTE IS FOR A QUANTITY OF 25 OR MORE UNITS]	1	2,525.00	2,525.00

Thank you for the opportunity to quote your surveillance needs.
[THIS QUOTE IS FOR A QUANTITY OF 25 OR MORE UNITS]

TOTAL **$4,450.00**

Accepted By

Accepted Date

KEYW Engineering
SAMURAI

17 APR 2013

SAMURAI is a miniature, Wi-Fi direction finding solution capable of detecting and measuring the signal strength of any 802.11a/b/g/n device in both the 2.4 GHz and 5 GHz bands. This handheld receiver builds on the previous generations of related handheld receivers with over one thousand devices in service worldwide. The radio is controlled and monitored via a Bluetooth data link to an Android application operating on select mobile phones such as the Samsung Galaxy Ace.

Capabilities:

- Close-range **direction finding** tool using received signal strength indication (RSSI) bar graph and numerical value (dBm) with 90 dB of dynamic range.
- **Traffic generation** techniques may be selected to assist in direction finding.
- **Access Point Scan mode** scans all channels and displays Access Points (AP) without transmitting data – (Includes AD-HOC and hidden APs).
- **MAC Monitor mode** displays devices on a selectable channel or associated with a selectable AP (including AD-HOC and hidden APs).
- **Internal GPS Receiver** – PCAP files are tagged with GPS information for survey purposes.
- Device details including associated AP MAC/SSID, type, vendor, group cipher, pair cipher and authentication.
- Expanded channel range covers unique European and Japanese standards.
- Devices can be added to a **Watch list** using the handheld GUI, transferred as a file via USB or imported from the SD Card.
- Packets can be collected in the industry standard **PCAP** file format for later upload to a PC and analysis using tools such as Wireshark.
- **SD Card slot** for external storage of PCAP files. SD Card also accessible via USB mass storage.
- Audible feed back during direction finding. Audio tone based on the measured signal strength of the target device, increasing frequency as signal strength increases.
- Audio is available using wired earphone and over the air via an internal FM transmitter.
- Vibration alert for indication of Watchlist list hit.
- Adjustable date/time – keeps time when powered off.
- External antenna connections (SMA)
    - 2 System antennas for MIMO operation
    - 1 GPS antenna
- Water resistant, glass reinforced polymer housing with a sturdy lanyard point, connections for Audio, USB and External Antennas
- Internal rechargeable battery with battery level indicator
    - > 4 hours of operation
- Dimensions: 3.65” x 2.5” x 0.75” inclusive of antennas

KEYW Engineering
7740 Milestone Parkway, Hanover, MD, 21076
443-270-5295 www.keywcorp.com

For additional information, please contact:
EIGProducts@keywcorp.com

KEYW Engineering
SAMURAI

17 APR 2013

Accessories include:

- 2x Dual Band Wi-Fi stub antennas
- 1x Dual Band body wearable patch antenna
- 2x High current power supplies for fast battery charging
    - Universal AC and 12/24VDC automotive power
- 2x USB power supplies
    - Universal AC and 12/24VDC automotive power
- USB cable for transferring files
- USB to Micro USB phone cable
- Wired ear bud headset (Motorola cell phone style)
- 2.5mm to 3.5mm adapter (for use with standard audio headphones)
- Adjustable Lanyard
- Pelican 1400 case with custom fitted foam insert
- Android Handset Controller (Samsung Galaxy Ace or equivalent)
- SAMURAI Wi-Fi Detector

These materials are controlled by the International Traffic in Arms Regulations, 22 C.F.R. Parts 120 - 130, and require an export license from the U. S. Department of State prior to transfer to a foreign person or foreign destination. If these materials are exported or otherwise retransferred without the necessary license(s) or in violation of the terms or conditions of any export license, recipient shall indemnify and hold harmless KEYW, its employees and parents, its and their successors and assigns, from and against any and all liability or harms, including attorney fees, arising therefrom.

SAMURAI Kit Price $8,000

(KEYW PN 201030-001)

KEYW Engineering
7740 Milestone Parkway, Hanover, MD, 21076
443-270-5295 www.keywcorp.com

For additional information, please contact:
EIGProducts@keywcorp.com

THE KEYW CORPORATION

SAMURAI

User Guide

9/30/2015

SAMURAI USER GUIDE (v2.1)

WELCOME

SAMURAI is a miniature, Wi-Fi direction finding solution capable of detecting and measuring the signal strength of any 802.11a/b/g/n device in both the 2.4 GHz and 5 GHz bands. This handheld receiver builds on the previous generations of related handheld receivers with over one thousand devices in service worldwide. The radio is controlled and monitored via a Bluetooth data link to the Wi-Fi Remote Control (WRC) Android application operating on select mobile phones.

While scanning for networks and stations, SAMURAI is a passive device that is virtually undetectable. When forcing a station to generate traffic for enhanced Direction Finding, the SAMURAI maintains its stealth presence by spoofing the MAC address of the station's associated access point (AP). Several methods of generating traffic are implemented to minimize the signature of the device while performing its mission.

SAMURAI USER GUIDE (v2.1)

Table of Contents

SAMURAI USER GUIDE (v2.1)

Revision History

4/9/2013 – Release for SAMURAI RC Version 1.0.0 and Firmware 1.0.0

5/3/2013 – Release for SAMURAI RC Version 1.1.0 and Firmware 1.1.0

- Added section for FM Radio and updated Diagrams to reflect FM in the status bar.
- Added section for AP Scan menu options.

5/21/2013 – Release for SAMURAI RC Version 1.2.0 and Firmware 1.2.0

- Added section for PCAP Antenna settings.
- Added description of STIM methods.

9/30/2015 – Release 2.1

- Deprecated SAMURAI RC Android app. Now remotely controlled by the WRC Android app.
- Encrypted Bluetooth communication with the WRC app.
- Added MAC Capture feature
- Added Probe Request screen
- Added Friendly and Target watch list categories
- Added SSID watch list type
- Added Survey of APs, or APs and Stations
- STIM method options
- Extended color coding by Station type
- Updated Status Bar to show selected channel
- Added Unassociated STIM method
- Improved performance
- Fixed bugs

Definition of Terms

AP – Access Point

CTS – Clear To Send

DF – Direction Finding

MAC – Media Access Control

PCAP – Packet Capture

PPI – Per-Packet Information

SD Card – Secure Digital Memory Card

Spoof – To impersonate or take on the identity of another Wi-Fi enabled device

SSID – Service Set Identifier

Station – A wireless device such as smartphone, laptop, etc.

STIM – Stimulate target by generating traffic to the target.

TIM – Traffic Indication Map

TPC – Transmit Power Control

RSSI – Received Signal Strength Indicator

RTS – Request To Send

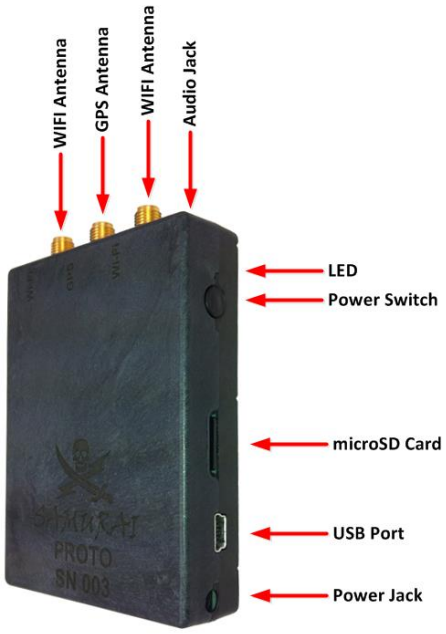
Watch List – List of target names and MAC addresses

WRC – Wi-Fi Remote Control

SAMURAI USER GUIDE (v2.1)

Get Started

Buttons and Connections on the SAMURAI



SAMURAI

Diagram 1

Turning the Device ON and OFF

Locate the POWER button on the right side of the device.

Press the POWER button to turn the device ON. The device will give a quick vibe to indicate it is on. The LED will also flash.

There are two ways to power the device OFF.

- Press and hold the POWER button for ~5 seconds. The device will give a quick vibe and the LED will go out.
- From the WRC app on the Android phone:
  - "Settings and Commands" from the main menu
  - "Device Commands"
  - "Shutdown"

Diagram 2

In the event the device locks up, press and hold the Power Button for 30 sec.

SAMURAI USER GUIDE (v2.1)

Charging the Device

There are two ways to charge the SAMURAI.

- Connect the supplied AC/DC adapter. The battery icon will display a charging icon at the top of the WRC app screen if the device is charging properly.
- The USB port will also charge the device.

Diagram 2a

The unit ships with an AC wall adapter and a DC car charger.

The expected battery life for normal usage is 4-5 hours.

Unit LED Color Information

LED Indication	Description
Off (unlit)	Unit is OFF
Alternating GREEN-BLUE-RED	Unit is charging while the unit is powered ON
Solid YELLOW	Unit is charging while the unit is powered ON and temperature is high
Flashing GREEN	Unit is ON and battery fully charged
Flashing BLUE	Unit is ON and battery level is low
Flashing RED	Unit is ON and battery level is critically low
Flashing YELLOW	Unit is ON and temperature is high
Flashing WHITE	Unit is upgrading
Solid RED	Unit is powering OFF
NOTE: LED is located above the power button	

Diagram 2b

External Audio Jack

A standard set of headphones are included in the kit. The Audio Jack is located on the top of the SAMURAI next to the antennas as shown in Diagram 2c.

Diagram 2c

NOTE: Any Motorola cell phone headset can be used.

NOTE: A 2.5mm to 3.5mm plug adapter is also included in the kit to allow any stereo headset to be used with the device.

SAMURAI USER GUIDE (v2.1)

Locating the Serial Number

The unit serial number is etched into the front at the bottom of the device as shown in Diagram 2d.

The serial number can also be found at the top of the WRC app.

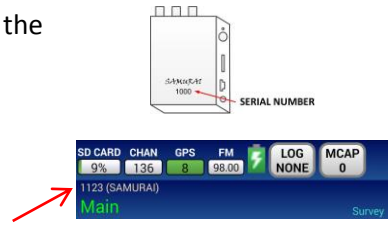


Diagram 2d

External Antenna Connectors

SAMURAI is equipped with three SMA style antenna connectors. The SAMURAI kit includes two Wi-Fi antennas and one GPS antenna. The operator may also use any 2.4/5GHz third party antenna.

NOTE: Only connect Wi-Fi 1 when using included body worn antenna OR optional Wi-Fi Handheld antenna. Wi-Fi 2 will be left open/unused.

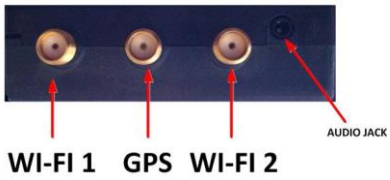


Diagram 2e

Accessing Internal Drives

If connected properly to a computer, the SAMURAI will show up as two removable drives named “SAM-####” (where #### is the unit serial number) and “SD-####” (this name may be different for user supplied SD Cards).

“SAM-####”: This drive contains two directories:

1. UpgradePackages – Used for field upgrades (see page 8).
2. Watchlists – Used to manually manage the watchlist file (watchlist.csv). Only one watchlist file is allowed in this directory. The watchlist file contains an explanation of the file format and includes examples.

“SD-####”: This drive is the removable SD Card. This drive contains two directories:

1. Pcaps – Contains standard PCAP files. The operator can delete/remove PCAP files when no longer needed. PCAP files will be split if they exceed 50MB.
2. MacCaps – Contains files recorded by the MAC Capture feature. This feature is accessible only via the WRC app. The operator can delete/remove MAC Capture files when no longer needed.

Note: Always “Remove Safely” both drives of the SAMURAI properly before disconnecting the USB cable.

Remote Control

Refer to the WRC User Guide for details.

SAMURAI USER GUIDE (v2.1)

Field Upgrade Instructions

1. Connect SAMURAI to computer via USB cable.

   If connected properly the SAMURAI will show up as two removable drives named “SAM-####” (where #### is the unit serial number) and “SD-####” (this name may be different for user supplied SD Cards).

2. Copy the SAMURAI upgrade package file to the “UpgradePackages” folder on the “SAM-####” drive connected in step 1.

3. Rename the file in the “UpgradePackages” folder to **samurai.upgrade.pkg.**

4. Once the file copy/rename has completed, SAFELY REMOVE both drives from the computer.

   - Windows - right click and select EJECT
   - Mac - drag the drive to the trash bin to eject the drive

5. Once safely ejected, the upgrade process will begin automatically. The USB cable can now be disconnected.

   This process can take a few minutes. The SAMURAI’s LED will be blinking white as it upgrades.

6. When the upgrade is completed the SAMURAI will reboot.

Warranty Statement

The KEYW Corporation warrants each new product manufactured to be free from defects in material and workmanship under normal use and service for the warranty period. This warranty is provided to the original end user and is not assignable or transferable. The KEYW Corporation will repair, without charge, any KEYW product which fails due to a defect in material or workmanship within the warranty period. This warranty excludes damage caused by improper operation, testing, repair, modification, alteration, adjustment, installation, or maintenance of the KEYW product. Damage resulting from either accident or neglect is also excluded. The preceding warranty is The KEYW Corporation's only warranty concerning the products, services and any deliverables resulting under this order, and is made expressly in lieu of all other warranties and representations, express or implied, including any implied warranties of fitness for a particular purpose, merchantability, non-infringement or otherwise.

NOTWITHSTANDING ANY OTHER PROVISION OF THIS WARRANTY AND EXCEPT AS OTHERWISE PROVIDED UNDER APPLICABLE LAW, IN NO EVENT SHALL KEYW BE LIABLE FOR INDIRECT, SPECIAL, CONSEQUENTIAL, MULTIPLE OR PUNITIVE DAMAGES, OR ANY DAMAGE DEEMED TO BE OF AN INDIRECT OR CONSEQUENTIAL NATURE ARISING OUT OF OR RELATED TO ITS PERFORMANCE UNDER THE WARRANTY, WHETHER BASED UPON BREACH OF CONTRACT, WARRANTY, NEGLIGENCE AND WHETHER GROUNDED IN TORT, CONTRACT, CIVIL LAW OR OTHER THEORIES OF LIABILITY, INCLUDING STRICT LIABILITY. THE KEYW CORPORATION SHALL NOT BE LIABLE FOR THE LOSS OF ANTICIPATORY PROFITS.

ITAR RESTRICTION

These materials are controlled by the International Traffic in Arms Regulations, 22 C.F.R. Parts 120 - 130, and require an export license from the U. S. Department of State prior to transfer to a foreign person or foreign destination. If these materials are exported or otherwise retransferred without the necessary license(s) or in violation of the terms or conditions of any export license, recipient shall indemnify and hold harmless KEYW, its employees and parents, its and their successors and assigns, from and against any and all liability or harms, including attorney fees, arising therefrom.

SAMURAI USER GUIDE (v2.1)

SAMURAI Kit Contents

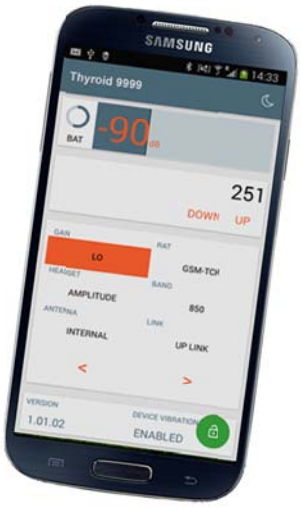
- Pelican 1400 case with custom fitted foam insert
- Android Handset Controller
- SAMURAI Wi-Fi detector
- Adjustable lanyard
- Wired ear bud headset (Motorola cell phone style)
- 2x High current power supplies for fast battery charging
    - Universal AC
    - 12/24VDC automotive adapter
- 2x USB power supplies
    - Dual port universal AC
    - Dual port 12/24VDC automotive adapter
- USB cable for transferring files and charging
- USB to micro USB for charging and upgrading Android phone
- 2.5mm to 3.5mm adapter (for use with standard audio headphones)
- 2x Dual Band Wi-Fi stub antennas
- 1x Dual Band body wearable patch antenna
- 1x GPS stub antenna
- 1x microSD with SD Adapter

KEYW CORPORATION

Universal Remote Control V2

User Guide DRAFT

8/19/2015



Document History

Revision	Date	Description
Initial	19 AUG 2015	Initial Release

Table of Contents

About This Document

- Universal Remote Control V2 mobile application will be referred to as: “URC2”
- The Android device running the URC2 mobile app will be referred to as: “Android”
- The Android Wear Watch will be referred to as: “Watch”
- The KEYW RF Detector will be referred to as: “Remote Device”

To change the settings in the URC2 the operator will tap finger on the field to be changed. The available values for that field will then be displayed.

The URC2 MENU button is accessible on the Android as shown in Figure 1 or Figure 2 depending on the Android model and OS version.

Figure 1

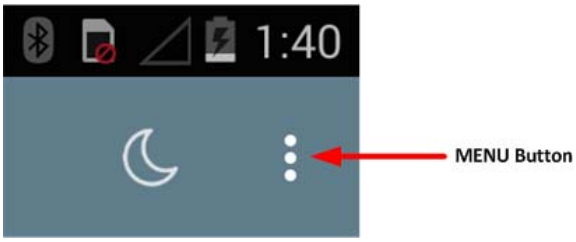


Figure 2

Glossary of Terms

.apk – Android Application Package

App – Application

RAT – Radio Access Technology

Android – Any Android device with the URC2 mobile app installed

RF – Radio Frequency

Remote Device – Any KEYW RF detector being controlled by the URC2 mobile app

Introduction

The URC2 is a tool developed for remotely controlling and monitoring KEYW's line of handheld radio frequency (RF) detectors, including JUGULAR (all versions), CAROTID, THORACIC[1] (all versions), ATRIUM, QUASIMODO[2], and THYROID products. This controller consists of a custom software application running on select Android mobile devices. Communication between the remote control Android and the Remote Device is over a wireless Bluetooth link.

The URC2 mobile application was developed to operate on **Android** (4.4.2 and later) based devices.

Capabilities:

- All main parameters/settings on the Remote Device can be controlled from the Android
- Local control of the Remote Device is fully enabled while connected remotely, with the parameters interactively updated on the Android and Remote Device displays
- Signal Strength (bar graph and numerical value) and GSM, iDEN, LTE DETECT notifications are updated in real time on the Android display
- After initial connection, the two devices will automatically reconnect if the wireless link is lost
- URC2 remembers previously connected Remote Devices and presents them as a list for quick reconnection
- The URC2 can only connect to one Remote Device at a time

Compatible Device Minimum Firmware Versions:

- ATRIUM 1.00.00
- JUGULAR 1.05.00
- JUGULAR2 1.00.01
- JUGULAR3 2.00.00
- JUGULAR4 1.00.00
- CAROTID 1.00.02
- THORACIC 1.00.00
- THORACIC2 1.00.00
- THYROID 1.00.00
- QUASIMODO 1.02.01

[1] KLEER Audio functions not supported by URC2.
[2] KLEER Audio functions not supported by URC2.

Getting Started

Installing the Mobile Application

The URC2 mobile application is installed from an Android Application Package (.apk) file.

If the Android has an earlier version of Universal RC please uninstall it before installing the new version.

Download a copy of the URC2 .apk file from the Software section of https://www.eigproducts.com (registration required) and copy (or email) to the Android.

Tap the icon and follow the onscreen prompts. On some Androids the user may be required to authorize the installation of the URC2.

When the URC2 is started for the first time, the user will be required to pair their Remote Device(s) with the Android. Pressing the "BLUETOOTH SETTINGS" option on this screen (see Figure 3) will open the Android's Bluetooth settings screen.

Figure 3

Note: Please refer to the Android's manufacturer provided user manual for instructions on how to pair a Bluetooth device.

Once a Remote Device has been paired it will appear on the "AVAILABLE DEVICES" list. For each device, the last device identifier (name and serial number) that was connected is displayed for quickly reconnecting.

Remote Device Bluetooth Pairing Code

The Bluetooth pairing code is four zeros (**0000**).

Android Wear (Watch) Pairing/Setup

Download and install the Android Wear mobile application from Google Play. If its already installed verify it is the latest version of the app. See Figure 4 for a picture of the apps' icon.

Figure 4

Tap the Android Wear icon on the Android to start the app.

Follow the onscreen instructions to complete the watch pairing.

- Tap the watch being paired from the list. (Figure 5)
- Follow the onscreen instructions in Figure 5 through Figure 8.
- Once the Watch and the Android have paired successfully, a sync/install will begin. The URC2 watch app will automatically install from the Android to the Watch (Figure 9). This process may take several minutes depending on the number of apps on the Android that support the Watch.
- After the syncing has completed, swipe to the left on the Watch to access the apps menu.
- Scroll down through the list (the apps are sorted alphabetically) until "UniversalRC" appears (Figure 10).
- While the URC2 is running on the Android, tap the icon on the Watch.
- When connected the Watch will display the signal strength in dB exactly as shown on the Android and Remote Device. (**Figure 11**)
- To EXIT the Watch app tap and hold on the screen for ~3 seconds. A red X will appear (as shown in Figure 12).

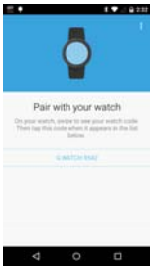


Figure 5

Figure 6

Figure 7

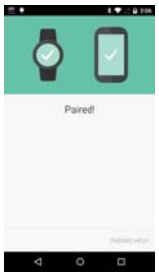


Figure 8

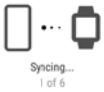


Figure 9

Figure 10

Figure 11

Figure 12

URC2 Graphical User Interface (GUI) Layout

Screen Display Modes

The following figures depict the main URC2 screen in PORTRAIT and LANDSCAPE display modes when a Remote Device is actively connected. When the Android is in LANDSCAPE display mode the tiles will automatically rearrange themselves on the screen (see Figure 14).

Note: The user may need to scroll up and down to see the entire screen.

PORTRAIT

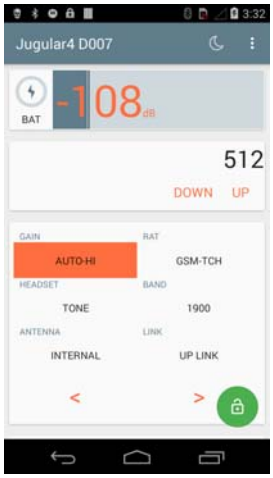


Figure 13

LANDSCAPE

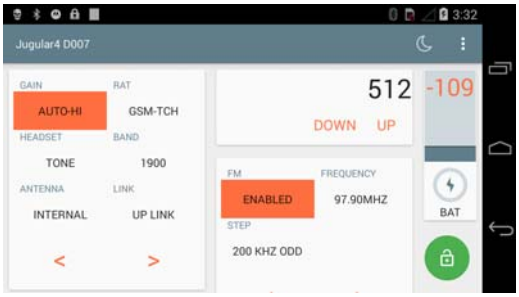


Figure 14

Main Screen Tiles

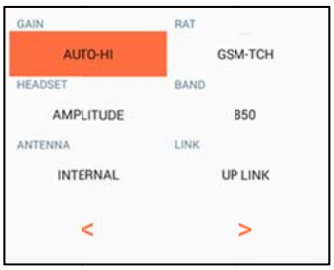
- DEVICE TYPE & SERIAL NUMBER
- DAY/NIGHT MODE SELECTOR

- BATTERY STATUS AND CHARGE INDICATOR

- SIGNAL STRENGTH W/DETECT INDICATOR

- CHANNEL NUMBER DISPLAY AND SELECTOR

- DEVICE SETTINGS

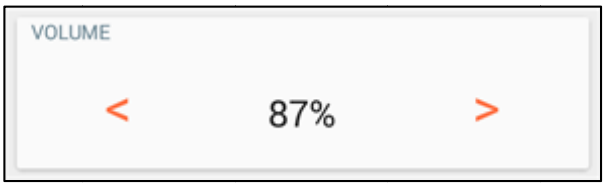


- FM SETTINGS

This tile is not available on all Remote Devices

- VOLUME SETTINGS

This tile is not available on all Remote Devices



- CONNECTED DEVICE VERSION
- DEVICE VIBRATION STATUS

- DEVICE SETTINGS LOCK/UNLOCK

Main Screen Fields

The following is a description of each tile's selectable parameters.

Device Serial #

The currently connected device type and serial number are displayed.

Toggle Day/Night Mode

When NIGHT mode is selected (by pressing the moon icon) the background changes to black with red text. To toggle back to DAY mode touch the icon again (it will now look like a sun).

Figure 15

Battery Status and Charge Indicator

The battery status indicator shows the connected device's battery charge level. If the connected device is being charged via USB, a lightning bolt icon is displayed (see Figure 16) in the center. When the battery is fully charged the circle indicator will be 100% dark.

Figure 16

Signal Strength w/DETECT Notification (LTE, GSM, and iDEN only)

The signal strength meter provides a visual scale of the signal strength level. The signal strength level is shown in dB. The single dark vertical bar to the far right indicates the highest signal strength detected. To reset simply tap the signal strength bar.

Figure 17

Note: The DETECT notification indicates only when a LTE, GSM, or iDEN detect is active.

Channel Number

The channel number for the selected mode and band is displayed. Only the channels supported in the selected frequency band will be displayed. Tap DOWN/UP to change the channel. Also, tapping the channel number will display a number pad for easier channel number entry.

Figure 18

GAIN (sensitivity)

The Gain setting for the connected Remote Device is displayed.

Options are:

- LO – Close Range
- HI – Long Range
- AUTO-HI/AUTO-LO – Allows Remote device to choose

HEADSET

The Remote Device's audio mode for the connected device is displayed. This mode affects the sound coming from the headset connected to the Remote Device's audio jack. The two supported audio modes are TONE and AMPLITUDE.

Note: Not all Remote Devices support all modes. Only the supported modes will be displayed as an option.

Antenna
(Not selectable on all Remote Devices) This field shows the antenna selection of the device. The two supported modes are INTERNAL and EXTERNAL.

Note: On some Remote Devices, the antenna may be fixed as either internal or external.

Radio Access Technology (RAT)
(Not all modes are available on older Remote Devices) The most common modes are listed below. The URC2 will only display the modes supported by the connected Remote Device.
LTE UMTS CDMA GSM (TCH and SDCCH) iDEN

BAND
(Not all bands are available on older Remote Devices) The URC2 will only display the bands supported by the connected device.

LINK
(Not available on all Remote Devices) The LINK setting for the connected Remote Device is displayed. Note that on some devices the LINK is not selectable and fixed to "UP LINK".

VOLUME
(Not available on all Remote Devices) The VOLUME setting controls the volume of the connected device.

FM
(Not available on all Remote Devices) The FM setting allows the device to broadcast its audio to a nearby FM radio.
FM: ENABLED or DISABLED
Step: Specifies the frequency step as 50 kHz, 100 kHz, 200 kHz odd, 200 kHz even.
Note: The Standard U.S. setting is 200 kHz odd.
Frequency: Specifies station frequency in MHz.

VERSION
This is the current firmware of the connected Remote Device.

Device Vibration
Displays the current status of the Remote Device's vibe setting. This setting cannot be changed from the URC2 mobile app. It must be set from the Remote Device.

Screen Lock
The screen lock will allow the user to lock the settings to protect from inadvertently changing the settings while operating the device. Slide the green padlock icon up to lock the screen. Slide the red padlock icon up to unlock the screen.


Figure 19

URC2 Settings Menu

The URC2 settings menu is displayed by pressing the MENU button on the Android (see Figure 1 and Figure 2 for location of MENU button). The following setting options are available.

SECURITY

Hide Application Launcher

By checking this box the operator will HIDE the URC2 icon from the Android's application list. To activate the URC2 the user must dial the Launcher Code (as if making a call). The default code is: 1234

Note: The URC2 will however still appear in the Application Manager on the Android.

Hidden Launcher Code

The user may set the launcher code to any number between 4 and 6 digits. The number cannot begin with leading zeros.

AUDIO FEEDBACK

Startup Tone Volume

Slide the volume bar left and right to adjust the URC2's startup volume level.
The default setting is set to mute.

Tone Balance

Slide the balance bar left or right to adjust the tone output between the left and right channels.
The default setting is balanced evenly.

PHONE VIBRATION

Vibe

Slide the ON/OFF switch to enable/disable vibe motor feedback on the Android. When Vibe is set to ON, the advanced vibe settings will operate as they are defined. Also, this Vibe setting is independent of the Remote Device's vibe in the Device Settings, which controls the vibe in the Remote Device.

Figure 20

Advanced Vibe

The Advanced Vibe Settings screen allows control of a background vibe heartbeat tied to the signal level for each individual RAT. The operational concept is the closer the device is to a signal source, the higher the signal level and, hence, the faster the vibe heartbeat. Up to four vibe levels can be individually enabled to vibe at a set heartbeat speed when the signal level is within the range of that vibe level. Individual vibe levels can be disabled to reduce the granularity of the heartbeat.

When the Vibe option is set to ON and the signal level is within the range of one of the four vibe levels, a vibe heartbeat will be active at the specified rate for the following conditions:

1. While the DETECT banner is shown for the LTE, GSM, or iDEN (uplink and downlink) modes
2. All other modes and links for which the DETECT banner is not displayed

BRIGHTNESS

Brightness Override

When enabled the Android's default brightness levels will be overridden by the operator's selection on the "Light Mode" and "Dark Mode" sections below.

Light Mode

Slide the brightness indicator left or right to adjust brightness in Light Mode.

Dark Mode

Slide the brightness indicator left or right to adjust brightness in Dark Mode.

BUILD

Version

Current version of the URC2 installed on this Android device.

Identifier

Unique identifier of this handset, used for debug purposes only.

Status

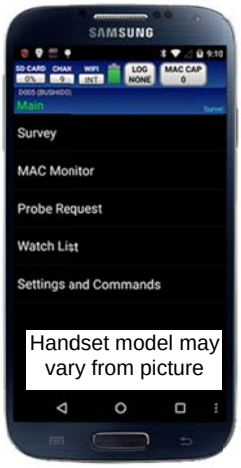
Status of the URC2 app – Release / Development

KEYW Engineering
Wi-Fi Remote Control (WRC)

18 AUG 2015

The **Wi-Fi Remote Control (WRC)** mobile application is a tool developed for remotely controlling and monitoring KEYW's Wi-Fi radio frequency (RF) receivers BUSHIDO & SAMURAI. This controller consists of a custom mobile application running on select Android mobile devices. Communication between the Android device and the RF receiver is over a wireless Bluetooth link.

The mobile application was developed to operate on **Android** (4.2 and later) devices.



Capabilities:

- MAC Capture – capture, mark (multiple times) and save data to a file.
- MAC Compare – compare data in real-time with the file saved from the MAC Capture.
- View Probe Requests – view SSIDs being probed and the MACs doing the probing.
- View SSID watch list history – view historical data for SSID watch list entries.
- After initial connection, the remote device will automatically reconnect if the wireless link is lost.
- WRC remembers the serial number of previously connected devices of each type for quick reconnection.
- All main parameters/settings on the remote device can be controlled from the Android device.
- The WRC mobile application can only connect to one remote device at a time.
- The application is not locked to a specific Android device and activation is not required.

Future Capabilities:

- Ability to direction find (DF) non-associated Wi-Fi devices.
- SAMURAI support will be available Q4 2015.

Compatible Device minimum firmware versions:

- BUSHIDO 2.0.0
- SAMURAI 2.0.0

Wi-Fi Remote Control Price

FREE for existing customers with their own Android device
Download from www.eigproducts.com

$500 for software pre-loaded and tested on an Android handset
(KEYW PN 201540-002 WRC software with a Motorola Moto G or equivalent handset)

KEYW Engineering
7740 Milestone Parkway, Hanover, MD, 21076
443-270-5295 www.keywcorp.com

For additional information, please contact:
EIGProducts@keywcorp.com

THE KEYW CORPORATION

WIRC
I-FI REMOTE CONTROL

User Guide

9/30/2015

WRC USER GUIDE (v1.2)

Table of Contents

WRC USER GUIDE (v1.2)

Revision History

6/30/2015 – Initial Release 1.0.0

9/30/2015 – Release 1.2

- Added SAMURAI support
- Added Unassociated STIM method
- Fixed bugs

Definition of Terms

AP – Access Point

CTS – Clear To Send

DF – Direction Finding

MAC – Media Access Control

OUI – Organizationally Unique Identifier

PCAP – Packet Capture

SD Card – Secure Digital Memory Card

Spoof – To impersonate or take on the identity of another Wi-Fi enabled device

SSID – Service Set Identifier

Station – A wireless device such as smartphone, laptop, etc.

STIM – Stimulate target by generating traffic to the target.

TIM – Traffic Indication Map

TPC – Transmit Power Control

RSSI – Received Signal Strength Indicator

RTS – Request To Send

Watch List (WL) – List of target and friendly names with MAC addresses and/or SSIDs

WDS – Wireless Distribution System

WRC – Wi-Fi Remote Control

WRC USER GUIDE (v1.2)

Get Started

Features only available in WRC

- MAC Capture – capture, mark (multiple times) and save data to a file
- MAC Compare – compare data in real-time with the file saved from MAC Capture
- View Probe Requests – view SSIDs being probed and MACs doing the probing
- View SSID watch list history – view historical data for SSID watch list entries

How to install the WRC mobile app on Android device

See the Field Upgrade Instructions on page 35.

Starting the WRC mobile app for the first time

After installation the WRC app icon will display on the Android Handset. This will be in Apps or a short cut can be created by dragging the icon out to the desired home screen as shown on Figure 1.

Press the WRC icon to start the app.

Figure 1

Pairing the Device with a Phone

Figure 2 shows the "Connect To:" screen. This is the screen displayed immediately after starting the WRC app. It will display the last device for BUSHIDO and SAMURAI that was connected (if any).

Select the last device that was connected or select "Search for devices."

The app will display any/all BUSHIDO and SAMURAI devices previously paired and found during discovery (Figure 3).

Select the device to be paired with this phone.

Serial Number: Select the device's Serial Number from the list. The serial number of a BUSHIDO is located on the upper back of the unit. The serial number of a SAMURAI is located on the face of the unit. Serial numbers are four digits.

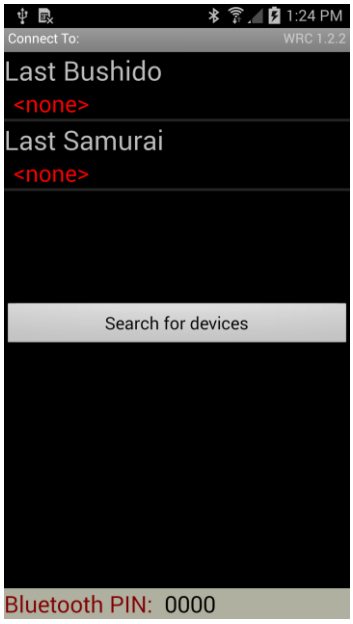


Figure 2

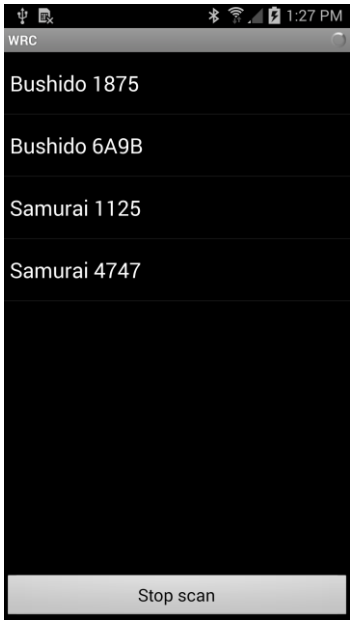


Figure 3

The first connection to a device requires entering the Bluetooth PIN code (Figure 4). Enter the Bluetooth pairing code (0000) and press OK. Note that the Bluetooth PIN is displayed at the bottom of Figure 2.

Data over the Bluetooth link is encrypted.

NOTE: WRC cannot communicate with SAMURAI firmware version 1.x.

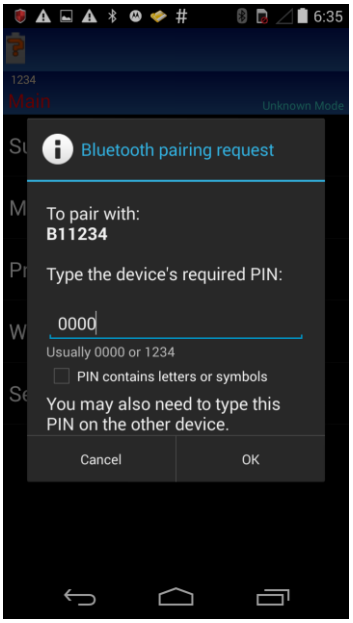


Figure 4

Using the WRC

Toolbar Icons

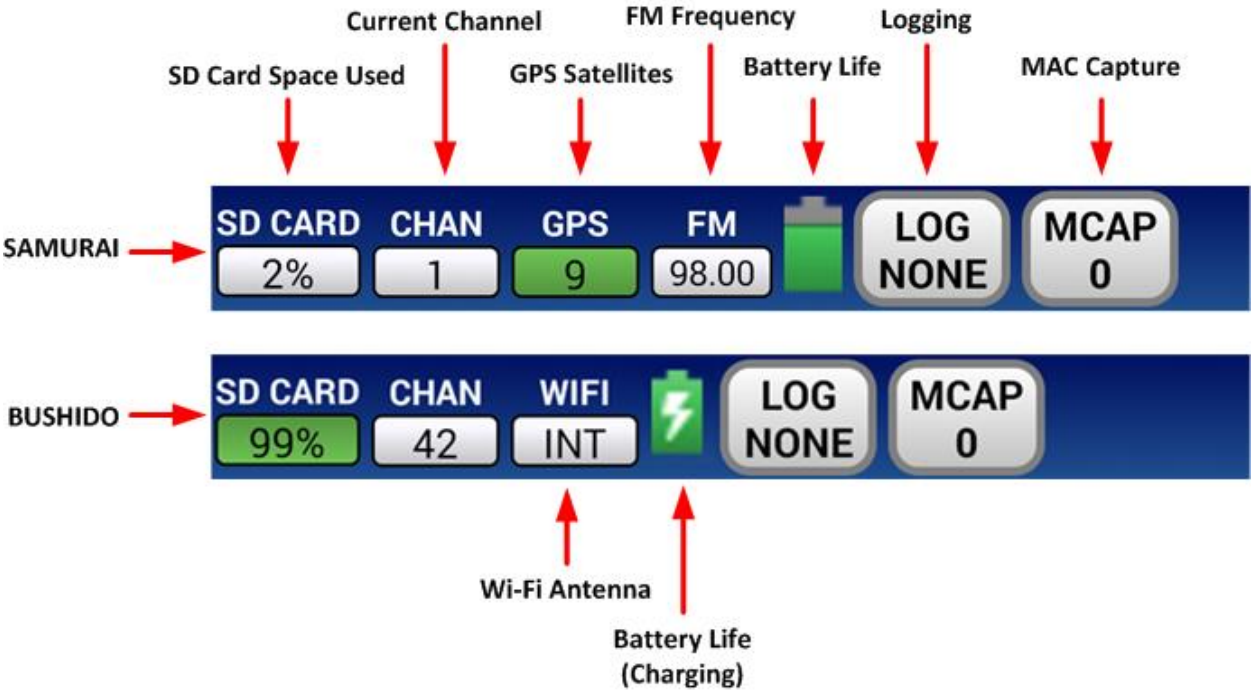


Figure 5

SD CARD percentage of card memory used is displayed.	**CHAN** is the current channel the device is set to.	**GPS** is the number of visible satellites (SAMURAI only). Red = no satellites Yellow = 3 or less satellites Green = 4 or more satellites
FM frequency (SAMURAI only). Green = transmitting White = not transmitting	**WIFI** indicates whether the device is using internal or external antenna (BUSHIDO only).	**BATTERY** icon will display the battery life of the connected device. It will also indicate when charging. When the WRC app is first connecting, the icon below is shown until the battery status is known. 
LOG button will indicate whether logging is enabled (PCAP) or not (NONE). The indicator turns yellow when logging. Press the button to toggle logging.	**MCAP** button indicates number of unmarked MACs detected during capture. See below for details.	

MCAP Button

Press the MCAP button on the toolbar to start, mark, or stop a capture session. Figure 6 shows the MAC Capture Start screen which is displayed when pressing the MCAP button while it's grey (OFF). The operator can either use the previous file name prefix ("mac_cap" in Figure 6) or type in something else. The file name will be appended with a timestamp and the ".csv" file extension.

Once the Start button is pressed, the MCAP button will turn green. Data will be captured in the device's internal memory in an unmarked state. The count of unique MACs detected since pressing Start is shown on the MCAP button.

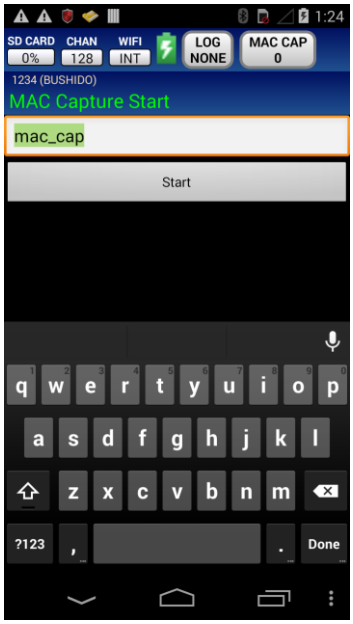


Figure 6

To mark the data with text, press the MCAP button again, while it is green, and Figure 7 will be shown. The red circle denotes the file name created when MAC Capture was started. The operator can either use the previous mark text ("location 1" in Figure 7) or type in something else. The mark text will be appended with a timestamp. Press the Mark button to perform the mark and continue collecting more data, or press the Stop button to perform the mark and stop collecting data. When marked, the data is then saved to the file. The file can contain multiple marks.

The file containing the marked data is now located on the device (BUSHIDO/SAMURAI - not the phone). To access the file, connect the device to a computer via USB, open the drive labeled "BUSHIDO" or "SD-####" (SAMURAI) and open the directory "MacCaps". The file header with an example entry is shown below (comma separated values):

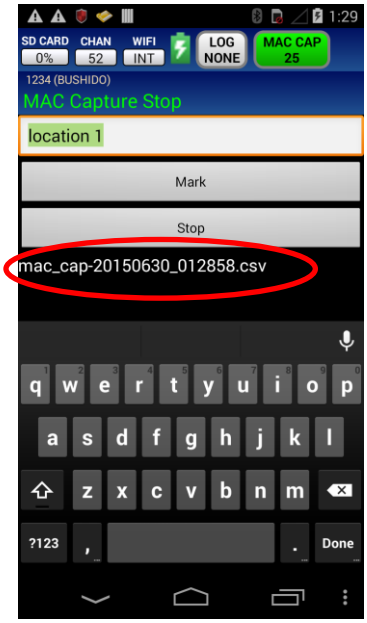


Figure 7

```
# mac, type, time first seen, time last seen, first seen rssi, last seen rssi, pkt count, mark
10:a5:d0:a1:b2:c3,st,2015-06-30 01:29:15,2015-06-30 01:32:37,-70,-65,4,location 1-20150630_013319
```

The "mac" field is the MAC address for the source device. The "type" field can be "st" for Station, "ap" for AP, or "adhoc" for Ad-Hoc. The "time first seen" and "time last seen" fields are time stamps, which can be the same if only one packet was detected for that MAC. The "first seen rssi" and "last seen rssi" fields are the RSSI values. The "pkt count" field is the number of packets detected for this MAC. The "mark" field is the mark text with the time stamp entered by the operator.

Main Menu

The WRC Main Menu allows the operator to select the function of the attached device (Figure 8).

Note that, depending on the Android phone used, there may be an actual MENU button on the phone, or there may be a 'three-dot' icon on the screen. Some phones may require that the RECENTS button be pressed and held to act as the MENU button, while others simply require a press. This document shows the 'three-dot' icon.

When connecting to a SAMURAI, the Main Menu will include a GPS menu item.

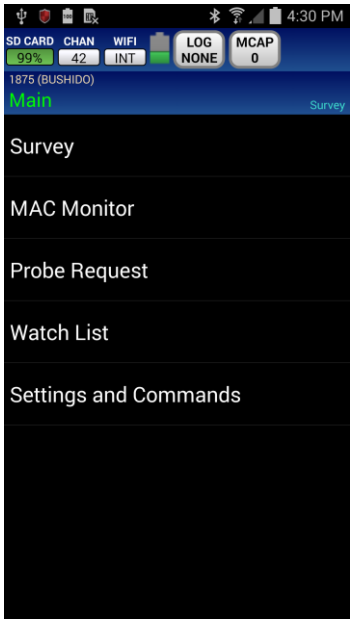


Figure 8

Pressing the MENU button from the Main Menu displays the Options menu. Select Version Info to show the Version Information for the WRC App and connected device (Figure 9).

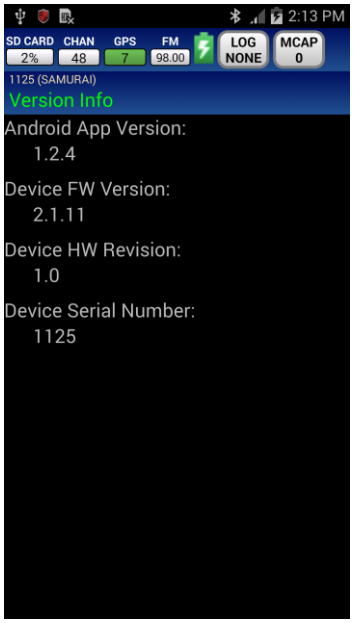


Figure 9

Survey

Survey will perform a scan on all 802.11 Access Points and Stations (including Ad-hocs) in range displaying SSID, Channel, and RSSI.

NOTE: The column sorting is changed by pressing the column headers. For example, to sort on RSSI press on RSSI, press it a second time to reverse sort order.

NOTE: If an AP is hidden the WRC will display the MAC address (no SSID). It's possible to determine the hidden SSID by selecting "Monitor AP MACs" (see page 33) and listening to the traffic for a while.

NOTE: Instead of transmitting probe request packets, the system passively listens for packets, making it invisible to the network.

Security indicators are:

- Gold Lock - Encrypted (non-WEP)
- Gold Lock w/ 'H' - Encrypted/Hidden (non-WEP)
- 'H' - Clear/Hidden
- Blue Lock - WEP Encryption
- Blue Lock w/ 'H' - Encrypted/Hidden (WEP)
- Grey Lock - Unknown security
- No Icon - Clear (no encryption)

Watch list targets are highlighted yellow.

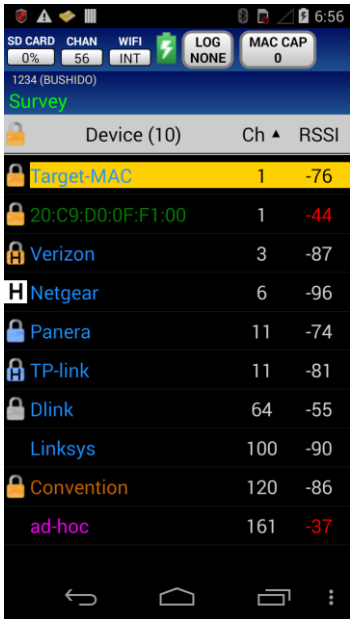


Figure 10

Pressing the phone's MENU button will access additional features (Figure 11).

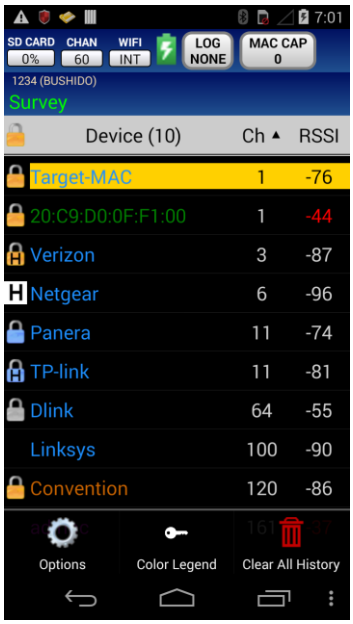


Figure 11

Options

- Device Filters
  - AP/Adhoc only – Survey will only show APs and Adhocs if checked. When unchecked, all devices are shown.
  - MAC compare – Survey will filter based on the following selections:
    - Previously detected – Only show devices that have been captured and marked in the current MAC Capture file since the device has been powered on (see MCAP Button on page 7).
    - Newly detected – Only show devices that have not been captured and marked in the current MAC Capture file since the device has been powered on (see MCAP Button on page 7).

- App Filters
  - Age Out – After 40 seconds of no activity, target will no longer be displayed.
  - Show (encryption) – Shows Clear, Encrypted, or both Clear and Encrypted devices.
  - Show (visibility) – Shows Visible, Hidden, or both Visible and Hidden devices.

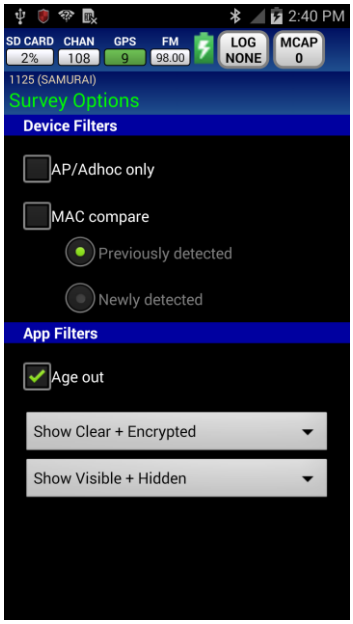


Figure 12

Color Legend

- Green – Station with known associated AP
- Yellow background – Station or AP on Watch List
- Purple – Ad-hoc device
- White – Station with unknown associated AP
- Blue – AP
- Orange - WDS
- Red – unknown device

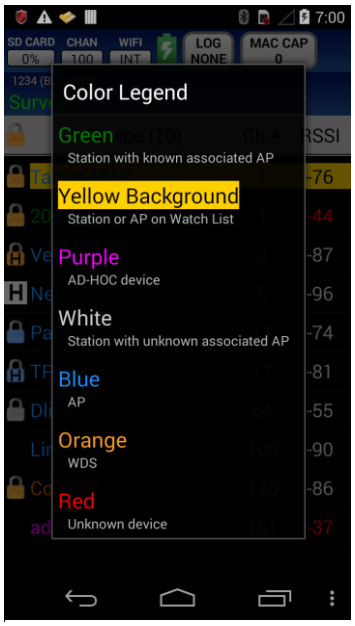


Figure 13

Clear All History

- Press the Clear All History button to clear all Survey data from the phone.

MAC Monitor

MAC Monitor displays all Wi-Fi devices on a specific channel.

Use the channel bar at the bottom of the screen to select channel.

Press the channel number in the middle (red circle on Figure 14) to access a keypad (Figure 15).

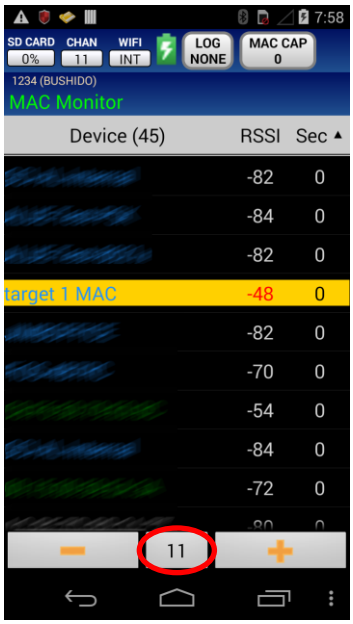


Figure 14

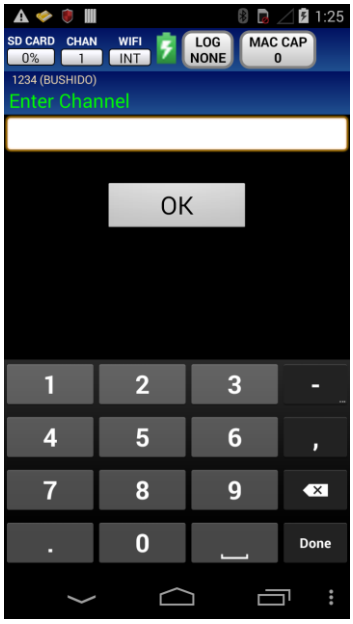


Figure 15

Pressing the phone's MENU button will access additional features. (Figure 16)

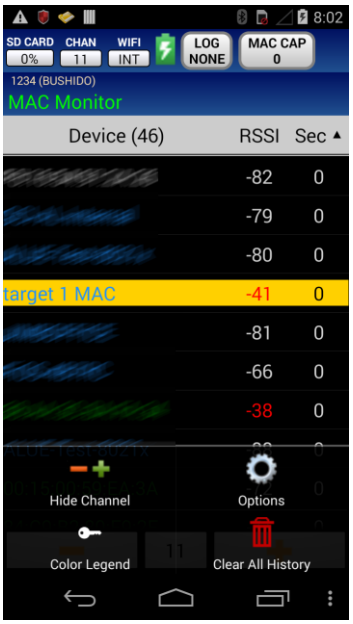


Figure 16

Show/Hide Channel

- Press the Show/Hide Channel button to show/hide the Channel Bar buttons displayed at the bottom of the screen.

Options

- App Filters – Check to enable
  - Show Stations
  - Shows APs
  - Show Hidden Aps
  - Show AD-HOC
  - Age Out – After 40 seconds of no activity, target will no longer be displayed.

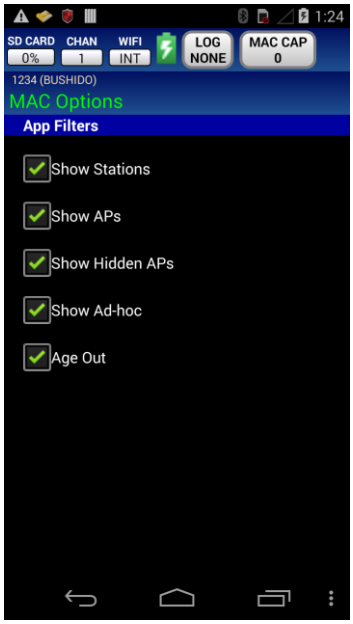


Figure 17

Color Legend

- Green – Station with known associated AP
- Yellow background – Station or AP on Watch List
- Purple – AD-HOC device
- White – Station with unknown associated AP
- Blue – AP
- Orange - WDS
- Red – unknown device

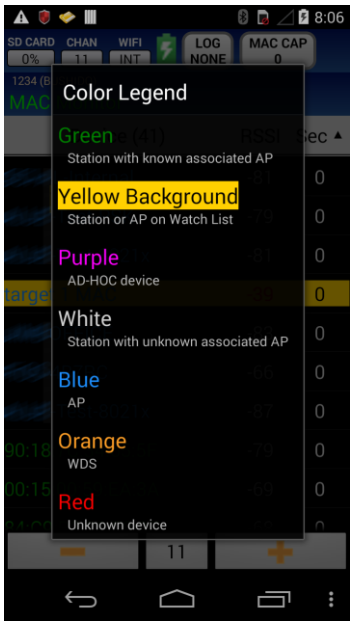


Figure 18

Clear All History

- Press the Clear All History button to clear all collected data from the phone.

Probe Request

The Probe Request screen (Figure 19) displays all probe requests detected. Each entry shows the SSID being probed, the channel where the probe request was detected, the number of MACs that have probed the SSID, and the number of seconds since the last detected probe request (stops incrementing at 999 seconds).

Pressing the phone's MENU button will access additional features as shown at the bottom of Figure 19.

Figure 19

Show/Hide Channel

- Press the Show/Hide Channel button to show/hide the Channel Bar buttons displayed at the bottom of the screen.

Clear All History

- Press the Clear All History button to clear all collected data from the phone.

Context Menu

Figure 20 shows the context menu after pressing and holding an SSID. See View Probe Requests on page 31 and Add Watch List on page 30 for details.

NOTE: A single click on an SSID is a quick way to select View Probe Requests.

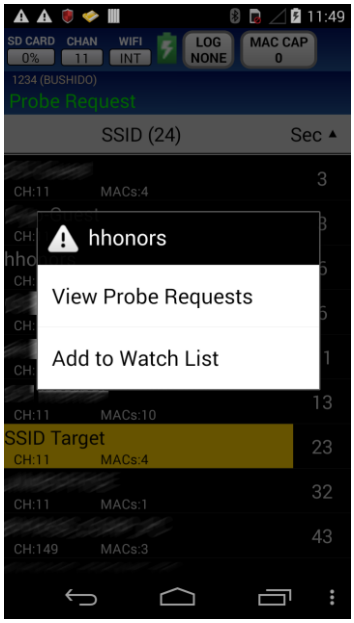


Figure 20

Watch List

The Watch List screen (Figure 21) displays all watch list items.

The letters “T” and/or “F” will display to identify the watch list item as a “Target” or “Friendly” device.

Pressing the phone’s MENU button will access additional features as shown at the bottom of Figure 21.

NOTE: Maximum number of targets on Watch List:
BUSHIDO – 100
SAMURAI – 2048

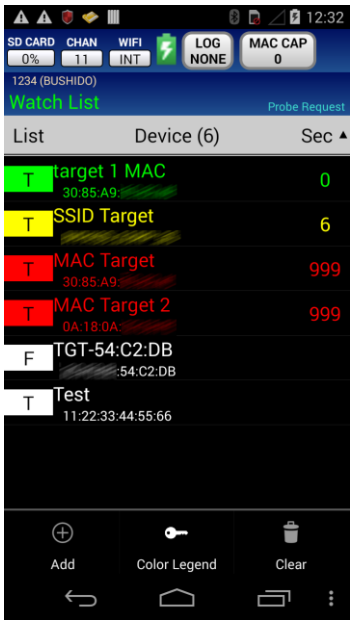


Figure 21

Add

- Choose the watchlist type (MAC or SSID or both) by checking the appropriate boxes (Figure 22).
- If Include MAC is checked, enter the Alias and MAC without colons (Figure 22).
- If Include SSID is checked, enter the Alias and SSID.
- Select Target or Friendly category.
- Press OK to add to the watchlist.

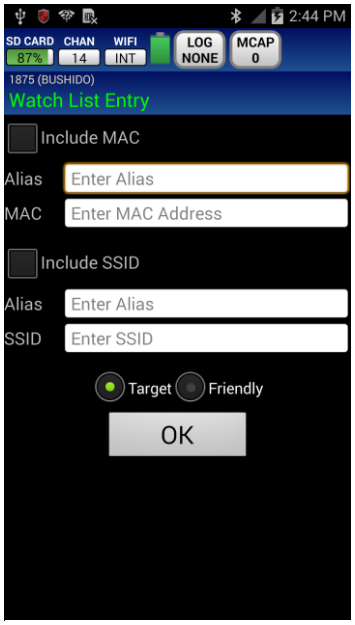


Figure 22

Color Legend

- *Green*: The target has been detected within the last 5 seconds
- *Yellow*: The target has been detected 6-10 seconds ago
- *Red*: The target has been detected more than 10 seconds ago
- *White*: The target has not been detected since connecting to the device

NOTE: Friendly watchlist entries will always be white.

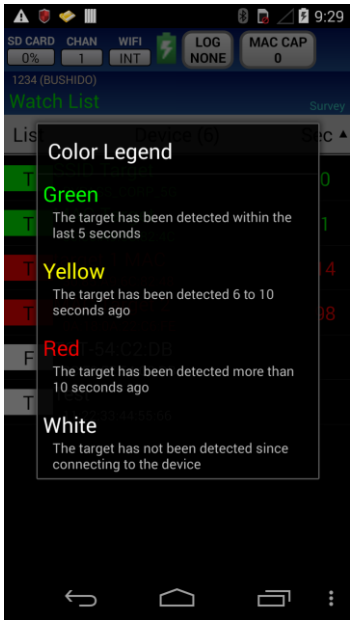


Figure 23

Clear

- Select Target, Friendly, or Both lists to clear

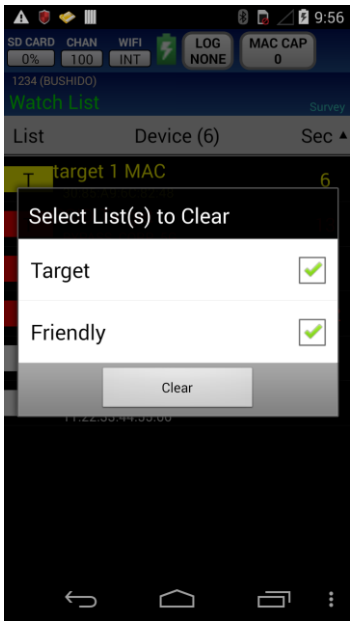


Figure 24

Context Menu

Figure 25 shows the context menu after pressing and holding a MAC entry. See DF (Direction Finding) on page 27 and View Probe Requests on page 31 for details. The menu options Edit and Delete are described below.

Figure 26 shows the context menu after pressing and holding a SSID entry. The View History Option opens the SSID Watchlist History. See page 32 for details.

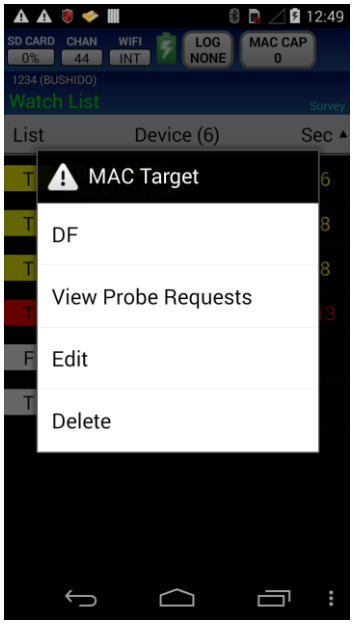


Figure 25

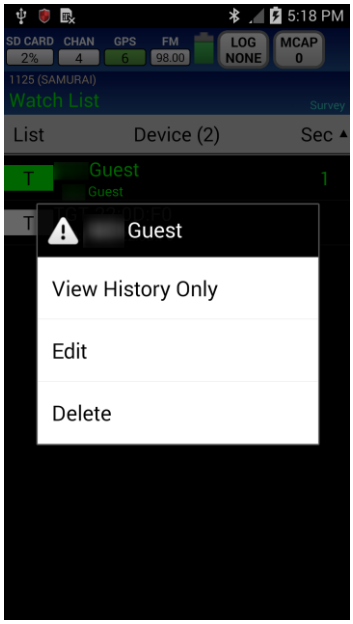


Figure 26

Edit

Figure 27 shows the Watch List Entry screen to edit a MAC entry.

Figure 28 shows the Watch List Entry screen to edit an SSID entry.

NOTE: Some predictive text keyboards add an extra SPACE character at the end.

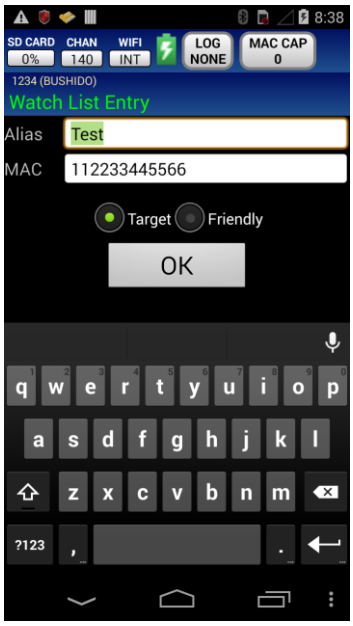


Figure 27

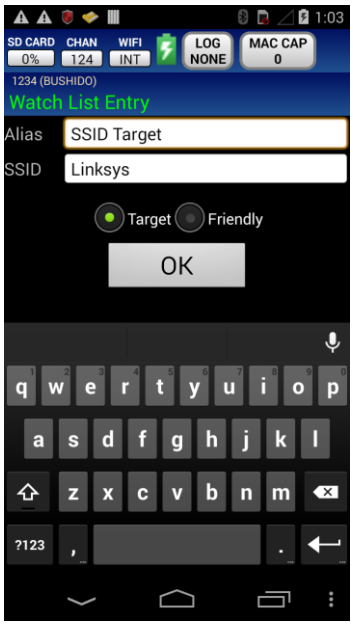


Figure 28

Delete

Removes the entry from the Watchlist.

WARNING! There is no confirmation dialog for Delete. Pressing Delete immediately deletes the Watchlist entry.

GPS (SAMURAI Only)

All current GPS information is displayed on the screen (Figure 29).

Color definitions of text:

Red: no satellites are visible.
Yellow: three or less satellites are visible.
Green: good satellite visibility

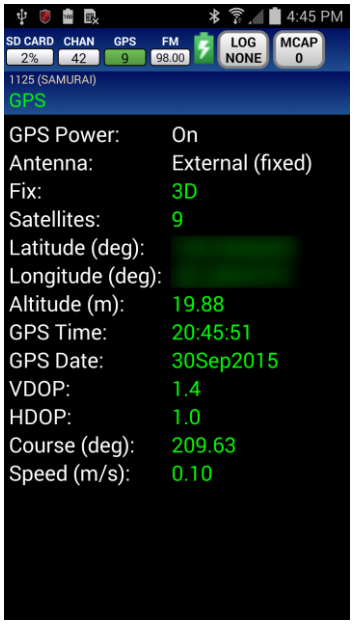


Figure 29

Settings and Commands

The Settings and Commands menu allows the user to select various settings of the Device and Phone.

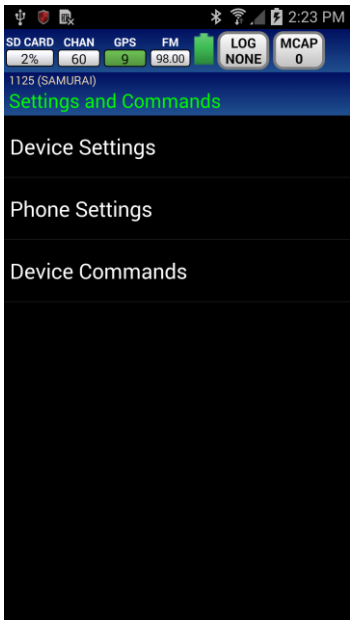


Figure 30

Device Settings

General

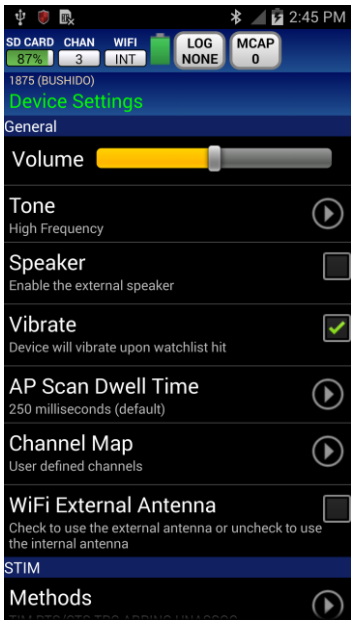


Figure 31

Volume

- Slide bar to adjust the device volume

Tone

- Low Frequency
- High Frequency
- Geiger

Speaker (BUSHIDO only)

- Check to enable external speaker

Vibrate

- Check to enable

AP Scan Dwell Time

- Select:
  - 100 milliseconds
  - 250 milliseconds (default)
  - 500 milliseconds
  - 1000 milliseconds
  - 2000 milliseconds
  - Custom value between 100 and 60000 milliseconds

Channel Map

- By default all channels are selected. (Figure 32)
- Press the phone's BACK button to return to previous screen.

WiFi External Antenna (BUSHIDO only)

- Check to use an external antenna; uncheck to use the internal device antenna.

Figure 32

STIM

Methods

- Select the methods to use for STIM (TIM, RTS/CTS, TPC, ARPING, UNASSOC). These methods can also be changed from the DF screen.

Rotation Delay

- Select the rotation delay (10, 25, 50, or 100 milli-seconds).

Power On/Off

Logging Enabled

- Start logging when device is powered on.

DC Instant On (SAMURAI only)

- Check to power on SAMURAI when external power is applied.

Auto Power Off (SAMURAI only)

- If DC Instant On is checked and power is removed the SAMURAI will shut down after 10 minutes unless WRC is connected.

Mode at Power Up

- Determines the operating mode the device will be in at power up. Survey, Survey (AP Only), and MAC Monitor.

NOTE: This setting is used in conjunction with "Logging Enabled" option. The BUSHIDO/SAMURAI will power on in the selected mode and start capturing PCAP data without the need of the Android.

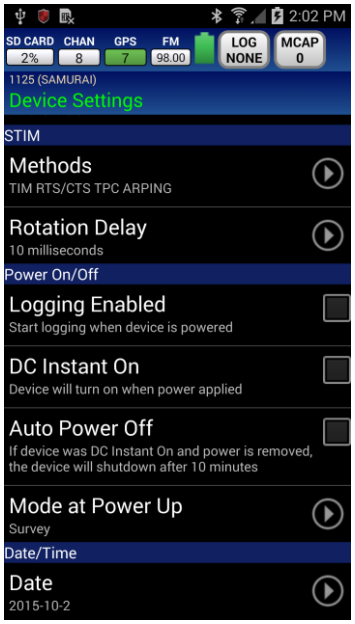


Figure 33

DATE/TIME

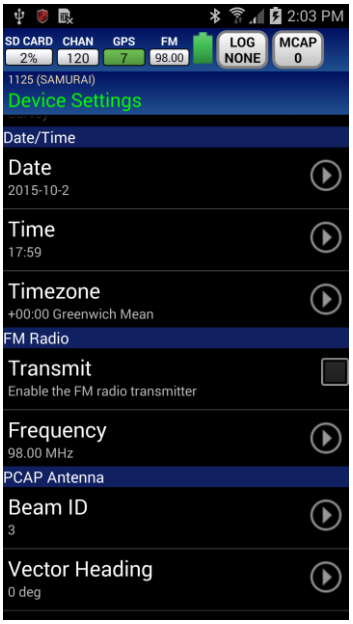


Figure 34

Date

- Device current date will be displayed in YYYY-MM-DD format.

Time

- Device current time will be displayed in HH:MM format.

Timezone

- Device current timezone will be displayed.

NOTE: Depending on the screen size of the phone it may be necessary to scroll up and down for more timezone options.

FM RADIO (SAMURAI only)

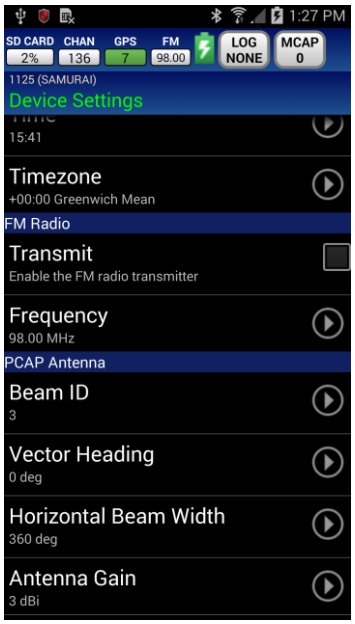


Figure 35

Transmit

- Check to enable the FM radio transmitter.

Frequency

- Enter a frequency ranging from 87.5 to 108.0 MHz.
- Frequency resolution is 50 KHz (i.e. 103.15 MHz is valid).

PCAP ANTENNA (SAMURAI only)

Beam ID

- Select a preset or enter a custom value.
- For Custom, enter a value in the range of 0 to 65535.

Vector Heading

- Select a preset or enter a custom value.
- For Custom, enter a heading ranging from 0 to 359 degrees.

Horizontal Beam Width

- Select a preset or enter a custom value.
- For Custom, enter a beam width ranging from 1 to 360 degrees.

Antenna Gain

- Enter a gain ranging from 0 to 255 dBi.

NOTE: All settings changes will need to be saved by pressing the phone's BACK button or MENU button, and select Save. If there are unsaved changes that option will appear in yellow.

Figure 36

Press the MENU button to access configuration save options.

Save – Saves all changes [colored yellow].

Revert – Reverts back to settings from the last save.

Reset to Defaults – Resets all settings back to the factory default settings. Remember to "Save" changes to make permanent.

Phone Settings

General

Vibrate

- When enabled the phone will vibrate on a Watch List hit.

Security

Hide Application Launcher

- If checked, the WRC app icon will not be displayed. When checked, the only way to start the WRC app is to enter the Hidden Launcher Code into the phone dialer.

Hidden Launcher Code

- Code to enter into the phone dialer. Select to view/change the Hidden Launcher Code. The code can be numbers only of length 1 to 4. The default Hidden Launcher Code is: **1234**

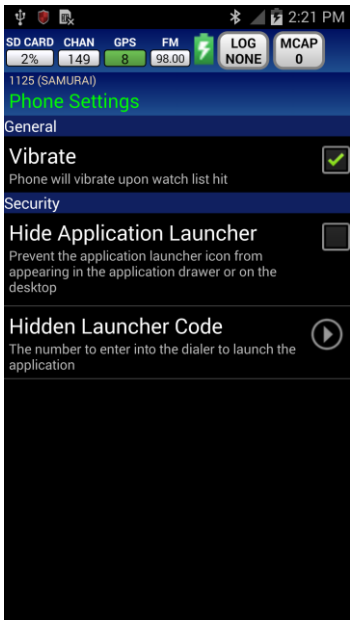


Figure 37

Device Commands

Import Watch List from SD Card

- SAMURAI only
- Import Watch List saved on the external microSD card to the SAMURAI's internal flash. This new watch list can replace the current list or be merged.

Set to GPS Date/Time

- SAMURAI only
- If the SAMURAI has a GPS lock, synchronize the SAMURAI's date and time to GPS.

Shutdown

- Select to remotely power off the device and exit the WRC mobile app.

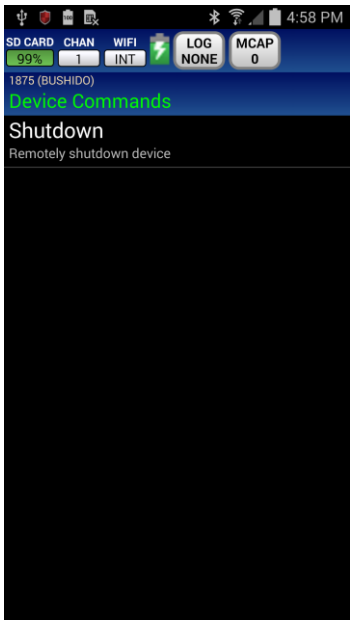


Figure 38

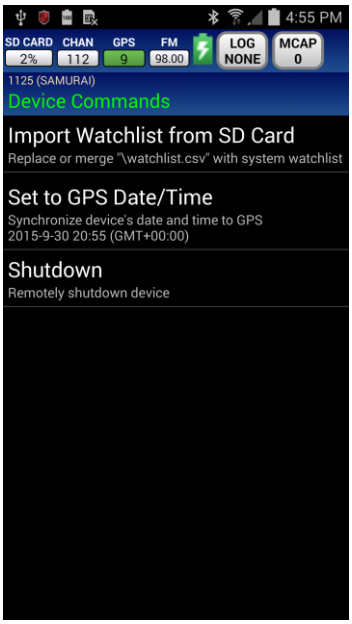


Figure 39

Context Menus for Survey and MAC Monitor

Figure 40 and Figure 41 show the context menus for the Survey and MAC Monitor screens, respectively. These menus are accessible by pressing and holding a device until the menu appears.

Each menu option is described below.

NOTE: Monitor AP MACs will not be visible when selecting an unassociated Station.

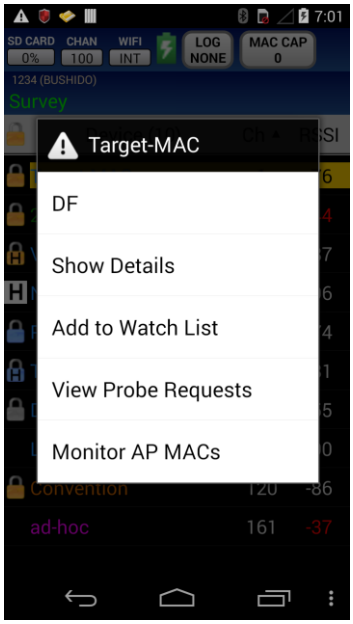


Figure 40

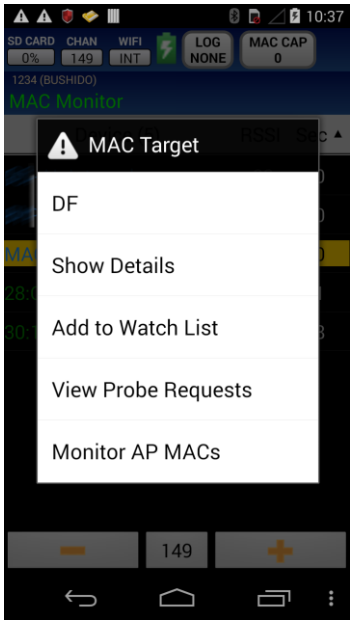


Figure 41

DF (Direction Finding)

Using the signal strength (Figure 42) slowly point the device in all directions. Proceed in the direction that displays the highest reading (closest to right-hand side which represents 10 dBm).

NOTE: The lighter color shade (red circle on Figure 42*) represents the highest RSSI this target has displayed. To reset, tap anywhere on the RSSI indicator bar. The darker shade is the current RSSI.*

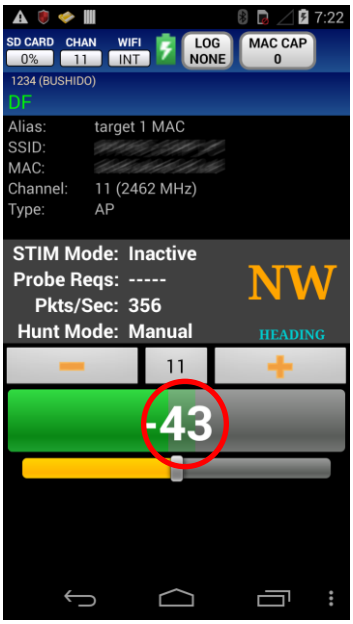


Figure 42

This screen also provides the user with the following information:

- Alias
- SSID
- MAC
- CHANNEL
- TYPE (AP, STATION, or AD-HOC)
- STIM Mode (Active or Inactive)
- PROBE REQUESTS
- PACKETS/SEC
- HUNT MODE (Manual, Auto, or Hunting)
- - / + Channel selector
- Slider bar (device volume control)

WRC mobile app will display the operator's heading based on the direction the phone is pointing. The phone's compass may require calibration.

Pressing the MENU button will access additional features (Figure 43) described below.

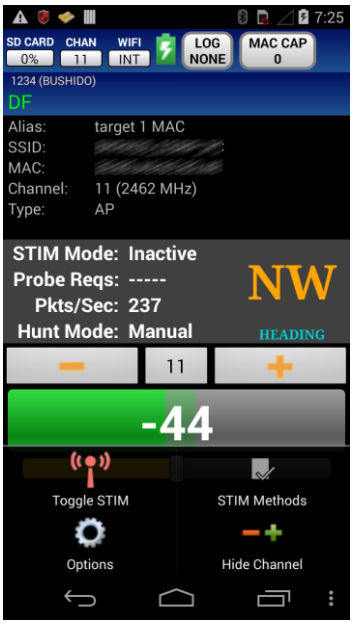


Figure 43

Toggle STIM

- Press the Toggle STIM button (Figure 43) to toggle on/off.
- STIM status is displayed on the screen (Figure 44).

NOTE: If the UNASSOC STIM method has been selected, a warning dialog will be shown to notify the user that the target device may alert its user. While the UNASSOC STIM method is active, the auto hunting option will be disabled.

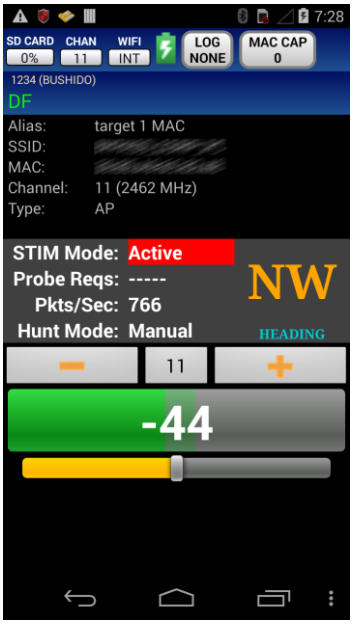


Figure 44

STIM Methods

Select the desired STIM Methods (Figure 45). A check in the box selects the method.

- **TIM** – Spoofed Traffic Indication packets are sent to the target causing it to request data from the AP.
- **RTS/CTS** – Request to send packets are sent to the target causing it to reply with a Clear to send packets.
- **TPC –** Transmit Power Control packets are sent to the target causing it to send power measurements.
- **ARPING –** Layer 2 ARP ping packets are sent to the target causing it to send ARP replies (open networks only).
- **UNASSOC** – Create multiple APs with SSID based on target's probe requests to initiate communication. This method does not work for clients that transmit broadcast probe requests instead of directed probe requests.

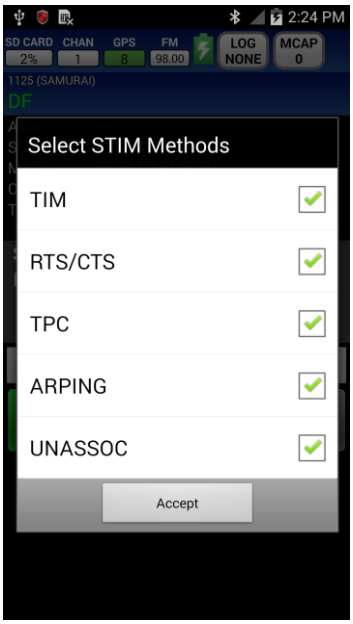


Figure 45

Options

- Auto Hunting
  - Activating this option will force the device to actively search for target MAC in the selected channel map.
  - While on the DF screen and hunt mode is enabled, if the device has not seen the target MAC address for more than 15 seconds, it will automatically enter hunt mode.
  - When in hunt mode, if the device has not done a scan for AP's within the last 60 seconds, it will begin traversing all the configured channels quickly scanning for AP's. If STIM is enabled, probe requests will be sent (using a randomized source MAC address) to cause the APs to indicate their presence. The device will dwell on each channel 400ms. If the target MAC is seen during this time, the device will abort hunt mode and begin DF'ing the target.
  - Once the list of AP channels in the area has been established, the device will begin scanning each channel searching for the target MAC for 3 seconds per channel. If STIM is enabled, the device will instead spend 3 seconds per AP, spoofing the AP's MAC in attempt to cause the target to generate traffic. The device will continue scanning until it has found the target MAC or 60 seconds have elapsed, in which time, it will restart the AP scanning process again.

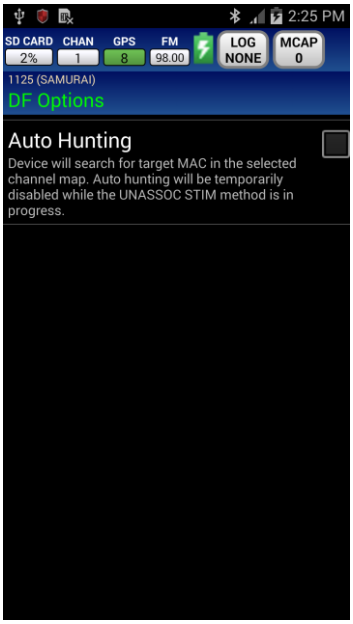


Figure 46

NOTE: Auto Hunt mode will be disabled while the UNASSOC STIM method is active.

Show/Hide Channel

Press the Show/Hide Channel button (Figure 43) to show/hide the Channel Bar buttons displayed on the screen (Figure 47).

Figure 47

Show Details

Display all details about the selected device (Figure 48).

- Alias (if on MAC or SSID watch list)
- MAC
- SSID
- AP MAC
- Channel
- Type (AP, STATION, or AD-HOC)
- Vendor
- Group Cipher
- Pair Cipher
- Authenticate

Press the MENU button and select Copy to copy the displayed data to the phone's clipboard.

Press the phone's BACK button to return to the previous screen.

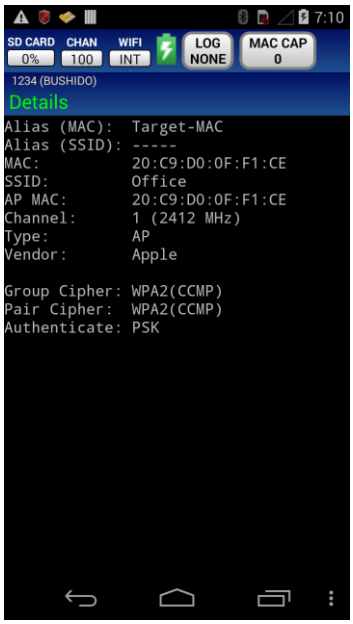


Figure 48

Add Watch List

Selecting Add to Watch List causes the "Watch List Entry" screen to appear (Figure 49). For an AP, the entry can be made on the MAC list, the SSID list, or both lists by checking the appropriate boxes. For a Station or Ad-hoc, the entry can only be on the MAC list.

Alias can be any name that the operator chooses to enter. The character limit is thirty-two (32). Separate aliases can be selected for MAC and SSID lists. MAC must be entered without separating colons.

Watch List categories:

- Target List – MACs of interest (default)
- Friendly List – MACs to ignore

NOTE: Friendly watch list items are omitted from the Survey and MAC Monitor screens.

Press OK to finish adding to the Watch List. The Watch List screen will be displayed once the operator saves the entry into the watch list.

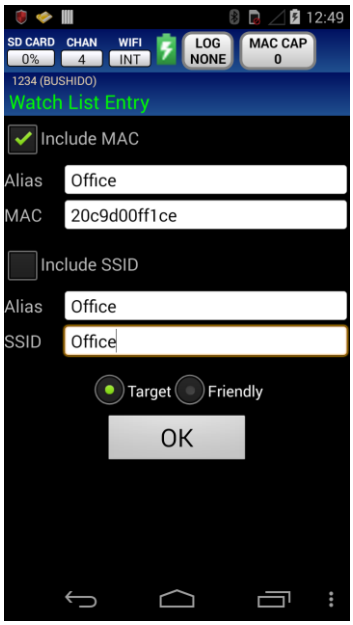


Figure 49

View Probe Requests

Figure 50 shows the MAC addresses that are sending probe requests for the SSID of the selected AP.

Press and hold a MAC until the context menu appears (Figure 51). The selected MAC can either be DF'd or added to the watchlist.

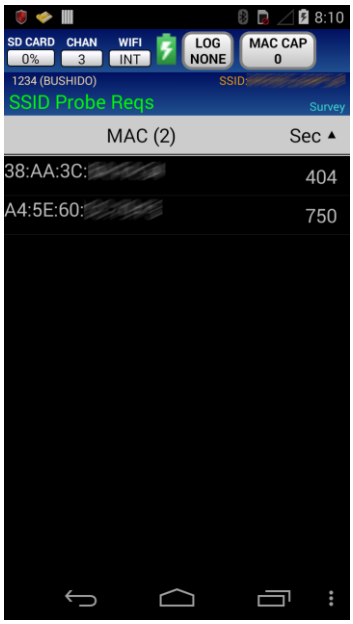


Figure 50

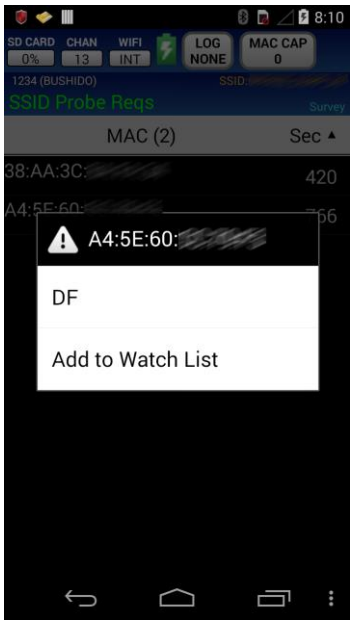


Figure 51

Figure 52 shows the SSID probe requests for the selected MAC.

Press and hold an SSID until the context menu appears (Figure 53). The selected SSID can be added to the watchlist.

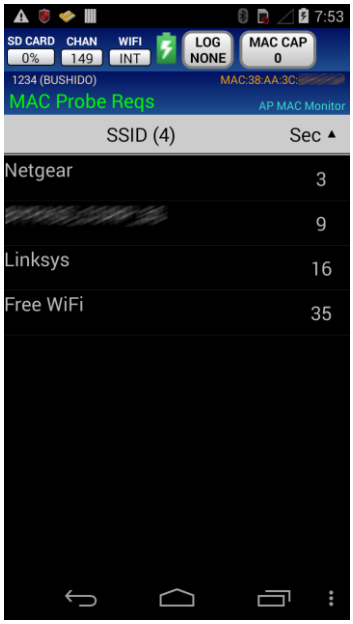


Figure 52

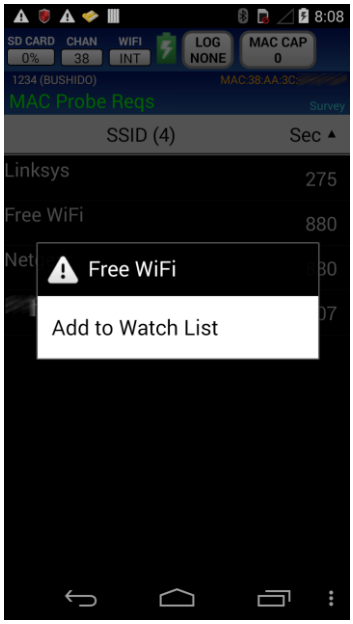


Figure 53

SSID Watchlist History

Figure 54 shows a snapshot of the MAC addresses that have sent probe requests for the SSID selected from the Watchlist screen.

Press and hold a MAC until the context menu appears (Figure 55). The selected MAC can either be DF'd or added to the watchlist.

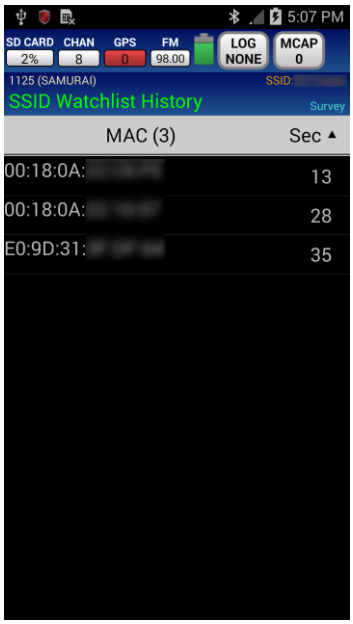


Figure 54

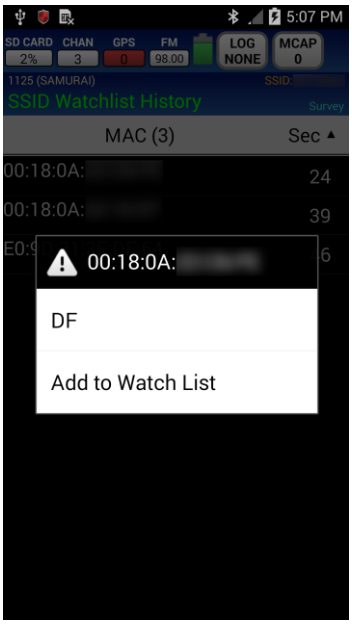


Figure 55

Monitor AP MAC

Shows the Stations associated with the selected AP. Stations are displayed by their MAC address. If a Station is already in the Watch List it will be displayed by the alias the operator assigned it.

Watch List targets will also be highlighted in yellow.

Press and hold on any device to access DF, Show Details, Add to Watch List, and View Probe Requests menu.

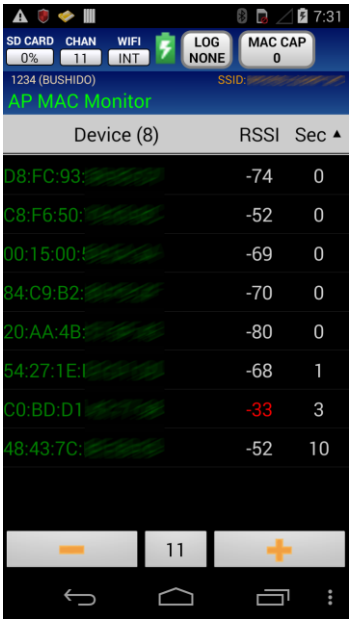


Figure 56

Pressing the MENU button will access additional features (Figure 57).

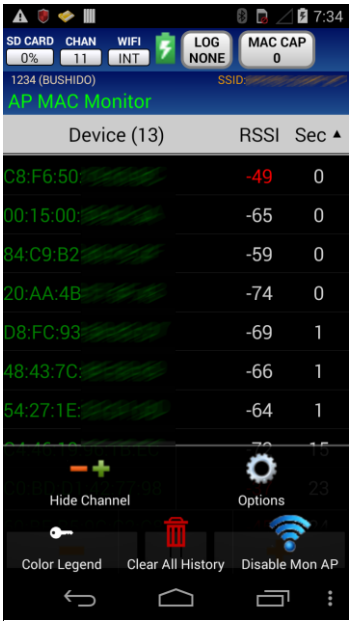


Figure 57

<u>Show/Hide Channel</u>

- Press the Show/Hide Channel button (Figure 57) to show/hide the Channel Bar buttons displayed at the bottom of the screen. (Figure 58)

Figure 58

MAC Options

- App Filters – Check to enable
  - Show Stations
  - Shows APs
  - Show Hidden Aps
  - Show AD-HOC
  - Age Out – After 40 seconds of no activity, target will no longer be displayed.

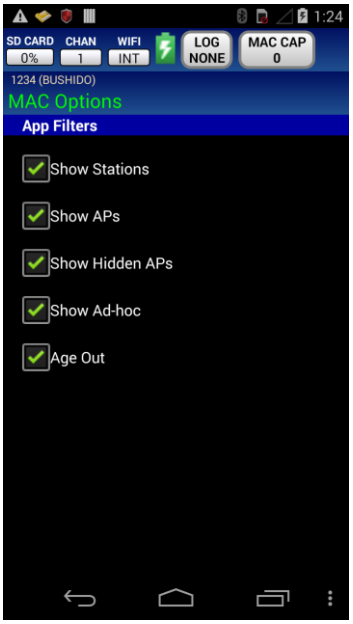


Figure 59

Color Legend

- Green – Station with known associated AP
- Yellow background – Station or AP on Watch List
- Purple – AD-HOC device
- White – Station with unknown associated AP
- Blue – AP
- Orange - WDS
- Red – unknown device

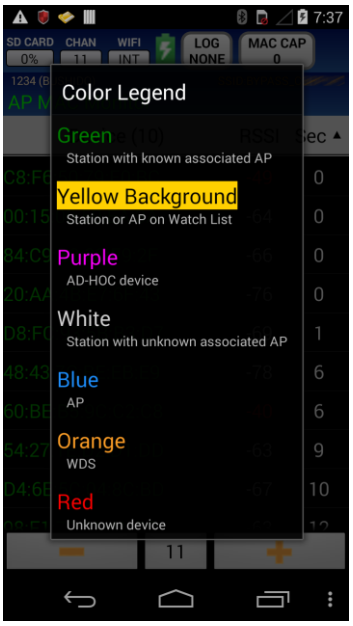


Figure 60

Clear All History

- Press the Clear All History button (Figure 57) to clear all collected data from the phone.

Disable Mon AP

- This button (Figure 57) will exit the AP MAC Monitor screen and return the operator to the MAC Monitor screen.

Field Upgrade Instructions

Items Required: Android Device, USB cables, computer, & install file

Installing the WRC app with the APK file

1. Obtain the APK file (see instructions above).
2. Uninstall any older versions of the WRC app from the Android device if applicable.
3. Connect the Android device to a computer via a USB cable.
4. If Windows does not open an Auto Play window, open Windows Explorer, find the Android in the device list and double click it. If an Auto Play window appears, select “Open device to view files”.
5. Windows Explorer will show one or more drives associated with the phone. There will be multiple folders under the drive(s).
6. Locate the WRC APK file on the computer. Drag/copy the WRC APK file to a folder on the phone. Important! The APK file must be placed in a folder that is accessible using the phone’s file explorer. On a Moto-G, the Download folder is accessible.
7. Eject the Android device from the PC. Once ejected, disconnect the Android device from the USB cable.
8. By default the Android device will not allow custom app to be installed. The “Unknown Sources” option must be enabled in the phone Settings.
9. Using the phone’s file explorer, navigate to the folder that contains the APK file.
10. Select the WRC APK file to be installed.
11. Follow the instructions on the phone to complete the installation.

Warranty Statement

The KEYW Corporation warrants each new product manufactured to be free from defects in material and workmanship under normal use and service for the warranty period. This warranty is provided to the original end user and is not assignable or transferable. The KEYW Corporation will repair, without charge, any KEYW product which fails due to a defect in material or workmanship within the warranty period. This warranty excludes damage caused by improper operation, testing, repair, modification, alteration, adjustment, installation, or maintenance of the KEYW product. Damage resulting from either accident or neglect is also excluded. The preceding warranty is The KEYW Corporation's only warranty concerning the products, services and any deliverables resulting under this order, and is made expressly in lieu of all other warranties and representations, express or implied, including any implied warranties of fitness for a particular purpose, merchantability, non-infringement or otherwise.

NOTWITHSTANDING ANY OTHER PROVISION OF THIS WARRANTY AND EXCEPT AS OTHERWISE PROVIDED UNDER APPLICABLE LAW, IN NO EVENT SHALL KEYW BE LIABLE FOR INDIRECT, SPECIAL, CONSEQUENTIAL, MULTIPLE OR PUNITIVE DAMAGES, OR ANY DAMAGE DEEMED TO BE OF AN INDIRECT OR CONSEQUENTIAL NATURE ARISING OUT OF OR RELATED TO ITS PERFORMANCE UNDER THE WARRANTY, WHETHER BASED UPON BREACH OF CONTRACT, WARRANTY, NEGLIGENCE AND WHETHER GROUNDED IN TORT, CONTRACT, CIVIL LAW OR OTHER THEORIES OF LIABILITY, INCLUDING STRICT LIABILITY. THE KEYW CORPORATION SHALL NOT BE LIABLE FOR THE LOSS OF ANTICIPATORY PROFITS.

ITAR RESTRICTION

These materials are controlled by the International Traffic in Arms Regulations, 22 C.F.R. Parts 120 - 130, and require an export license from the U. S. Department of State prior to transfer to a foreign person or foreign destination. If these materials are exported or otherwise retransferred without the necessary license(s) or in violation of the terms or conditions of any export license, recipient shall indemnify and hold harmless KEYW, its employees and parents, its and their successors and assigns, from and against any and all liability or harms, including attorney fees, arising therefrom.