Coletor de Dados Honeywell Dolphin 7850

Combinando ergonomia focada no usuário com construção industrial e tecnologias avançadas, o Honeywell Dolphin 7850 foi projetado para aumentar a produtividade de seus funcionários e maximizar seu retorno sobre o investimento.

Honeywell

Honeywell WLAN Secure Wireless Client (SWC)

For Dolphin™ mobile devices with
Windows® CE 5.0
Windows Mobile® 5.x
Windows Mobile® 6.x
Windows® Embedded Handheld 6.x

User's Guide

Disclaimer

Honeywell International Inc. (“HII”) reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult HII to determine whether any such changes have been made. The information in this publication does not represent a commitment on the part of HII.

HII shall not be liable for technical or editorial errors or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing, performance, or use of this material.

Web Address: www.honeywellaidc.com

Trademarks

Dolphin, Dolphin RF, HomeBase, Mobile Base, and QuadCharger are trademarks or registered trademarks of Hand Held Products, Inc. or Honeywell International Inc.

Microsoft, Windows, Windows Mobile, Windows CE, Windows NT, Windows 2000, Windows ME, Windows XP, ActiveSync, Outlook, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the property of their respective owners.

Patents

For patent information, please refer to www.honeywellaidc.com/patents.

Table of Contents

1

Configuring the WLAN Connection

Introduction

This WLAN Secure Wireless Client (SWC) User's Guide is relevant for Dolphin terminals with a Windows CE 5.0, Windows Mobile 5.0, Windows Mobile 6.x or Windows Embedded Handheld 6.5 operating system and an integrated 802.11a/b/g/n radio.

Note: Screen captures/icons in this user's guide may differ from what appears on your device due to operating system and model type.

The WLAN SWC application configures the wireless connection of the 802.11a/b/g/n radio in the Dolphin terminal. To verify the WLAN SWC version loaded on the terminal, do one of the following based on the device OS type:

- Tap the **WLAN SWC** icon on the **Today** or **Desktop** screen, then select the **About** tab.

  OR

- Tap **Start** > **WLAN SWC**, then select the **About** tab.

WLAN SWC Screen Layout

The layout of the WLAN SWC application window differs slightly depending on the operating system; however, the content of the window is consistent for all supported OS versions unless otherwise noted. For example, on terminals running Windows CE, the access tabs for additional screens appear near the top of the window instead of near the bottom of the window for Windows Mobile or Windows Embedded Handheld devices.

Server-Assigned IP Addresses

Please note that all server-assigned IP addresses use Dynamic Host Configuration Protocol (DHCP).

Accessing the WLAN SWC

Windows Default (Titanium) Home Screen in Windows Embedded Handheld

To access the WLAN SWC, tap **Start** > **WLAN SWC**.

The WLAN SWC opens to the **Status** tab, which is empty until a connection is configured. After a connection to an access point or network is configured and active, the tab displays the connection status.

Changing the Windows Default (Titanium) Home Screen to the Classic Today Screen Layout

To customize the default screen layout:

1. Tap **Start** > **Getting Started** > **Set Background**.
2. Tap the arrow next to "Change the background image in **Setting** > **Home**."
3. Tap **Items** on the horizontal scroll bar at the top of the screen.
4. Un-check the **Windows Default** box to switch to the Classic **Today** screen layout.
5. Select the items (e.g., calendar, time, email) you want to appear on the Classic **Today** screen.

6. Tap **OK**, then **OK** again.

Classic Today Screen in Windows CE, Windows Mobile and Windows Embedded Handheld

To access the WLAN SWC, tap the  icon on the **Today** screen command bar.

The WLAN SWC application opens displaying the **Status** tab, which is empty until a connection is configured. After a connection to an access point or network is configured and active, the tab displays the connection status.

Note: The WLAN SWC icon changes color to indicate the status of the radio; see Command Bar WLAN SWC Status Icon.

Command Bar WLAN SWC Status Icon

The command bar WLAN SWC icon  changes color according to the status of the 802.11a/b/g/n radio. The color of the icon matches the status displayed on Status Tab (see page 1-16) of the WLAN SWC application window.

Note: The Windows Default (Titanium) Home screen does not include a command bar. To see the command bar and WLAN SWC status icon, you would need to switch to the Classic Today screen layout.

Color	Meaning	Matching Status
Gray 	The radio is • Disabled • Idle • Not connecting	NO RADIO RADIO OFF DISCONNECTED INACTIVE
Yellow 	The connection is • Associating (icon stops spinning) • Authenticating (icon stops spinning) • Negotiating DHCP address (icon spins clockwise) • Out-of-Range	ASSOCIATING AUTHENTICATING
Red 	Authentication failed and the connection failed as a result.	ASSOCIATED (but not authenticated)
Green 	The connection is authenticated with a valid DHCP address.	COMPLETE

Connection Status Indicator

A radio signal strength indicator  appears at the top of the screen or on the command bar near the bottom of the screen (Classic Today screen only). The quantity of bars highlighted indicates the strength of the signal when the radio is transmitting. The higher the quantity the higher the signal strength. If the radio is not transmitting, a small “x” appears either over or near the bars.

Enabling the WLAN Radio Driver

The radio driver must be enabled for the radio to transmit a signal. You cannot connect to a network unless the radio is enabled. For details about enabling and disabling the terminal radios, refer to the User's Guide specific to your Dolphin model.

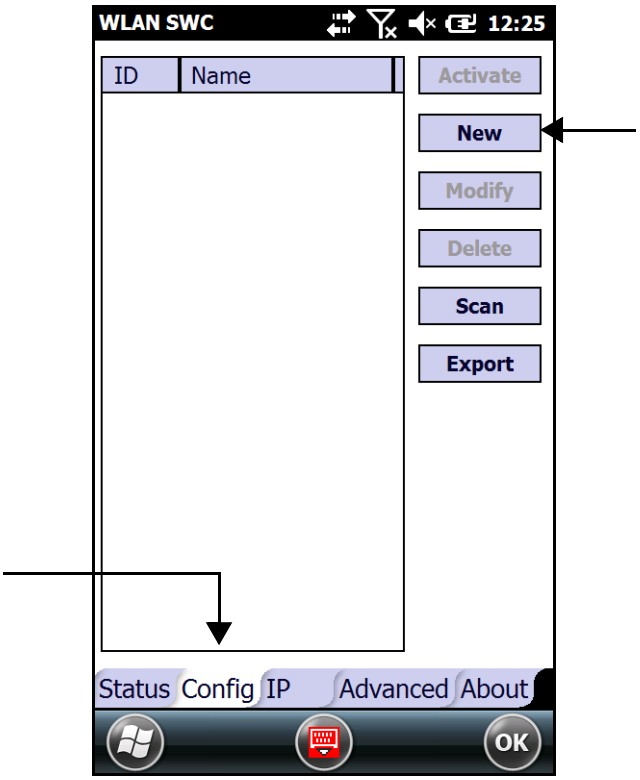
Note: User's Guides are available for download at www.honeywellaidc.com.

For Dolphin Devices running:	To access radio configuration settings . . .
Windows CE 5.0	Tap the UP arrow in the lower, right corner of the screen.
Windows Mobile 6.x, Windows Embedded Handheld 6.5	Tap **Start** > **Settings** > **Connections** > **Dolphin Wireless Manager**.
Windows Mobile 5.0	Tap **Start** > **Settings** > **Connections** tab > **Radio Manager**.

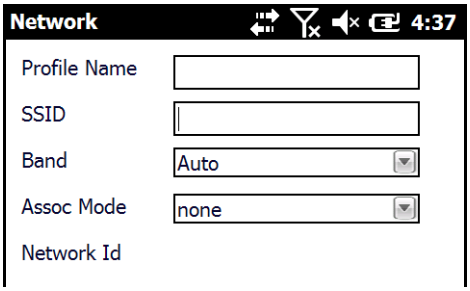
Establishing a Connection

The parameters you enter in the WLAN SWC depend entirely upon the wireless network established in your facility. If you do not know what to enter in these fields, contact your network administrator.

1. Open the WLAN SWC; see Accessing the WLAN SWC on page 1-1.
2. Tap the **Config** tab and tap **New**.



3. You can create multiple profiles that use the same SSID by giving each profile a unique name in the “Profile Name” field on the Network window.



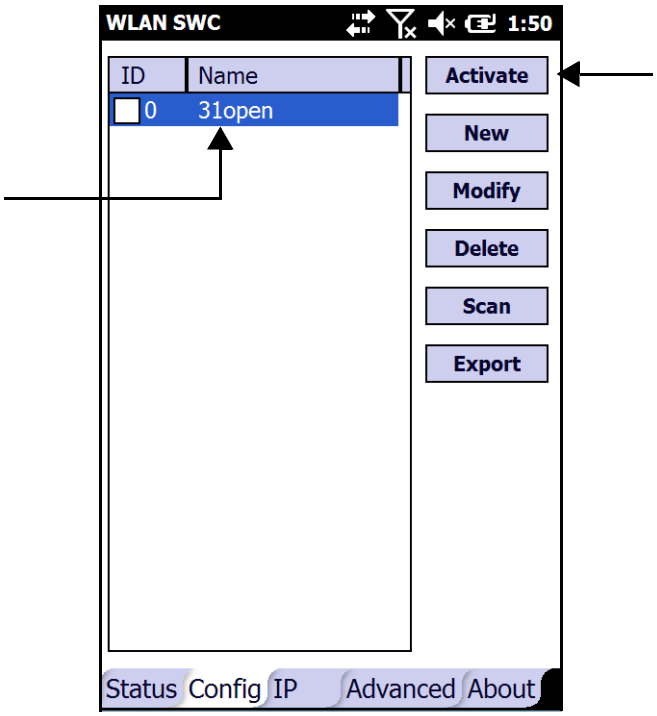
4. Type in the **SSID**.
5. Select a specific band if the connection is to be limited to b/g/n or a/n or leave the band set to **Auto**.
6. Select the **Assoc. Mode** that corresponds to your network configuration from the drop-down list.

Select	To connect with…	For more information…
None	No authentication or encryption.	None (page 1-9)
WEP	WEP encryption.	WEP (page 1-11)
IEEE 802.1X (WEP)	EAP authentication.	IEEE 802.1X (WEP) (page 1-9)
WPA-Personal (PSK) **WPA2-Personal (PSK)**	WPA encryption and PSK authentication.	WPA-Personal (PSK) & WPA2-Personal (PSK) (page 1-11)
WPA-Enterprise (EAP) **WPA2-Enterprise (EAP)**	WPA encryption and EAP authentication.	WPA-Enterprise (EAP) & WPA2-Enterprise (EAP) (page 1-12)

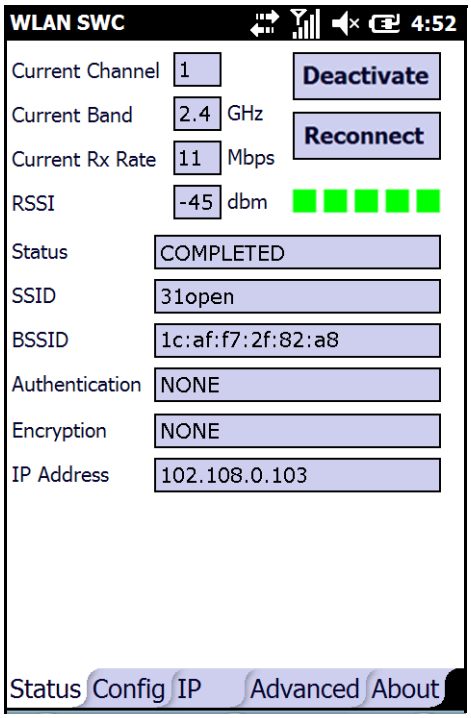
Note: The Dolphin 7600 with Windows CE 5.0 does not support EAP methods.

7. The fields and options required by the association mode, encryption, and EAP methods appear on the Network Window (see page 1-8) after each is selected.
8. If required by the association mode, select the **Encryption** method.
9. If required by the association mode, select the **EAP Method**; (see page 1-9).
10. If required or desired, enter keys or passwords.
11. Tap **OK**. You are returned to the Config tab where the SSID now appears in the list.

12. Select the device in the list and tap **Activate**. The configuration activates and the Dolphin terminal attempts to connect to the network according to the parameters you entered.

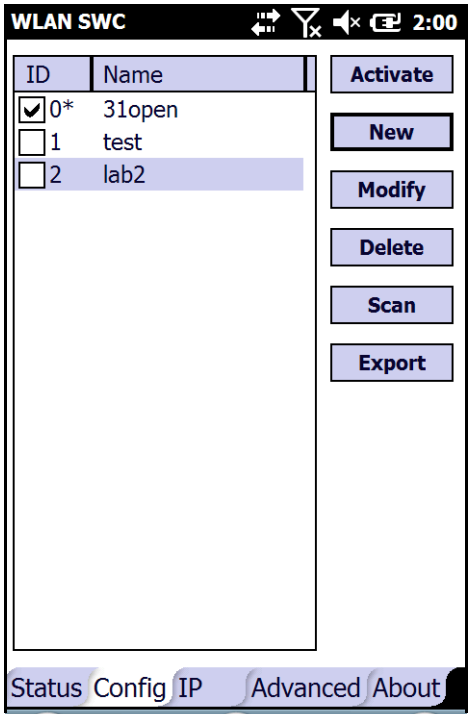


13. The **Status** tab appears displaying the connection status.



Config Tab

You manage connections and configurations on the **Config** tab. You also determine which configuration the terminal uses to connect.



Activating the Configuration

To connect, you **must** select the configuration in the list and tap **Activate**. The terminal will not attempt to connect until you tap **Activate**.

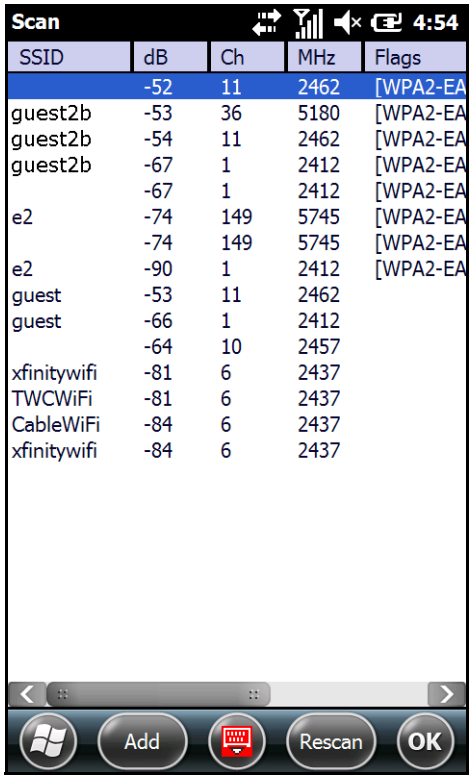
The Config tab stores all the configurations you have created in the list. Multiple configurations can be enabled allowing for profile roaming. The active configuration will have an asterisk (*) next to its ID in the first column. To switch connections, simply select it on the Config tab and tap **Activate**.

Buttons

Modify	To modify an existing configuration, select it in the list and tap **Modify**. The Network window appears displaying the data for the selected configuration. Make your changes and tap **OK** to save. Then, tap **Activate** to start connecting.
New	To manually add a connection, tap **New**. A blank Network window appears. Complete Steps 5–8 of Establishing a Connection (see page 1-3).
Delete	To delete a connection, select it in the list and tap **Delete**.
Export	To export the configured network profiles to a registry file, tap Export. This file can be used to provision other devices. All user name/password information is encrypted.

Using the Scan Feature

The Scan button on the Config tab queries for the local, configured, wireless network for devices in range of the terminal. when you tap **Scan** on the Config tab, the query starts, and the results appear on the Scan window.



Buttons

Add Tap this button after you've selected an item in the list. It opens the Network Window (see page 1-8) so that you can configure the connection.

Rescan Tap this button to rescan the wireless network if you don't see the Access Point you're looking for in the list.

Close or OK Tap this button to close the Scan window and return to the Config Tab.

Columns

SSID Displays the SSID of the Access Point. (This is the name of the Access Point you are connecting to.)

db Displays the signal in dBMs.

Ch Displays the operating channel number.

MHz Displays the operating frequency in MHz

Flags Displays the association mode and encryption required to connect to the device.

BSSID Displays the full BSSID. (This is the MAC address of the Access Point.)

Network Window

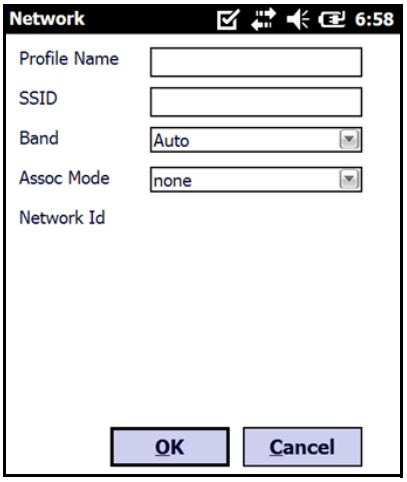
The Network window contains the configuration options to configure how the terminal connects to your wireless network.

You access the Network window from the Config Tab (see page 1-6) by doing one of the following:

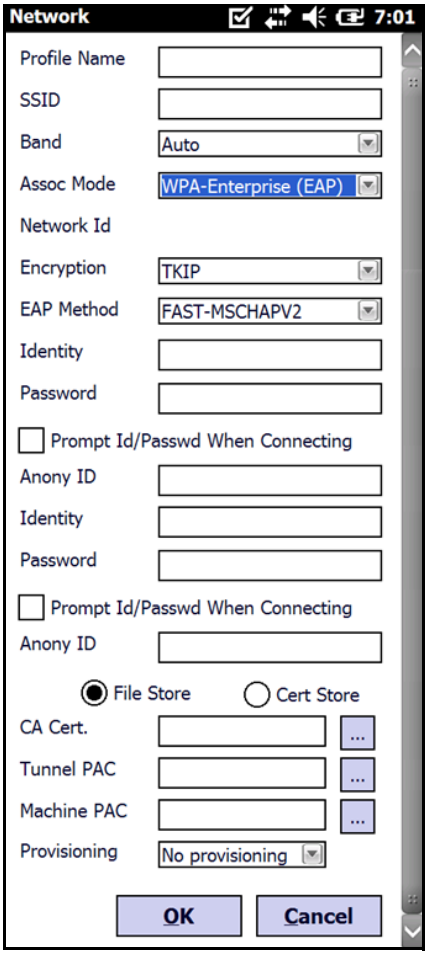
- Tapping **New** on the Config tab.
- Scanning for wireless network devices and adding them to your network; see Using the Scan Feature on page 1-7.
- Selecting an existing configuration and tapping **Modify**.

The Network window prompts you to complete the fields required by the connection options you select. For example,

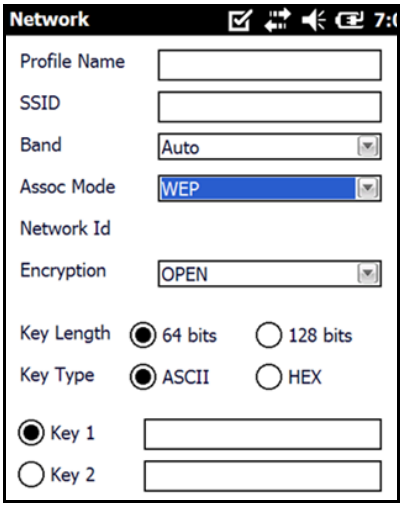
No Authentication or Encryption



WPA (EAP)



WEP



(Use the **Browse** button ... to load files located on the terminal into this configuration.)

Association Modes

The association mode you select from the Assoc. Mode drop-down list determine the fields that appear on the Network window. Different types of association modes require specific information or offer certain configuration options.

The available association modes are:

- None (see page 1-9)
- WEP (see page 1-11)
- IEEE 802.1X (WEP) (see page 1-9)
- WPA-Personal (PSK) & WPA2-Personal (PSK) (see page 1-11)
- WPA-Enterprise (EAP) & WPA2-Enterprise (EAP) (see page 1-12)

Note: The Dolphin 7600 with Windows CE 5.0 does not support EAP methods.

None

Selecting **None** as the association mode means that there is no authentication or encryption in the connection process.

IEEE 802.1X (WEP)

Available EAP Methods

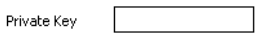
IEEE 802.1X (WEP) (page 1-9) and WPA-Enterprise (EAP) & WPA2-Enterprise (EAP) (page 1-12) support the following EAP methods:

- LEAP
- PEAPv0-MSCHAPV2
- PEAPv1-MSCHAPV2
- PEAPv1-GTC
- PEAPv1-TLS
- FAST-MSCHAPV2
- FAST-GTC
- FAST-TLS
- TLS
- TTLS-MD5
- TTLS-MSCHAPV2
- TTLS-GTC

Completing the EAP Fields

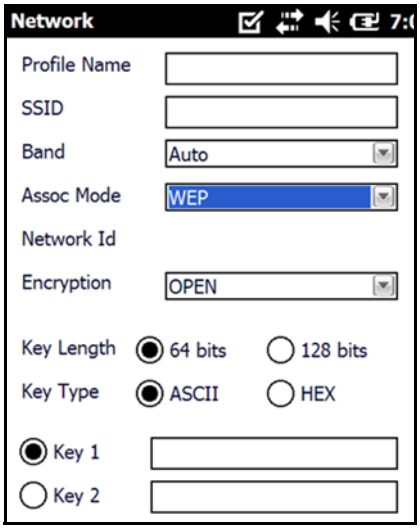
Depending on the EAP method selected, the following fields (may) appear or disappear based on what the selected protocol requires or offers for its configuration:

Field	Description
Identity	This is the 802.1X identity supplied to the authenticator. The identity value can be up to 63 ASCII characters and is case-sensitive.
Password	This is the password used for MD5-Challenge or EAP authentication. It may contain up to 63 ASCII characters and is case-sensitive. Asterisks appear instead of characters for enhanced security.

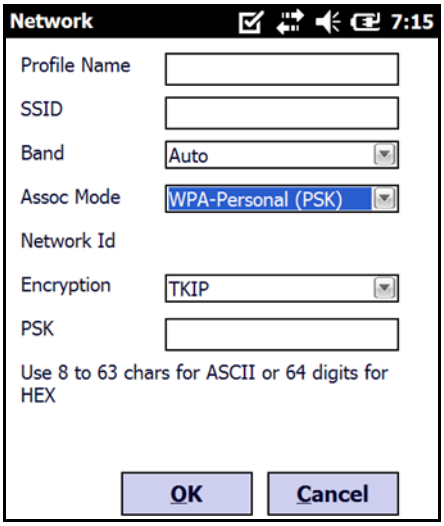
Field	Description
Anonymous ID	Enter the anonymous ID. This ID creates a tunnel through which the real ID (as entered in the Identity field) can pass. For additional security, make this ID different than the one entered in the Identity field.
File Store **Cert Store**	Click one of these radio buttons to select the location of the certificate(s). For example, if the certificate is stored in IPSM or an SD card as a file, then use **File Store**. Or, if the certificate is installed on the device in the Windows Certificate Store, then choose **Cert Store**.
CA Cert. & Client Cert. 	Tap the **Browse** button to load a CA or Client certificate located on the terminal [...]. • CA certificates are any certificates created by a certified authority (CA). This certificate is used to verify the identity of the RADIUS server. • Client certificates contain information that identifies the user, as well as information about the organization that issued the certificate. This ensures that you can encrypt data end-to-end.
Private Key 	Tap the **Browse** button to load a private key located on the terminal [...].
Priv Key Pass	If you have loaded a private key, enter the password that unlocks the private key.
Tunnel PAC &/or Machine PAC	Tap the **Browse** button to load a tunnel and/or machine PAC located on the terminal [...]. *Note: For EAP-FAST, a one-time provisioning exchange establishes a shared secret, called a Protected Access Credential (PAC) Key. That PAC Key is used for all subsequent authentications.*
Provisioning	Provisioning refers to service activation and involves programming various network databases with the customer's information. Select the provisioning method from the following options: • No Provisioning • Anonymous • Authenticated • Anonymous + Authenticated

WEP

When you select WEP as the association mode, you can select Open or Shared **Encryption** and enter your keys.



WPA-Personal (PSK) & WPA2-Personal (PSK)



Supported Encryption Methods

- TKIP
- AES-CCMP
- TKIP+CCMP

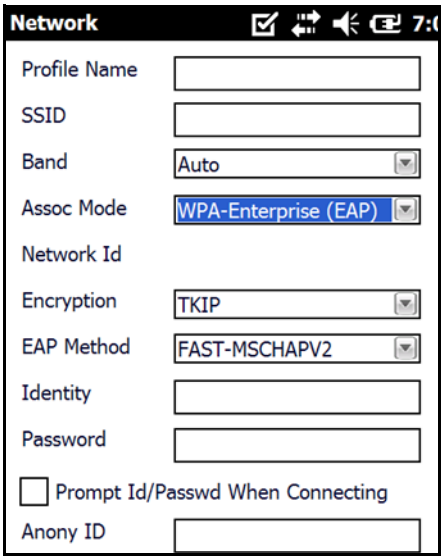
PSK (Pre-Shared Key)

The PSK field is where you enter the pre-shared key. This field accepts ASCII keys between 8–63 characters long. A hexadecimal PSK can also be entered instead of an ASCII key. Hexadecimal PSKs must be exactly 64 characters and can only contain hexadecimal digits (A–F, 0–9).

Characters are visible the first time you enter them in this field; however, those characters will appear as asterisks (*) the next time this configuration is opened.

Secret passwords or encryption keys are entered into both sides of the message exchange ahead of time. Preshared keys (PSK) are typed into the clients and servers (authentication servers, access points, etc.).

WPA-Enterprise (EAP) & WPA2-Enterprise (EAP)



Note: The Dolphin 7600 with Windows CE 5.0 does not support EAP methods.

Supported Encryption Methods

- TKIP
- AES-CCMP
- TKIP+CCMP

Available EAP Methods

The following EAP methods are supported:

- LEAP
- PEAPv0-MSCHAPV2
- PEAPv1-MSCHAPV2
- PEAPv1-GTC
- PEAPv1-TLS
- FAST-MSCHAPV2
- FAST-GTC
- FAST-TLS
- TLS
- TTLS-MD5
- TTLS-MSCHAPV2
- TTLS-GTC

For details, see Completing the EAP Fields on page 1-9.

The checkbox under the Password field prompts the user to the SSID and password every connection attempt.

Common Configurations

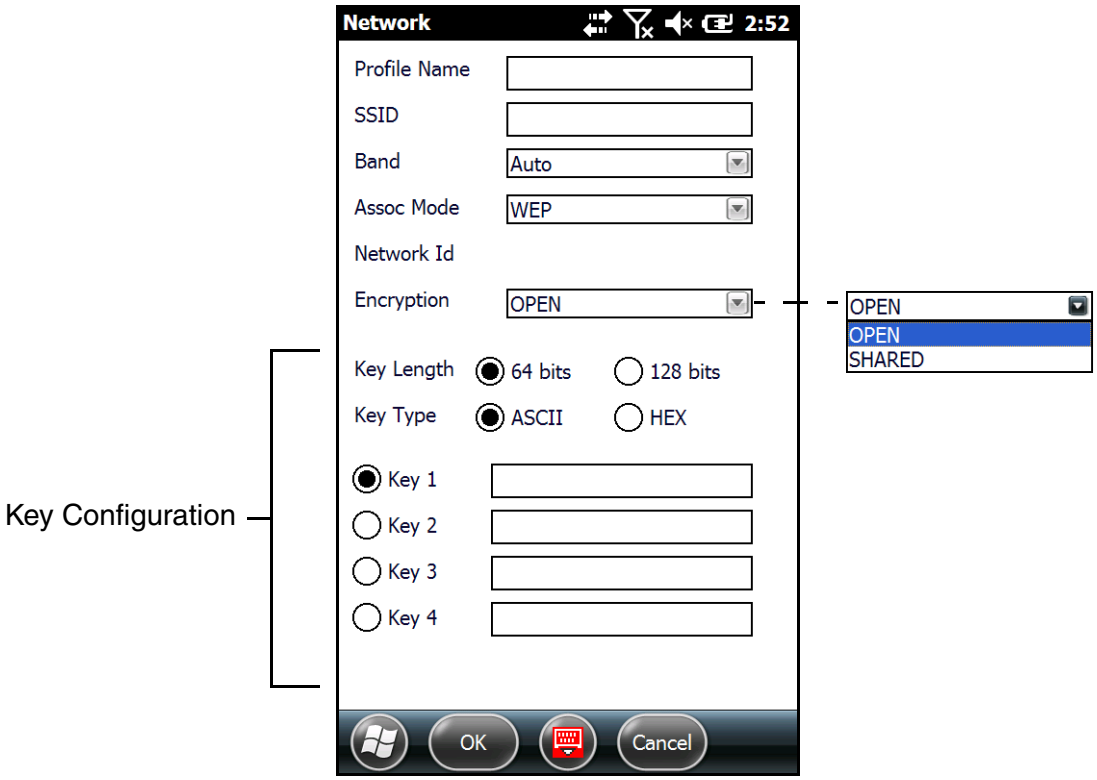
This section contains some of the most common network configurations in detail, including:

- WEP (see page 1-13)
- PEAPv1-MSCHAPV2 (see page 1-14)
- WPA-PSK (see page 1-14)

WEP

When you select WEP as the association mode, you can select Open or Shared encryption to authenticate via a specific key.

1. Open the WLAN SWC; see Accessing the WLAN SWC on page 1-1.
2. Tap the **Config** tab.
3. Tap **New**.
4. On the Network window, type in the **SSID**.
5. Select **WEP** as the **Assoc. Mode**.
6. Select an **Encryption** method (i.e., Open or Shared), configure your Key(s), then tap **OK**.



7. On the Config tab, select the network in the list and tap **Activate**. The terminal begins connecting.
8. When connected, the Status Tab (page 1-16) appears displaying the results.

PEAPv1-MSCHAPV2

1. Open the WLAN SWC; see Accessing the WLAN SWC on page 1-1.
2. Tap the **Config** tab.
3. Tap **New**.
4. On the Network window, type in the **SSID**.
5. Select **IEEE 802.1X (WEP)** as the **Assoc. Mode**.
6. Select **PEAPv1-MSCHAPV2** as the **EAP Method**.
7. Enter the **Identity** (see page 1-9) and **Password** (see page 1-9).
8. If you want to, you can enter an **Anonymous ID** (see page 1-10) or a **CA** or **Client** certificate (see page 1-10).

   Note: If you selected PEAPv1-TLS, you can also load a Private Key (page 1-10) and enter a private key password.
9. Tap **OK** and you are returned to the Config tab.
10. On the Config tab, select the network in the list and tap **Activate**.
11. The terminal begins connecting.
12. When connected, the Status tab (see page 1-16) appears displaying the results.

WPA-PSK

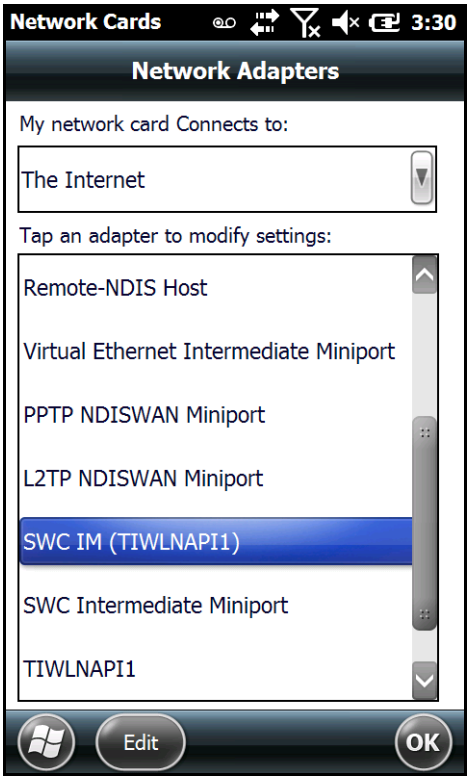
1. Open the WLAN SWC; see Accessing the WLAN SWC on page 1-1.
2. Tap the **Config** tab.
3. Tap **New**.
4. On the Network window, type in the **SSID**.
5. Select **WPA-Personal (PSK)** as the **Assoc. Mode**.
6. Select the **Encryption** method (TKIP, AES-CCMP, or TKIP + CCMP).
7. Enter the pre-share key (see page 1-11) in the **PSK** field.
8. Tap **OK** and you are returned to the Config tab.
9. On the Config tab, select the network in the list and tap **Activate**.
10. The terminal begins connecting.
11. When connected, the Status Tab (page 1-16) appears displaying the results.

Static IP

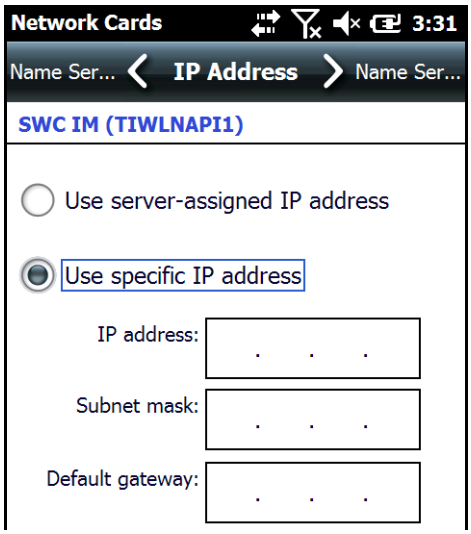
You establish a static IP through the radio driver, not the WLAN SWC. After the static IP address is established in the radio driver, you configure your wireless connection in WLAN SWC as usual.

Setting up a Static IP on Windows Mobile and Windows Embedded Handheld Devices

1. Tap **Start** > **Settings** > **Connections** (tab or icon) > **Network Cards**.



2. Tap on the network adapter. The adapter name will begin with “SWC IM” followed by the radio driver name in parentheses.
3. The IP address tab opens. Select **Use specific IP address**.



a. Enter the **IP address:**

b. Enter the **Subnet mask:**

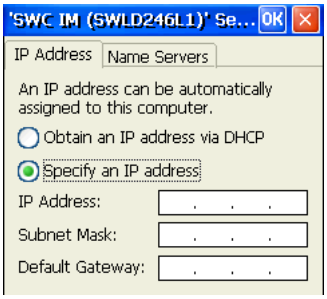
c. Enter the **Default gateway:**

4. Tap **OK**.
5. Open the WLAN SWC and configure the wireless connection.

Setting up a Static IP on Windows CE 5.0 Devices

1. Tap **Start** > **Control Panel** > **Network and Dial-up Connections**.
2. Double-tab the radio driver.

3. The radio driver opens displaying the IP Address tab. Select **Specify an IP address**.



a. Enter the **IP address:**

b. Enter the **Subnet mask:**

c. Enter the **Default gateway:**

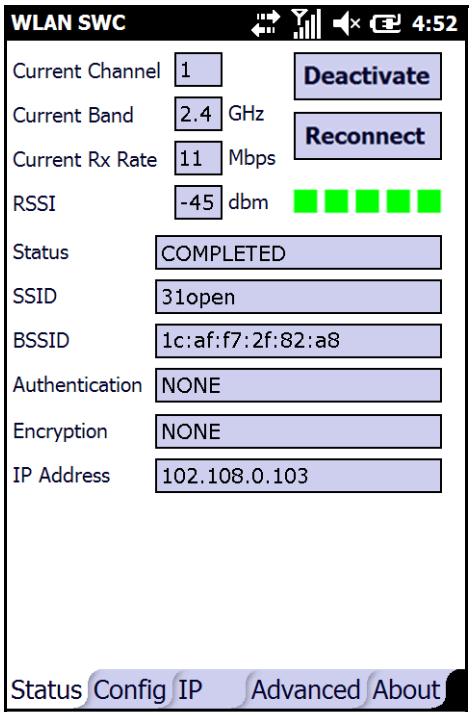
4. Tap **OK**.
5. Open the SWC and configure the wireless connection.

Status Tab

The Status tab displays the connection status of the current, activated connection; see Activating the Configuration on page 1-6.

The WLAN SWC opens to the **Status** tab, which is empty until a connection is configured. After a connection to an access point or network is configured and active, the tab displays the connection

status. See Accessing the WLAN SWC on page 1-1.



Buttons

Deactivate

The Deactivate button disconnects the device from the network and deactivates the profile.

Reconnect

Use the Reconnect button to refresh the connection by forcing the client to disconnect first.

Status Field

Status	Description
NO RADIO	The SWC does not recognize the WLAN radio driver.
RADIO OFF	The radio is not enabled.
DISCONNECTED	The radio connection is disconnected.
INACTIVE	There are either no profiles or there are no activated profiles on the Config tab.
ASSOCIATING	The terminal connection is associating.
ASSOCIATED	The terminal connection is associated.
AUTHENTICATING	Authentication is in process.
COMPLETE	The connection is associated, authentication completed successfully, and active.

BSSID Field

The BSSID is the MAC address of the Access Point.

2 Working in Ad Hoc Mode

Introduction

Most installed wireless LANs today use "infrastructure" mode that requires the use of one or more access points. With this configuration, the access point provides an interface to a distribution system (e.g., Ethernet), which enables wireless users to utilize corporate servers and Internet applications.

As an optional feature, however, the 802.11 standard specifies "ad hoc" mode, which allows the radio network interface card (NIC) to operate in what the standard refers to as an independent basic service set (IBSS) network configuration. With an IBSS, there are no access points. User devices communicate directly with each other in a peer-to-peer manner.

Even though it is a peer-to-peer connection, there must still be a host and a client; a host to initiate an ad hoc connection and a client to join an existing ad hoc connection.

Requirements

Both peer devices must have static IPs with the same Default Gateway. Therefore, you must set up a static IP on the terminal (see Static IP on page 1-15).

Initiating an Ad Hoc Connection

You need to set up an ad hoc profile in the WLAN SWC.

1. Open the WLAN SWC; see Accessing the WLAN SWC on page 1-1.
2. Tap the **Config** tab and tap **New**.
3. On the Network window, select **Ad Hoc** or **Ad Hoc (WEP)** as the **Assoc Mode**.
4. In the **SSID** field, enter the network name to use for the connection.
5. Tap **OK**.
6. On the Config tab, select the name of the profile (the SSID name) and tap **Activate** to launch the connection.

3

Setting up the WLAN SWC with DeviceConfig

Overview

DeviceConfig configures the Dolphin terminal. DeviceConfig consists of the DeviceConfig.exe and the DeviceConfig.exm file. DeviceConfig.exe looks for and applies the settings in the DeviceConfig.exm file.

You can use the EZConfig Editor to edit the WiFi settings in the DeviceConfig.exm file on the terminal. When you Hard reset (Cold Boot) the terminal and enable the WiFi radio (if it is not enabled by default), the WLAN SWC connects according to the modified settings located in the DeviceConfig.exm.

DeviceConfig.exm File

The DeviceConfig.exm file contains terminal configuration settings. This file's configuration settings persist through reboots and should be considered system defaults.

Configuring the DeviceConfig.exm File using the EZConfig Editor

EZConfig Editor creates, edits, and manages EXM files for Dolphin terminals. There are two versions of EZConfig Editor: one for the Dolphin terminal and one for the workstation. In the workstation editor, EXM files are edited, saved, then transferred to the terminal. In the terminal editor, EXM files are edited and saved right on the terminal.

Installing EZConfig for Mobility on your Workstation (PC)

1. Access the Honeywell web site at www.honeywellaidc.com.
2. Locate the product page for your Dolphin model.
3. Select the **Software** tab.
4. Under the **Tools and Utilities** heading, click on the listing for **EZConfig for Mobility Setup**.
5. Follow the security directions as prompted on the screen and click on **Download**.
6. When prompted, select **Save**, then select a location on your PC (e.g., your desktop).
7. Double click on the downloaded **EZConfig for Mobility Setup.zip** file.
8. Double click on the **Setup.exe** file. Select **OK**.
9. Follow the screen prompts to install the **EZConfig for Mobility** program. Once the software is installed, you may delete the zip file.

Modifying the DeviceConfig.exm file

The following instructions explain how to modify the DeviceConfig.exm file using the workstation (PC) version of EZConfig Editor.

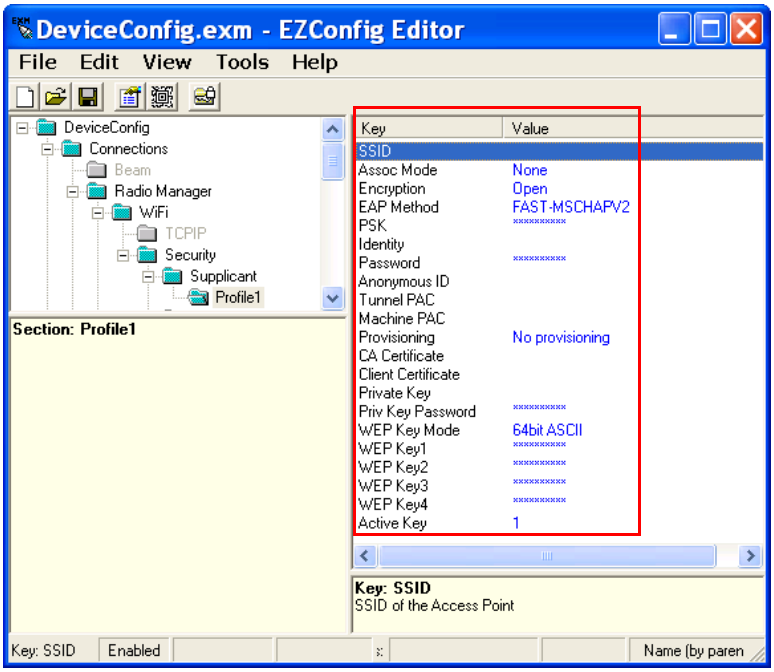
1. On your PC, click **Start > All Programs** > **Honeywell** > **EZConfig for Mobility > EZconfig for Mobility**.
2. Select **File** > **Open** or click on the **Open** toolbar button  .
3. Select the **DeviceConfig.exm** file, then click **Open**.
4. By default, all sections except the About section are disabled in the DeviceConfig.exm, which means that the key values are not applied to the terminal. To use the DeviceConfig.exm file to configure the

terminal, enable the sections and keys required by your configuration.

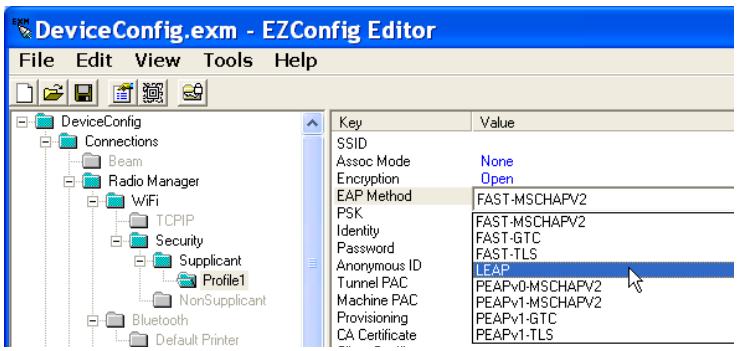
Right-click and select **Enable** on the following sections: **Radio Manager** > **WiFi** > **Security** > **Supplicant** > **Profile 1**.

Note: Enabling the WiFi section turns the 802.x radio on at startup.

5. Select the **Profile 1** section.



6. The keys in the Profile 1 section match the field on the Network Window (see page 1-8). Double-tap on each key value you want to configure and select the desired configurations from the drop-down list.



7. The items in each drop-down list are the same as the items in the drop-down lists on the Network Window (see page 1-8).

8. Select or enter all the items required by your configuration.

a. For Tunnel PAC, Machine PAC, and CA and Client Certificate keys, enter the exact path on the terminal where the PAC and certificate files are located.

The PAC and certificate files **must** be saved on the terminal first!

b. If your configuration uses WEP, select the key type from the drop-down list.

Key validation does not occur when you enter the key in WEP Key1–4 but does occur when the DeviceConfig.exm file is activated on the terminal.

9. Save the DeviceConfig.exm file on your workstation for future reference and close.

Setting up the Terminal

1. Select **File** > **Save to Device As**.
2. Select the appropriate folder(s) for your Dolphin model.

Note: If you want the settings to persist through all types of resets (e.g, Soft, Hard and Factory Resets) and kernel upgrades, save the DeviceConfig.exm file to both the permanent and active storage locations.

Dolphin Model	**Active Storage** Persist through Soft (Warm) and Hard (Cold) Resets	**Permanent Storage** Persist through a Factory Reset and Kernel Upgrades
Dolphin 60s Dolphin 6000 Dolphin 6100 Dolphin 6110 Dolphin 6500 Dolphin 70e Black Dolphin 7800 Dolphin 99EX	**`\Honeywell`**	**`\IPSM\Honeywell`**
Dolphin 7600 Dolphin 7850 Dolphin 9700 Dolphin 9900	**`\IPSM`**	**`\IPSM`**

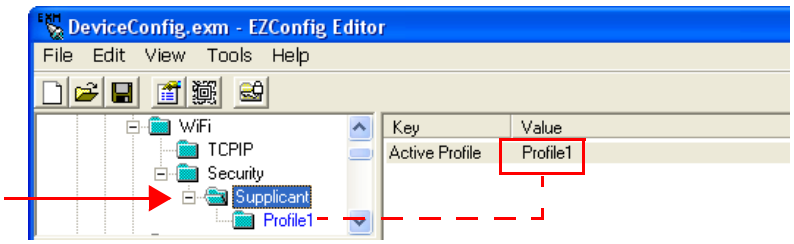
3. Hard Reset (Cold Boot) the terminal.

Note: Refer to the terminal User's Guide for additional information on the methods and types of resets supported by your Dolphin model.

4. The WLAN SWC should start connecting using the DeviceConfig settings during Autoinstall.
5. After Autoinstall is complete and the terminal has finished rebooting, open the WLAN SWC (see page 1-1) to verify the configuration is connected and correct.

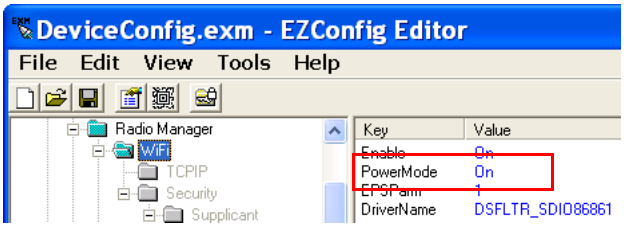
Enabling a Profile

You can have multiple profiles in the WLAN SWC section; however, one needs to be selected as the default configuration so that the configuration connects when the terminal boots up. To select a default configuration, enter the name of the profile as the Value in the **Active Profile** key of the **WiFi > Security > Supplicant** section.



Changing Power Save Mode

Power Save Mode is enabled in the radio by default.



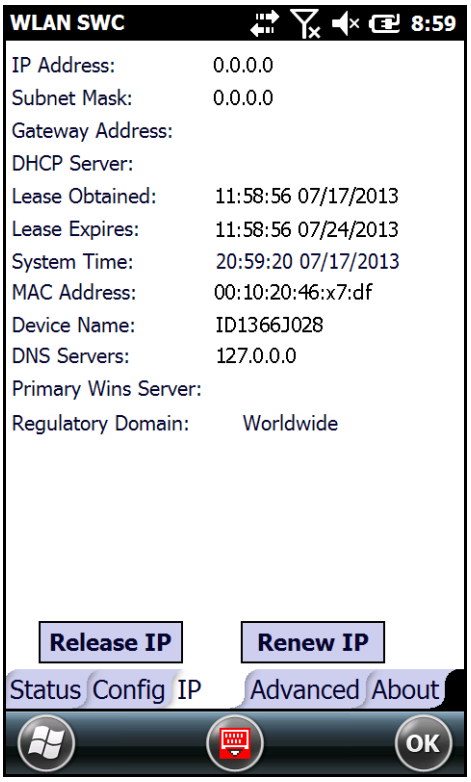
4 Administrative Tools

Overview

The WLAN SWC offers a number of tools to help you administer your network configurations.

IP Tab

The IP tab enables you to view statistics about the terminal and active network connection.

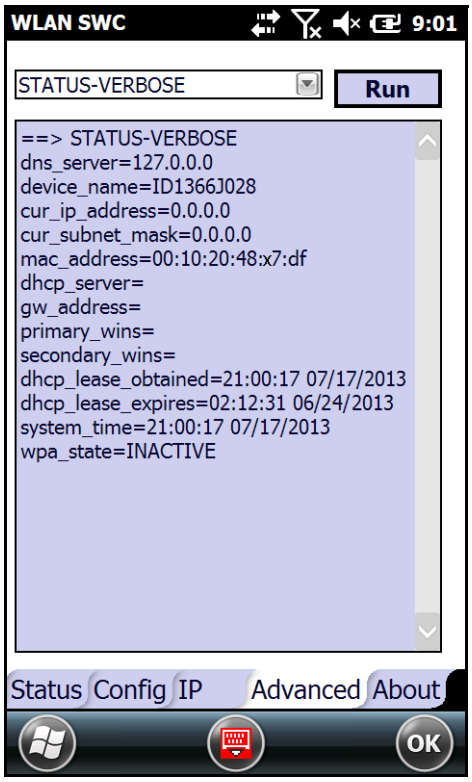


Release IP Tap this button to release the current IP address (usually assigned by DHCP).

Renew IP Tap this button to obtain a new IP address from the DHCP server.

Advanced Tab

The Advanced tab runs several reports that allow you to monitor the background processing of the WLAN SWC. In addition, you can also execute certain commands.



The WLAN SWC supports the following reports and commands (the available options vary depending on the version of SW):

- STATUS (see below)
- STATUS_VERBOSE (see page 4-3)
- DEBUG on (see page 4-3)On
- DEBUG off (see page 4-3)Off

Select the report or command from the pull-down menu, then tap **RUN** to initiate. The results display on the screen.

STATUS

STATUS queries and retrieves current WPA/EAPOL/EAP status information.

For example:

```
bssid=02:00:01:02:03:04
ssid=test network
pairwise_cipher=CCMP
group_cipher=CCMP
key_mgmt=WPA-PSK
wpa_state=COMPLETED
ip_address=192.168.1.21
Supplicant PAE state=AUTHENTICATED
suppPortStatus=Authorized
EAP state=SUCCESS
```

STATUS_VERBOSE

STATUS_VERBOSE is the same as STATUS with more verbosity (i.e., more `variable=value` pairs).

For example:

```
bssid=02:00:01:02:03:04
ssid=test network
id=0
pairwise_cipher=CCMP
group_cipher=CCMP
key_mgmt=WPA-PSK
wpa_state=COMPLETED
ip_address=192.168.1.21
Supplicant PAE state=AUTHENTICATED
suppPortStatus=Authorized
heldPeriod=60
authPeriod=30
startPeriod=30
maxStart=3
portControl=Auto
Supplicant Backend state=IDLE
EAP state=SUCCESS
reqMethod=0
methodState=NONE
decision=COND_SUCC
ClientTimeout=60
```

DEBUG on

Enables debug output to a file in **`\IPSM`** folder.

DEBUG off

Disables previously enabled debug output.

5 Customer Support

Technical Assistance

If you need assistance installing or troubleshooting your device, please contact us by using one of the methods below:

Knowledge Base: www.hsmknowledgebase.com

Our Knowledge Base provides thousands of immediate solutions. If the Knowledge Base cannot help, our Technical Support Portal (see below) provides an easy way to report your problem or ask your question.

Technical Support Portal: www.hsmsupportportal.com

The Technical Support Portal not only allows you to report your problem, but it also provides immediate solutions to your technical issues by searching our Knowledge Base. With the Portal, you can submit and track your questions online and send and receive attachments.

Web form: www.hsmcontactsupport.com

You can contact our technical support team directly by filling out our online support form. Enter your contact details and the description of the question/problem.

Telephone: www.honeywellaidc.com/locations

For our latest contact information, please check our website at the link above.

Honeywell Scanning & Mobility
9680 Old Bailes Road
Fort Mill, SC 29707

www.honeywellaidc.com