© 2015 ZIH Corp and/or its affiliates. All rights reserved.

No part of this publication may be reproduced or used in any form, or by any electrical or mechanical means, without permission in writing from Zebra. This includes electronic or mechanical means, such as photocopying, recording, or information storage and retrieval systems. The material in this manual is subject to change without notice.

The software is provided strictly on an "as is" basis. All software, including firmware, furnished to the user is on a licensed basis. Zebra grants to the user a non-transferable and non-exclusive license to use each software or firmware program delivered hereunder (licensed program). Except as noted below, such license may not be assigned, sublicensed, or otherwise transferred by the user without prior written consent of Zebra. No right to copy a licensed program in whole or in part is granted, except as permitted under copyright law. The user shall not modify, merge, or incorporate any form or portion of a licensed program with other program material, create a derivative work from a licensed program, or use a licensed program in a network without written permission from Zebra. The user agrees to maintain Zebra’s copyright notice on the licensed programs delivered hereunder, and to include the same on any authorized copies it makes, in whole or in part. The user agrees not to decompile, disassemble, decode, or reverse engineer any licensed program delivered to the user or any portion thereof.

Zebra reserves the right to make changes to any software or product to improve reliability, function, or design.

Zebra does not assume any product liability arising out of, or in connection with, the application or use of any product, circuit, or application described herein.

No license is granted, either expressly or by implication, estoppel, or otherwise under any Zebra, intellectual property rights. An implied license only exists for equipment, circuits, and subsystems contained in Zebra products.
## Revision History

Changes to the original manual are listed below:

<table>
<thead>
<tr>
<th>Change</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-01 Rev A</td>
<td>09/08</td>
<td>Initial release.</td>
</tr>
<tr>
<td>-02 Rev A</td>
<td>03/15</td>
<td>Zebra rebranding.</td>
</tr>
</tbody>
</table>
Table of Contents

Revision History ........................................................................................................................................... iii

About This Guide
Introduction ................................................................................................................................................. ix
Chapter Descriptions ............................................................................................................................. ix
Notational Conventions .......................................................................................................................... x
Related Documents .................................................................................................................................... x
Service Information ................................................................................................................................. xi

Chapter 1: Getting Started
Introduction .............................................................................................................................................. 1-1
Signal Strength Icon ................................................................................................................................. 1-2
Turning the WLAN Radio On and Off ...................................................................................................... 1-3

Chapter 2: Find WLAN Application
Introduction .............................................................................................................................................. 2-1

Chapter 3: Manage Profiles Application
Introduction .............................................................................................................................................. 3-1
Changing Profiles ................................................................................................................................... 3-2
Editing a Profile ...................................................................................................................................... 3-3
Creating a New Profile ............................................................................................................................ 3-3
Deleting a Profile .................................................................................................................................... 3-4
Ordering Profiles ..................................................................................................................................... 3-4
Export a Profile ....................................................................................................................................... 3-4

Chapter 4: Profile Editor Wizard
Introduction .............................................................................................................................................. 4-1
### Chapter 5: Manage Certificates Application

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>5-1</td>
</tr>
<tr>
<td>Certificate Properties</td>
<td>5-2</td>
</tr>
<tr>
<td>Import a Certificate</td>
<td>5-3</td>
</tr>
<tr>
<td>Delete a Certificate</td>
<td>5-4</td>
</tr>
</tbody>
</table>

### Chapter 6: Manage PACs Application

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>6-1</td>
</tr>
<tr>
<td>PAC Properties</td>
<td>6-2</td>
</tr>
<tr>
<td>Delete PAC</td>
<td>6-2</td>
</tr>
</tbody>
</table>

### Chapter 7: Options

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>7-1</td>
</tr>
<tr>
<td>Operating Mode Filtering</td>
<td>7-1</td>
</tr>
<tr>
<td>Regulatory Options</td>
<td>7-2</td>
</tr>
<tr>
<td>Band Selection</td>
<td>7-3</td>
</tr>
<tr>
<td>System Options</td>
<td>7-3</td>
</tr>
<tr>
<td>Auto PAC Settings</td>
<td>7-4</td>
</tr>
<tr>
<td>Change Password</td>
<td>7-4</td>
</tr>
<tr>
<td>Export</td>
<td>7-5</td>
</tr>
</tbody>
</table>

### Chapter 8: Wireless Status Application

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>8-1</td>
</tr>
<tr>
<td>Signal Strength Window</td>
<td>8-2</td>
</tr>
<tr>
<td>Current Profile Window</td>
<td>8-3</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>IPv4 Status Window</td>
<td>8-4</td>
</tr>
<tr>
<td>Wireless Log Window</td>
<td>8-5</td>
</tr>
<tr>
<td>Saving a Log</td>
<td>8-5</td>
</tr>
<tr>
<td>Clearing the Log</td>
<td>8-6</td>
</tr>
<tr>
<td>Versions Window</td>
<td>8-6</td>
</tr>
<tr>
<td>Chapter 9: Wireless Diagnostics Application</td>
<td></td>
</tr>
<tr>
<td>Introduction</td>
<td>9-1</td>
</tr>
<tr>
<td>ICMP Ping Window</td>
<td>9-1</td>
</tr>
<tr>
<td>Graphs</td>
<td>9-2</td>
</tr>
<tr>
<td>Trace Route Window</td>
<td>9-3</td>
</tr>
<tr>
<td>Known APs Window</td>
<td>9-3</td>
</tr>
<tr>
<td>Chapter 10: Log On/Off Application</td>
<td></td>
</tr>
<tr>
<td>Introduction</td>
<td>10-1</td>
</tr>
<tr>
<td>User Already Logged In</td>
<td>10-1</td>
</tr>
<tr>
<td>No User Logged In</td>
<td>10-1</td>
</tr>
<tr>
<td>Chapter 11: Persistence</td>
<td></td>
</tr>
<tr>
<td>Chapter 12: Configuration Examples</td>
<td></td>
</tr>
<tr>
<td>Introduction</td>
<td>12-1</td>
</tr>
<tr>
<td>EAP–FAST/MS Chap v2 Authentication</td>
<td>12-1</td>
</tr>
<tr>
<td>Glossary</td>
<td></td>
</tr>
<tr>
<td>Index</td>
<td></td>
</tr>
</tbody>
</table>
This guide provides information about using the Wireless Applications software on a Zebra mobile computer.

**NOTE** Screens and windows pictured in this guide are samples and can differ from actual screens.

### Chapter Descriptions

Topics covered in this guide are as follows:

- **Chapter 1, Getting Started** provides information enabling the wireless radio.
- **Chapter 2, Find WLAN Application** provides information about the Find WLAN application.
- **Chapter 3, Manage Profiles Application** provides information about managing profiles.
- **Chapter 4, Profile Editor Wizard** explains how to configure a profile.
- **Chapter 5, Manage Certificates Application** explains how to manage certificates.
- **Chapter 6, Manage PACs Application** explains how to manage PACs.
- **Chapter 7, Options** explains how to configure the application options.
- **Chapter 8, Wireless Status Application** describes the status indication.
- **Chapter 9, Wireless Diagnostics Application** explains how to diagnose the wireless connection.
- **Chapter 10, Log On/Off Application** explains how to log on and off the wireless network.
- **Chapter 11, Persistence** explains how to configure persistence and describes registry settings.
- **Chapter 12, Configuration Examples** provides examples for setting up various authentication and encryption types.
Notational Conventions

The following conventions are used in this document:

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

NOTE This symbol indicates something of special interest or importance to the reader. Failure to read the note will not result in physical harm to the reader, equipment or data.

CAUTION This symbol indicates that if this information is ignored, the possibility of data or material damage may occur.

WARNING! This symbol indicates that if this information is ignored the possibility that serious personal injury may occur.

Related Documents

• Enterprise Mobility Developer Kit for C (EMDK for C), available at: http://www.zebra.com/support.

For the latest version of this guide and all guides, go to: http://www.zebra.com/support.
Service Information

If you have a problem with your equipment, contact Zebra support for your region. Contact information is available at: http://www.zebra.com/support.

When contacting Zebra support, please have the following information available:

- Serial number of the unit
- Model number or product name
- Software type and version number

Zebra responds to calls by email, telephone or fax within the time limits set forth in support agreements.

If your problem cannot be solved by Zebra Support, you may need to return your equipment for servicing and will be given specific directions. Zebra is not responsible for any damages incurred during shipment if the approved shipping container is not used. Shipping the units improperly can possibly void the warranty.

If you purchased your business product from a Zebra business partner, contact that business partner for support.
Introduction

Wireless Local Area Networks (LANs) allow mobile computers to communicate wirelessly and send captured data to a host device in real time. Before using the mobile computer on a WLAN, the facility must be set up with the required hardware to run the wireless LAN and the mobile computer must be configured. Refer to the documentation provided with the access points (APs) for instructions on setting up the hardware.

802.11d is enabled by default. When enabled, the AP must be configured the same in order to connect.

To configure the mobile computer, a set of wireless applications provide the tools to configure and test the wireless radio in the mobile computer. The Wireless Application menu on the task tray provides the following wireless applications:

- Find WLANs
- Manage Profiles
- Manage Certs
- Manage PACs
- Options
- Wireless Status
- Wireless Diagnostics
- Log On/Off
- Enable/Disable Radio.

Tap the Signal Strength icon to display the Wireless Applications menu.
Signal Strength Icon

The Signal Strength icon in the task tray indicates the mobile computer’s wireless signal strength as follows:

Table 1-1 Signal Strength Icons Descriptions

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>Excellent signal strength</td>
<td>Wireless LAN network is ready to use.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Very good signal strength</td>
<td>Wireless LAN network is ready to use.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Good signal strength</td>
<td>Wireless LAN network is ready to use.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Fair signal strength</td>
<td>Wireless LAN network is ready to use. Notify the network administrator that the signal strength is only “Fair”.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Poor signal strength</td>
<td>Wireless LAN network is ready to use. Performance may not be optimum. Notify the network administrator that the signal strength is “Poor”.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Out-of-network range (not associated)</td>
<td>No wireless LAN network connection. Notify the network administrator.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>No wireless LAN network card detected</td>
<td>No wireless LAN network card detected, Wireless LAN disabled or radio disabled. Notify the network administrator.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>None</td>
<td>No wireless LAN network card detected or Wireless LAN disabled or radio disabled. Notify the network administrator.</td>
</tr>
</tbody>
</table>
Turning the WLAN Radio On and Off

To turn the WLAN radio off tap the Signal Strength icon and select Disable Radio.

Figure 1-2 Disable Radio

To turn the WLAN radio on tap the Signal Strength icon and select Enable Radio.

Figure 1-3 Enable Radio
Chapter 2 Find WLAN Application

Introduction

Use the Find WLANs application to discover available networks in the vicinity of the user and mobile computer. To open the Find WLANs application, tap the Signal Strength icon > Find WLANs. The Find WLANs window displays.

![Find WLANs Window](image)

**Figure 2-1  Find WLANs Window**

**NOTE** The Find WLANs display is limited to 32 items (ESSIDs or MAC addresses). A combination of up to 32 ESSIDs/APs may be displayed.

Manually enter valid ESSIDs not displayed in the Find WLANs window.

The Find WLANs list displays:

- WLAN Networks - Available wireless networks with icons that indicate signal strength and security. The signal strength and encryption icons are described in *Table 2-1* and *Table 2-2*.
- Network Type - Type of network. 802.11(a), 802.11(b) or 802.11(g).
- Channel - Channel on which the AP is transmitting.
- Signal Strength - The signal strength of the signal from the AP.
Tap-and-hold on a WLAN network to open a pop-up menu which provides two options: **Connect** and **Refresh**. Select **Refresh** to refresh the WLAN list. Select **Connect** to create a WLAN profile from that network. This starts the **Profile Editor Wizard** which allows you to set the values for the selected network. After editing the profile, the mobile computer automatically connects to this new profile.

<table>
<thead>
<tr>
<th>Table 2-1</th>
<th><strong>Signal Strength Icon</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Icon</td>
<td>Description</td>
</tr>
<tr>
<td>![signal_1]</td>
<td>Excellent signal</td>
</tr>
<tr>
<td>![signal_2]</td>
<td>Very good signal</td>
</tr>
<tr>
<td>![signal_3]</td>
<td>Good signal</td>
</tr>
<tr>
<td>![signal_4]</td>
<td>Fair signal</td>
</tr>
<tr>
<td>![signal_5]</td>
<td>Poor signal</td>
</tr>
<tr>
<td>![signal_6]</td>
<td>Out of range or no signal</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 2-2</th>
<th><strong>Encryption Icon</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Icon</td>
<td>Description</td>
</tr>
<tr>
<td>![encryption_1]</td>
<td>No encryption. WLAN is an infrastructure network.</td>
</tr>
<tr>
<td>![encryption_2]</td>
<td>WLAN is an Ad-Hoc network.</td>
</tr>
<tr>
<td>![encryption_3]</td>
<td>WLAN access is secured and required configuration.</td>
</tr>
</tbody>
</table>
Chapter 3 Manage Profiles Application

Introduction

The Manage Profiles application provides a list of user-configured wireless profiles. Define up to 32 profiles at any one time. To open the Manage Profiles application, tap the Signal Strength icon > Manage Profiles.

![Figure 3-1 Manage Profiles Window]

Icons next to each profile identify the profile’s current state.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>✗</td>
<td>Profile is disabled.</td>
</tr>
<tr>
<td>✗</td>
<td>Profile is cancelled. A cancelled profile is disabled until a connect or login function is performed through the configuration editor.</td>
</tr>
<tr>
<td>🌍</td>
<td>Profile is in use and describes an infrastructure profile not using encryption.</td>
</tr>
</tbody>
</table>
The profiles are listed in priority order for use by the automatic Profile Roaming feature. Change the order by moving profiles up or down. To edit existing profiles, tap and hold one in the list and select an option from the menu to connect, edit, disable (enable), or delete the profile. (Note that the Disable menu item changes to Enable if the profile is already disabled.)

The profiles are listed in priority order for use by the automatic Profile Roaming feature. Change the order by moving profiles up or down. To edit existing profiles, tap and hold one in the list and select an option from the menu to connect, edit, disable (enable), or delete the profile. (Note that the Disable menu item changes to Enable if the profile is already disabled.)

### Table 3-1 Profile Icons (Continued)

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Profile is in use and describes an infrastructure profile using encryption.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Profile is in use and describes an ad-hoc profile not using encryption.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Profile is in use and describes an ad-hoc profile using encryption.</td>
</tr>
<tr>
<td><img src="image" alt="Icon" /></td>
<td>Profile is not valid in the device current operating regulatory domain.</td>
</tr>
</tbody>
</table>

The profiles are listed in priority order for use by the automatic Profile Roaming feature. Change the order by moving profiles up or down. To edit existing profiles, tap and hold one in the list and select an option from the menu to connect, edit, disable (enable), or delete the profile. (Note that the Disable menu item changes to Enable if the profile is already disabled.)

### Changing Profiles

A completed profile is a set of configuration settings that can be used in different locations to connect to a wireless network. Create different profiles to have pre-defined operating parameters available for use in various network environments. When the WLAN Profiles window displays, existing profiles appear in the list.
Tap and hold a profile and select **Connect** from the pop-up menu to set this as the active profile. Once selected, the mobile computer uses the setting configured for the profile (i.e., authentication, encryption, ESSID, IP Config, power consumption, etc.).

**Editing a Profile**

Tap and hold a profile and select **Edit** from the pop-up menu to display the **Profile Wizard** where the profile settings are configured. See *Introduction on page 3-1* for instruction on editing a profile.

**Creating a New Profile**

To create new profiles from the **Manage Profiles** window, tap-and-hold anywhere in this window.

Select **Add** to display the **Profile Wizard** wherein the settings for the new profile are configured, such as profile name, ESSID, security, network address information, and the power consumption level. See *Introduction on page 3-1* for instruction on creating a profile.
Deleting a Profile

To delete a profile from the list, tap and hold the profile and select **Delete** from the pop-up menu. A confirmation dialog box appears.

Ordering Profiles

Tap and hold a profile from the list and select **Move Up** or **Move Down** to order the profile. If the current profile association is lost, the mobile computer attempts to associate with the first profile in the list, then the next, until it achieves a new association.

NOTE Profile Roaming must be enabled in the Options application. See Chapter 7, Options.

Export a Profile

To export a profile to a registry file, tap and hold a profile from the list and select **Export** from the pop-up menu. The **Save As** dialog box displays with the **Application** folder and a default name of WCS_PROFILE{profile GUID}.reg (Globally Unique Identifier).

![Save As Dialog Box](image)

If required, change the name in the **Name** field and tap **Save**. A confirmation dialog box appears after the export completes.
Chapter 4 Profile Editor Wizard

Introduction

Use the Profile Editor Wizard to create a new WLAN profile or edit an existing profile. If editing a profile, the fields reflect the current settings for that profile. If creating a new profile, default values appear in the fields.

Navigate through the wizard using the Next and Back buttons. Tap X to quit. On the confirmation dialog box, tap No to return to the wizard or tap Yes to quit and return to the Manage Profiles window. See Chapter 3, Manage Profiles Application for instructions on navigating to and from the Profile Editor Wizard.

Profile ID

In the Profile ID dialog box in the Profile Editor Wizard, enter the profile name and the ESSID.

![Profile ID Dialog Box](image)

Figure 4-1 Profile ID Dialog Box

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>The name and (WLAN) identifier of the network connection. Enter a user friendly name for the mobile computer profile used to connect to either an AP or another networked computer. Example: The Public LAN.</td>
</tr>
<tr>
<td>ESSID</td>
<td>The ESSID is the 802.11 extended service set identifier. The ESSID is 32-character (maximum) case sensitive string identifying the WLAN, and must match the AP ESSID for the mobile computer to communicate with the AP.</td>
</tr>
</tbody>
</table>
Tap Next. The Operating Mode dialog box displays.

### Operating Mode

Use the Operating Mode dialog box to select the operating mode (Infrastructure or Ad-Hoc) and the country location.

![Operating Mode Dialog Box](image)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Mode</td>
<td>Select <strong>Infrastructure</strong> to enable the mobile computer to transmit and receive data with an AP. Infrastructure is the default mode. Select <strong>Ad Hoc</strong> to enable the mobile computer to form its own local network where mobile computers communicate peer-to-peer without APs using a shared ESSID.</td>
</tr>
<tr>
<td>Country</td>
<td><strong>Country</strong> determines if the profile is valid for the country of operation. The profile country must match the country in the options page or it must match the acquired country if 802.11d is enabled. <strong>Single Country Use:</strong> When the device is only used in a single country, set every profile country to <strong>Allow Any Country</strong>. In the Options &gt; Regulatory dialog box (see Figure 7-2 on page 7-2), select the specific country the device is used in, and deselect the <strong>Enable 802.11d</strong> option. This is the most common and efficient configuration, eliminating the initialization overhead associated with acquiring a country via 802.11d.</td>
</tr>
</tbody>
</table>

**NOTE** Two profiles with the same user friendly name are acceptable but not recommended.
Tap Next. If Ad-Hoc mode was selected the Ad-Hoc Channel dialog box displays. If Infrastructure mode was selected the Security Mode dialog box displays. See Security Mode on page 4-5 for instruction on setting up authentication.
Ad-Hoc

Use the Ad-Hoc Channel dialog box to configure the required information to create an Ad-hoc profile. This dialog box does not appear if you selected Infrastructure mode.

1. Select a channel number from the Channel drop-down list.

![Figure 4-3  Ad-Hoc Channel Selection Dialog Box]

**NOTE** In the case of a country where DFS is implemented in band 5150-5250 MHz, Ad-hoc is not allowed and the user needs to move and select a channel in the 2.4 GHz band.

**NOTE** Ad-hoc channels are specific to the country selected.

<table>
<thead>
<tr>
<th>Band</th>
<th>Channel</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4 GHz</td>
<td>1</td>
<td>2412 MHz</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>2417 MHz</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>2422 MHz</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>2427 MHz</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>2432 MHz</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>2437 MHz</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>2442 MHz</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>2447 MHz</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>2452 MHz</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>2457 MHz</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>2462 MHz</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>2467 MHz</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>2472 MHz</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>2484 MHz</td>
</tr>
</tbody>
</table>
2. Tap Next. The Encryption dialog box displays. See Encryption on page 4-17 for encryption options.

### Security Mode

Use the Security Mode dialog box to configure the Security and Authentication methods. If Ad-Hoc mode is selected, this dialog box is not available and authentication is set to None by default.

Select the security mode from the Security Mode drop-down list. The selection chosen affects the availability of other choices for Authentication Type and Encryption methods.

- **LEGACY (Pre-WPA)** - This mode allows the user to configure protocols not available in the other Security Mode selections: Open authentication / encryption; Open authentication with WEP 40 or WEP 128; and 802.1X authentications that use WEP128 Encryption.
- **WPA-Personal** - This mode allows the user to configure a WPA-TKIP-PSK protocol.
- **WPA2-Personal** - This mode allows the user to configure WPA2-PSK protocols with the Advanced Encryption Standard (AES) encryption method.
- **WPA-Enterprise** - This mode allows the user to configure profiles with 802.1X Authentication that uses WPA and TKIP encryption method.
- **WPA2-Enterprise** - This mode allows the user to configure profiles with 802.1X Authentication that uses WPA2 with AES encryption method.

---

### Table 4-3 Ad-Hoc Channels

<table>
<thead>
<tr>
<th>Band</th>
<th>Channel</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 GHz</td>
<td>36</td>
<td>5180 MHz</td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>5200 MHz</td>
</tr>
<tr>
<td></td>
<td>44</td>
<td>5220 MHz</td>
</tr>
<tr>
<td></td>
<td>48</td>
<td>5240 MHz</td>
</tr>
</tbody>
</table>

---

**Figure 4-4 Authentication Dialog Box**

Select the security mode from the Security Mode drop-down list. The selection chosen affects the availability of other choices for Authentication Type and Encryption methods.
**Table 4-4  Security Modes**

<table>
<thead>
<tr>
<th>Security Mode</th>
<th>Authentication Types</th>
<th>Encryption Types</th>
<th>Pass-phrase/Hexkey Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legacy (Pre-WPA)</td>
<td>None, EAP-TLS, EAP-FAST, PEAP, LEAP, TTLS</td>
<td>Open, WEP-40 (40/24), WEP-104 (104/24), TKIP, AES</td>
<td>Enabled. User input required with pass-phrase/hex key configuration.</td>
</tr>
<tr>
<td>WPA - Personal</td>
<td>None</td>
<td>TKIP</td>
<td>Enabled. User input required with pass-phrase/hex key configuration.</td>
</tr>
<tr>
<td>WPA2 - Personal</td>
<td>None</td>
<td>AES</td>
<td>Enabled. User input required with pass-phrase/hex key configuration.</td>
</tr>
<tr>
<td>WPA - Enterprise</td>
<td>EAP-TLS, EAP-FAST, PEAP, LEAP, TTLS</td>
<td>TKIP</td>
<td>Disabled. No user input required for encryption key.</td>
</tr>
<tr>
<td>WPA2 - Enterprise</td>
<td>EAP-TLS, EAP-FAST, PEAP, LEAP, TTLS</td>
<td>AES</td>
<td>Disabled. No user input required for encryption key.</td>
</tr>
</tbody>
</table>

### Authentication Type

Select an available authentication type from the drop-down list. The options listed in the drop-down list are based on the selected Security Mode as shown in Table 4-4.

The authentication types, other than **None**, all use IEEE 802.1x authentication to ensure that only valid users and sometimes servers can connect to the network. Each authentication type uses a different scheme using various combinations of tunnels, username/passwords, user certificates, server certificates, and Protected Access Credentials (PACs).

**Table 4-5  Authentication Options**

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Use this setting when authentication is not required on the network.</td>
</tr>
<tr>
<td>EAP-TLS</td>
<td>Select this option to enable EAP-TLS authentication. A user certificate is required; validating the server certificate is optional.</td>
</tr>
<tr>
<td>EAP-FAST</td>
<td>Select this option to enable EAP-FAST authentication. This type uses a PAC (Protected Access Credential) to establish a tunnel and then uses the selected tunnel type to verify credentials. PACs are handled behind the scenes, transparently to the user. Automatic PAC provisioning can, depending on the tunnel type, require a user certificate and the validation of a server certificate. Manual PAC provisioning is currently not supported.</td>
</tr>
</tbody>
</table>
Profile Editor Wizard 4 - 7

Tap Next. Selecting PEAP, TTLS or EAP-FAST displays the Tunneled Authentication Type dialog box. Selecting None displays the Encryption dialog box. Selecting EAP-TLS displays the Installed User Certs dialog box. Selecting LEAP displays the User Name dialog box.

### Tunneled Authentication

Use the Tunneled Authentication Type dialog box to select the tunneled authentication options. The content of the dialog will differ depending on the Authentication Type chosen.

To select a tunneled authentication type:

1. Select a tunneled authentication type from the drop-down list. See Table 4-6 for the Tunnel authentication options for each authentication type.

2. Select the User Certificate check box if a certificate is required. If the TLS tunnel type that requires a user certificate is selected, the check box is already selected.

3. Tap Next. The Installed User Certificates dialog box appears.
### Table 4-6  Tunneled Authentication Options

<table>
<thead>
<tr>
<th>Tunneled Authentication</th>
<th>Authentication Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PEAP</td>
<td>TTLS</td>
</tr>
<tr>
<td>CHAP</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>EAP-GTC</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>MD5</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>MS CHAP</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>MS CHAP v2</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>PAP</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>TLS</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
User Certificate Selection

If the user checked the User Certificate check box on the Tunneled Authentication dialog box or if TLS is the selected authentication type, the Installed User Certificates dialog box displays. Select a certificate from the drop-down list of currently installed certificates before proceeding. The selected certificate’s name appears in the drop-down list. If the required certificate is not in the list, install it.

User Certificate Installation

There are two methods available to install a user certificate for authentication. The first is to obtain the user certificate from the Certificate Authority (CA). This requires connectivity with that CA. The second method is to install the user certificate from a file that has been placed on the device.

To install a user certificate from the CA:

1. Tap Install Certificate. The Import Certificate dialog box appears.

2. Select Import User Cert from Server and tap OK. The Install from Server dialog box appears.
3. Enter the User:, Password: and Server: information in their respective text boxes.

4. Tap Retrieve. A Progress dialog indicates the status of the certificate retrieval or tap Exit to exit.

After the installation completes, the Installed User Certs dialog box displays and the certificate is available in the drop-down for selection.

✓ **NOTE** To successfully install a user certificate, the mobile computer must already be connected to a network from which the server is accessible.

To install a user certificate from a file:

1. Tap Install Certificate. The Import Certificate dialog box appears.

![Import Certificate Dialog Box](image)

2. Choose Import from File and tap OK.

   The Open dialog box appears.

![Open Dialog Box](image)

3. In the Type drop-down list, select Personal Certs (*.pfx).

4. Browse to the file and tap OK.

   The Personal Certificate dialog box appears.
5. Enter the password and select **OK**. The certificate(s) are imported.


![Personal Certificate Window](image1.jpg)

**Figure 4-11**  *Personal Certificate Window*

- **NOTE** Installing a user certificate from a file requires that the file be of type “*.pfx”. Also this file type requires the user to supply a password in order to be read by Fusion.

### Server Certificate Selection

If the user selects the **Validate Server Certificate** check box, a server certificate is required. Select a certificate from the drop-down list of currently installed certificates in the **Installed Server Certificates** dialog box. An hour glass may appear as the wizard populates the existing certificate list. If the required certificate is not listed, install it.

![Installed Server Certificates Dialog Box](image2.jpg)

**Figure 4-12**  *Installed Server Certificates Dialog Box*

### Server Certificate Installation

To install a server certificate for authentication:

1. Tap **Install Certificate**. The **Import Certificate** dialog box appears. Choose **Import from File (.cer, .pfx)** and tap **OK**.

![Import Certificates Dialog Box](image3.jpg)

**Figure 4-13**  *Import Certificates Dialog Box*

2. A dialog box appears that lists the certificate files found with the default extension.
3. Browse to the file and tap **OK**.

4. A confirmation dialog verifies the installation. If the information in this dialog is correct, tap the **Yes** button; if the information in this dialog is not correct tap the **No** button. The wizard returns to the **Installed Server Certs** dialog box. Select the newly-installed certificate from the drop down list.

**Figure 4-14  Open Window**

**Figure 4-15  Confirmation Dialog Box**

**User Name**

The user name and password can be entered (but is not required) when the profile is created. If the username and password are not entered in the profile, then when attempting to connect, the user will be prompted to supply them. The entered information (credentials) will be saved (cached) for future reconnections.

Whether or not the username and password are entered into the profile affects how the profile is treated during a Profile Roaming operation. Profiles are excluded from consideration if they require user entry of credential information.

If the profile uses an authentication tunnel type of EAP-GTC and Token is selected (see **Password on page 4-13**), then you can control certain behavior by whether you choose to enter a value in the **Enter User Name** field. If you enter a value in the **Enter User Name** field, then whenever the Fusion software prompts you to enter credentials, the username field in the interactive credential dialog will be initialized with the value that you entered when you created the profile. If you enter a different value in the username field of the interactive credential dialog, it is cached and used to initialize the username field the next time the interactive credential dialog is shown for that profile. If you do not enter a value in the **Enter User Name** field when you create an EAP-GTC token profile, then the username field in the interactive credential dialog is initialized to blank. After you enter a username in the interactive credential dialog, it is cached as usual, but it is not be used to initialize the username field the next time the interactive credential dialog is shown for that profile; the username field will still be initialized to blank. In summary, the user can control whether the username field in the interactive credential dialog box is initialized, either with the last-interactively-entered username for that profile or with the username entered into the profile, by whether any value is entered in the **Enter User Name** field during profile entry.
Password

Use the **Password** dialog box to enter a password. If EAP/TLS is the selected authentication type, the password dialog box does not display. Note that if a username was entered and no password is entered, Fusion assumes that no password is a valid password.

1. Enter a password in the **Enter Password** field.
   
   If an authentication tunnel type of EAP-GTC is used, a **Password** dialog box with additional radio buttons displays.

Two radio buttons are added to allow the user to choose a token or static password.

Choose the **Token** radio button when using the profile in conjunction with a token generator (hardware or software). The system administrator should supply the user with a token generator for use with EAP-GTC token profiles. A token generator generates a numeric value that is entered into the password field at connect time, usually along with a PIN. Tokens have a very limited lifetime and usually expire within 60 seconds. The token generator is time-synchronized with a token server. When authenticating, the RADIUS server asks the token server to verify the token entered. The token server knows what value the token generator generates given the time of day and the username. Since tokens expire, EAP-GTC token profiles are treated differently. A prompt appears at the appropriate time to enter a token, even if a token has previously been entered. Tokens are never cached in the credential cache (though the username that is entered when the token is entered is cached).
Choose the Static radio button, the Enter Password field is enabled and a password can be entered if desired. A profile that uses an EAP-GTC tunnel type with a static password is handled in the same manner as other profiles that have credentials that don’t expire.

1. Select the Advanced ID check box, if advanced identification is desired.

2. Tap Next. The Prompt for Login at dialog box displays. See Credential Cache Options on page 4-14.

---

**Advanced Identity**

Use the Advanced ID dialog box to enter the 802.1X identity to supply to the authenticator. This value can be 63 characters long and is case sensitive. In TTLS and PEAP, it is recommended entering the identity anonymous (rather than a true identity) plus any desired realm (e.g., anonymous@myrealm). A user ID is required before proceeding.

![Profile Entry Dialog Box](image)

Figure 4-19 Advanced Identity Dialog Box

Tap Next. The Encryption dialog box displays.

---

**Credential Cache Options**

If the user selected any of the password-based authentication types then different credential caching options are available. These options specify when the network credential prompts appear: at connection, on each resume, or at a specified time.

Entering the credentials directly into the profile permanently caches the credentials. In this case, the mobile computer does not require user login. If a profile does not contain credentials entered through the Profile Editor Wizard, credentials must be entered when prompted, either when connecting to the profile in the Manage Profiles window, or when logging onto the profile using the Log On/Off command.

Credential caching options only apply to a profile when credentials are entered through the login dialog box. This includes using the Log On/Off command to log on to a profile for which the credentials were directly entered into the profile (the username / password fields left blank).
If the mobile computer does not have the credentials, a username and password must be entered. If the mobile computer has the credentials (previous entered via a login dialog box), it uses these credentials unless the caching options require the mobile computer to prompt for new credentials. If credentials were entered via the profile, the mobile computer does not prompt for new credentials (except for profiles where the credentials expire, such as EAP-GTC token profiles). Table 4-7 lists the caching options.

**Table 4-7  Cache Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>At Connect</td>
<td>Select this option to have mobile computer prompt for credentials whenever it tries to connect to the profile. Deselect this to use the cached credentials to authenticate. If the credentials are not cached, the user is prompted to enter credentials. This option only applies when the user has previously logged in to the profile.</td>
</tr>
<tr>
<td>On Resume</td>
<td>Selecting this reauthenticate an authenticated user when a suspend/resume occurs. Once reauthenticated, the user is prompted for credentials. If the user does not enter the same credentials that were entered prior to the suspend/resume within three attempts, the user is disconnected from the network. This option only applies when the user has previously logged in to the profile.</td>
</tr>
<tr>
<td>At Time</td>
<td>Select this option to perform a local verification on an authenticated user at a specified time. The time can be an absolute time or a relative time from the authentication, and should be in at least five minute intervals. Once the time has passed, the user is prompted for credentials. If the user does not enter the same credentials that were entered prior to the At-Time event within three attempts, the user is disconnected from the network. This option only applies when the user has previously logged in to the profile.</td>
</tr>
</tbody>
</table>

**NOTE**  
Entering credentials applies the credentials to a particular profile. Logging out clears all cached credentials. Editing a profile clears any cached credentials for that profile.

Users who configure their APs to use the Fast Session Resume capability available with some Authentication Types (e.g., PEAP) should not check At Connect or On Resume if they wish to avoid being prompted to re-enter credentials in circumstances in which Fast Session Resume would allow them not to be.

The following authentication types have credential caching:

- EAP-TLS
- PEAP
- LEAP
- TTLS
• EAP-FAST.

Some exceptions to the credential caching rules apply for profiles where the credentials expire, such as EAP-GTC token profiles. Since the token expires after a short period, the user is prompted for credentials even when credentials have already been entered and cached for that profile. The At Connect caching option has a slightly different function. If the user leaves the At Connect box unchecked, then the Fusion software tries to authenticate without prompting the user for a new token. If Fast Session Reconnect is enabled on the RADIUS server and the mobile computer has been previously connected and authenticated using the same profile, then the mobile computer may be able to reconnect without going through the entire authentication process. In this case, new credentials are not required (even though the old ones have expired) and the Fusion software does not prompt the user for new credentials. If Fast Session Reconnect is not enabled on the RADIUS server or if the user has checked the At Connect checkbox, then the user is prompted to enter new credentials. Note also that the On Resume caching option will always be forced to “checked” for profiles where the credentials expire. This is necessary because the Fusion software does not support the use of Fast Session Reconnect across a suspend / resume cycle; therefore, new credentials will always be needed.

Selecting the At Time check box displays the Time Cache Options dialog box.

1. Tap the Interval radio button to check credentials at a set time interval.
2. Enter the value in minutes in the Min text box.
3. Tap the At (hh:mm) radio button to check credentials at a set time.
4. Tap Next. The At Time dialog box appears.

5. Enter the time using the 24 hour clock format in the (hh:mm) text box.
6. Tap > to move the time to the right. Repeat for additional time periods.
7. Tap Next. The Encryption dialog box displays.
Encryption

NOTE The only available encryption methods in Ad-hoc are Open, WEP40 and WEP104.

Use the Encryption dialog box to select an encryption method. This page contains the fields to configure the encryption method and corresponding keys, if any. The drop-down list includes encryption methods available for the selected security mode and authentication type.

Based on the encryption method and the authentication type, the user may have to manually enter pre-shared encryption keys (or a passkey phrase). When the user selects any authentication type other than None, 802.1x authentication is used and the keys are automatically generated.

Table 4-8 Encryption Options

<table>
<thead>
<tr>
<th>Encryption</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>Select Open (the default) when no data packet encryption is needed over the network. Selecting this option provides no security for data transmitted over the network.</td>
</tr>
<tr>
<td>WEP-40 (40/24)</td>
<td>Select WEP-40 (40/24) to use 64-bit key length WEP encryption (the other 24 bits are generated automatically). If WEP-40 (40/24) is selected, other controls appear that allow you to enter keys. If the Use Passkey checkbox is checked, then the user will be asked to enter a passphrase between 4 and 32 characters long on the next page. Once the profile is saved, the passphrase will be converted into a key and the passphrase will be lost. Also, if a passkey is used only one key can be set. If the Use Passkey checkbox is not checked, then the user can enter up to four hexadecimal keys on the next page. Which key is to be entered is determined by selecting a key in the Key Index drop-down menu. The key index chosen also selects the key that will be used for encryption. Note that Fusion sets default values for these keys, so that entry is not absolutely required, but remember that the keys must match the AP.</td>
</tr>
<tr>
<td>WEP-104 (104/24)</td>
<td>Select WEP-104 (104/24) to use a 128-bit key length WEP encryption. If WEP-104 (104/24) is selected, other controls appear that allow you to enter keys. If the Use Passkey checkbox is checked, then the user will be asked to enter a passphrase between 4 and 32 characters long on the next page. Once the profile is saved, the passphrase will be converted into a key and the passphrase will be lost. Also, if a passkey is used only one key can be set. If the Use Passkey checkbox is not checked, then the user can enter up to four hexadecimal keys on the next page. Which key is to be entered is determined by selecting a key in the Key Index drop-down menu. The key index chosen also selects the key that will be used for encryption. Note that Fusion sets default values for these keys, so that entry is not absolutely required, but remember that the keys must match the AP.</td>
</tr>
</tbody>
</table>
If either WEP-40 (40/24) or WEP-104 (104/24) is selected, the wizard displays the key entry dialog box unless the Use Passkey check box was selected in the Encryption dialog box (see Figure 4-23 on page 4-17). The Key Entry dialog box shows only if the authentication is set to None.

### Hexadecimal Keys

To enter the hexadecimal key information select the Hexadecimal Keys radio button. An option is provided to hide the characters that are entered for added security. To hide the characters select the For added security - Mask characters entered check box.

To enter a hexadecimal key with characters hidden:

1. Select the For added security - Mask characters entered check box.
2. Tap Next.
3. For WEP only, in the **Edit Key** drop-down list, select the key to enter.

4. In the **Key** field, enter the key.
   a. For WEP-40 enter 10 hexadecimal characters.
   b. For WEP-104 enter 26 hexadecimal characters.
   c. For TKIP enter 64 hexadecimal characters.
   d. For AES enter 64 hexadecimal characters.

5. In the **Confirm Key** field, re-enter the key. When the keys match a message appears indicating that the keys match.

6. Repeat for each WEP key.

7. For WEP only, in the **Transmit Key** drop-down list, select the key to transmit.

8. Tap **Next**. The **IP Address Entry** dialog box displays.

To enter a hexadecimal key without characters hidden:

1. Tap **Next**.

2. For WEP only, in each **Key** field, enter the key.
   a. For WEP-40 enter 10 hexadecimal characters.
   b. For WEP-104 enter 26 hexadecimal characters.
   c. For TKIP enter 64 hexadecimal characters.
   d. For AES enter 64 hexadecimal characters.

3. For WEP only, in the **Transmit Key** drop-down list, select the key to transmit.

4. Tap **Next**. The **IP Address Entry** dialog box displays.
Pass-phrase Dialog

When selecting None as an authentication and WEP as an encryption, choose to enter a pass-phrase by checking the Pass-phrase radio button. The user is prompted to enter the pass-phrase. For WEP, the Pass-phrase radio button is only available if the authentication is None.

When selecting None as an authentication and TKIP as an encryption, the user must enter a pass-phrase. The user cannot enter a pass-phrase if the encryption is TKIP and the authentication is anything other than None.

When selecting None as an authentication and AES as an encryption, the user must enter a pass-phrase. The user cannot enter a pass-phrase if the encryption is AES and the authentication is anything other than None.

To enter a pass-phrase with characters hidden:

1. Select the For added security - Mask characters entered check box.
2. Tap Next.

![Figure 4-26 WEP-40 and WEP-104 WEP Keys Dialog Boxes](image)

3. In the Key field, enter the key.
   a. For WEP-40 enter between 4 and 32 characters.
   b. For WEP-104 enter between 4 and 32 characters.
   c. For TKIP enter between 8 and 63 characters.
   d. For AES enter between 8 and 63 characters.
4. In the Confirm Key field, re-enter the key. When the keys match a message appears indicating that the keys match.
5. Tap Next. The IP Address Entry dialog box displays.

To enter a pass-phrase key without characters hidden:

1. Tap Next.

![Figure 4-27 WEP-40 and WEP-104 WEP Keys Dialog Boxes](image)
2. In the Key field, enter the key.
a. For WEP-40 enter between 4 and 32 characters.
b. For WEP-104 enter between 4 and 32 characters.
c. For TKIP enter between 8 and 63 characters.
d. For AES enter between 8 and 63 characters.

Tap Next. The IP Address Entry dialog box displays.

---

**IP Address Entry**

Use the **IP Address Entry** dialog box to configure network address parameters: IP address, subnet mask, gateway, DNS, and WINS.

![Profile Entry](image)

**Figure 4-28** IP Address Entry Dialog Box

<table>
<thead>
<tr>
<th>Encryption</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>Select Dynamic Host Configuration Protocol (DHCP) from the IP Address Entry drop-down list to obtain a leased IP address and network configuration information from a remote server. DHCP is the default setting for the mobile computer profile. Ad-hoc mode does not support DHCP. Use only Static IP address assignment.</td>
</tr>
<tr>
<td>Static</td>
<td>Select Static to manually assign the IP, subnet mask, default gateway, DNS, and WINS addresses the mobile computer profile uses.</td>
</tr>
</tbody>
</table>

Select either **DHCP** or **Static** from the drop-down list and tap Next. Selecting **Static** displays the IP Address Entry dialog box. Selecting **DHCP** displays the Transmit Power dialog box.

Use the **IP Address Entry** dialog box to enter the IP address and subnet information.

![Profile Entry](image)

**Figure 4-29** Static IP Address Entry Dialog Box
Select the **Advanced** check box, then tap **NEXT** to display the **Advanced Address Entry** dialog box. Enter the Gateway, DNS, and WINS addresses. Tap **NEXT** without selecting the **Advanced** check box to display the **Transmit Power** dialog box.

![Advanced Address Entry Dialog Box](image)

#### Table 4-11 Static IP Address Entry Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The Internet is a collection of networks with users that communicate with each other. Each communication carries the address of the source and destination networks and the particular machine within the network associated with the user or host computer at each end. This address is called the IP address (Internet Protocol address). Each node on the IP network must be assigned a unique IP address that is made up of a network identifier and a host identifier. Enter the IP address as a dotted-decimal notation with the decimal value of each octet separated by a period, for example, 192.168.7.27.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Most TCP/IP networks use subnets to manage routed IP addresses. All IP addresses have a network part and a host part. The network part specifies a physical network. The host part specifies a host on that physical network. The subnet mask allows a network administrator to use some of the bits that are normally used to specify the host to instead specify physical sub-networks within an organization. This helps organize and simplify routing between physical networks.</td>
</tr>
</tbody>
</table>

The IP information entered in the profile is only used if the **Enable IP Mgmt** check box in the **Options > System Options** dialog box was selected (*System Options on page 7-3*). If not selected, the IP information in the profile is ignored and the IP information entered in the Microsoft interface applies.

#### Table 4-12 IP Config Advanced Address Entry Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>G/W</td>
<td>The default gateway forwards IP packets to and from a remote destination.</td>
</tr>
<tr>
<td>DNS</td>
<td>The Domain Name System (DNS) is a distributed Internet directory service. DNS translates domain names and IP addresses, and controls Internet email delivery. Most Internet services require DNS to operate properly. If DNS is not configured, Web sites cannot be located and/or email delivery fails.</td>
</tr>
<tr>
<td>WINS</td>
<td>WINS is a Microsoft® NetBIOS name server. WINS eliminates the broadcasts needed to resolve computer names to IP addresses by providing a cache or database of translations.</td>
</tr>
</tbody>
</table>

Tap **Next**. The **Transmit Power** dialog box displays.
Transmit Power

The Transmit Power drop-down list contains different options for Ad-Hoc and Infrastructure mode. Automatic (i.e., use the current AP settings) and Power Plus (use higher than the current AP settings) are available for Infrastructure mode.

Adjusting the radio transmission power level enables the user to expand or confine the transmission coverage area. Reducing the radio transmission power level reduces potential interference to other wireless devices that might be operating nearby. Increasing the radio transmission power level increases the range at which other wireless devices can “hear” the radio’s signal.

Table 4-13 Transmit Power Dialog Box (Infrastructure Mode)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automatic</td>
<td>Select <strong>Automatic</strong> (the default) to use the AP power level.</td>
</tr>
<tr>
<td>Power Plus</td>
<td>Select <strong>Power Plus</strong> to set the mobile computer transmission power one level higher than the level set for the AP. The power level is set to conform to regulatory requirements.</td>
</tr>
</tbody>
</table>

Table 4-14 Power Transmit Options (Ad-Hoc Mode)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full</td>
<td>Select <strong>Full</strong> power for the highest transmission power level. Select <strong>Full</strong> power when operating in highly reflective environments and areas where other devices could be operating nearby, or when attempting to communicate with devices at the outer edge of a coverage area.</td>
</tr>
<tr>
<td>30 mW</td>
<td>Select <strong>30 mW</strong> to set the maximum transmit power level to 30 mW. The radio transmits at the minimum power required.</td>
</tr>
<tr>
<td>15 mW</td>
<td>Select <strong>15 mW</strong> to set the maximum transmit power level to 15 mW. The radio transmits at the minimum power required.</td>
</tr>
</tbody>
</table>
Tap **Next** to display the **Battery Usage** dialog box.

---

**Battery Usage**

Use the **Battery Usage** dialog box to select power consumption of the wireless LAN. There are three settings available: CAM, Fast Power Save, and MAX Power Save. Battery usage cannot be configured in Ad-Hoc profiles.

![Battery Usage Dialog Box](image)

**Figure 4-33**  **Battery Usage Dialog Box**

![Battery Usage Options](image)

**Table 4-15 Battery Usage Options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAM</td>
<td>Continuous Aware Mode (CAM) provides the best network performance, but yields the shortest battery life.</td>
</tr>
<tr>
<td>Fast Power Save</td>
<td><strong>Fast Power Save</strong> (the default) performs in the middle of CAM and MAX Power Save with respect to network performance and battery life.</td>
</tr>
<tr>
<td>MAX Power Save</td>
<td><strong>Max Power Save</strong> yields the longest battery life while potentially reducing network performance. In networks with minimal latency, Max Power Save performs as well as Fast Power Save, but with increased battery conservation.</td>
</tr>
</tbody>
</table>
Chapter 5 Manage Certificates Application

Introduction

Users can view and manage security certificates in the various certificate stores. Tap the Signal Strength icon > Manage Certs. The Certificate Manager window displays.

Figure 5-1  Certificate Manager Window

Various certificate types display at one time. Select the Certificate Type drop-down box to filter the certificate list to display All, only Root/Server, or only User/Client certificates.
The Certificate Manager window contains command buttons at the bottom of the window. A button might be disabled (gray) if the operation cannot be performed based on any selected object.

These buttons can be hidden to allow more space for displaying the list of certificates. To hide the buttons tap-and-hold and/or double-tap the stylus in the list area depending on the mobile computer. It can also be brought up by pressing the Enter key on the keyboard. The pop-up menu appears.

Select Hide Buttons to hide the command buttons.

To display the buttons select View Buttons from the pop-up menu.

The pop-up menu also allows the user to select the Properties, Import, and Delete commands.

Certificate Properties

To display the detailed properties of a certificate, select a certificate in the list and tap the Properties button. The window display the properties of the certificate. Select a property in the upper list and the detailed information displays in the Expanded Value section.
Import a Certificate

Import certificates from either files or from a server machine:

- .CER file - DER encrypted Root/Server certificates.
- .PFX file - Personal inFormation eXchange formatted file containing one or more Root/Server and/or User/Client Certificates. These files are usually protected by a password, so a password will be prompted for. If there is no password, enter nothing and select the OK button.
- Server - User/Client certificates can be requested directly from a Certificate Authority (CA) on the network. A User name, Password (optional), and the Server (an IP address) must be provided to obtain a certificate for the User from the CA.

Tap the Import button or select from the context menu. The Import Certificate dialog box displays.

Select the Import from File (.cer, .pfx) radio button to import a certificate file. The Open window displays. Select the file to import.
Select the **Import User Cert from Server** radio button to import a certificate from a server. The **Install From Server** window displays.

Enter the user, password, and server information in the respective text boxes.

Tap the **Retrieve** button to import the certificate.

---

**Delete a Certificate**

To delete a certificate:

Select the certificate to delete.
Figure 5-8  *Import Certificate Dialog Box*

Tap the **Delete** button or select **Delete** from the pop-up menu.
Chapter 6 Manage PACs Application

Introduction

Users can view and manage Protected Access Credentials (PACs) used by Cisco's EAP-FAST authentication protocol. Tap the Signal Strength icon > Manage PACs. The PAC Manager window displays.

PACs are uniquely identified by referencing a PAC Authority Identifier (A-ID) (the server that issued the PAC) and by the individual user identifier (I-ID). The PACs display sorted by A-ID (default) or by I-ID in a tree display.

The PAC Manager window contains buttons at the bottom of the window. A button might be disabled (gray) if the operation cannot be performed based on any selected object.

These buttons can be hidden to allow more space for displaying the list of certificates. To hide the buttons tap-and-hold and/or double-tap the stylus in the list area depending on the mobile computer.

Select Hide Buttons to hide the buttons.

To display the buttons select View Buttons from the pop-up menu.

The pop-up menu also allows the user to select the Properties and Delete commands.

You can always sort by A-ID, sort by I-ID, view buttons and hide buttons in the pop-up menu.
PAC Properties

Display the detailed properties of a PAC by selecting an item in a sub-tree, and selecting the **Properties** button or pop-up menu. The following Window appears with the list of properties in the upper portion of the window. By selecting an entry in the upper list, the expanded details of the entry property displays in the lower list of the window.

![Figure 6-2 Command Buttons and Context Menu](image)

To return to the main page, tap the **Ok** button, **Escape**, or **X** button depending on the mobile computer.

Delete PAC

To delete a single PAC, tap a leaf item (right most tree item) to select the PAC, then select the **Delete** button or pop-up menu. A confirmation dialog box appears.

To delete a group of PACs having the same A-ID or same I-ID, sort the PACs by desired ID type, then tap on the parent item (left most tree item) to select the group. Select the **Delete** button or pop-up menu and a confirmation dialog box appears.
Chapter 7 Options

Introduction

Use the wireless Option dialog box to select one of the following operation options from the drop-down list:

- Operating Mode (Op Mode) Filtering
- Regulatory
- Band Selection
- System Options
- Auto PAC Settings
- Change Password
- Export.

Operating Mode Filtering

The Operating Mode Filtering options cause the Find WLANs application to filter the available networks found.

Figure 7-1  OP Mode Filtering Dialog Box

The AP Networks and Ad-Hoc Networks check boxes are selected by default.
Tap **Save** to save the settings or tap **X** to discard any changes.

### Regulatory Options

Use the **Regulatory** settings to configure the country the mobile computer is in. Due to regulatory requirements (within a country) a mobile computer is only allowed to use certain channels.

![Regulatory Options Dialog Box](image)

**Figure 7-2  Regulatory Options Dialog Box**

### Table 7-2  Regulatory Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>Select a country from the drop-down list. If the Enable 802.11d check box is not selected, a profile’s country selection must match this setting in order to connect to that profile.</td>
</tr>
<tr>
<td>Enable 802.11d</td>
<td>If the <strong>Enable 802.11d</strong> check box is selected, the WLAN adapter follows the 802.11d standard. It passively scans until valid country information is received from an AP. It limits transmit power settings based on maximums received from the AP. Profiles which use Infrastructure mode can only connect if the country selected in the profile matches the AP country setting, or if the profile country setting is <strong>Allow Any Country</strong>. Profiles which use Ad-hoc mode are not 802.11d compliant.</td>
</tr>
</tbody>
</table>
Band Selection

The **Band Selection** settings identify the frequency bands to scan when finding WLANs. These values refer to the 802.11 standard networks.

![Band Selection Dialog Box](image)

**NOTE** Select one band for faster access when scanning for WLANs.

Not all mobile devices support both 2.4 GHz and 5 GHz bands.

![System Options Dialog Box](image)

**System Options**

Use **System Options** to set miscellaneous system setting.

![System Options Dialog Box](image)

**Table 7-3** **Band Selection Options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4GHz Band</td>
<td>The <strong>Find WLANs</strong> application list includes all networks found in the 2.4 GHz band (802.11b and 802.11g).</td>
</tr>
<tr>
<td>5GHz Band</td>
<td>The <strong>Find WLANs</strong> application list includes all networks found in the 5 GHz band (802.11a).</td>
</tr>
</tbody>
</table>

Tap **Save** to save the settings or tap **X** to discard any changes.

**Table 7-4** **System Options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Roaming</td>
<td>Configures the mobile computer to roam to the next available WLAN profile when it moves out of range of the current WLAN profile.</td>
</tr>
</tbody>
</table>
Auto PAC Settings

Use the Auto PAC Settings to configure whether to allow automatic PAC provisioning and automatic PAC refreshing when using the EAP-FAST authentication protocol.

If the master key has expired then the PAC on the device that was generated with this expired key will have to be manually deleted and a new PAC provisioned even when “Allow Refreshing” is turned ON.

Change Password

Use **Change Password** to require that a user enter a password before being allowed to create or edit a profile or change the **Options**. This allows pre-configuring profiles and prevents users from changing the network settings. The user can use this feature to protect settings from a guest user. By default, the password is not set.
Enter the current password in the **Current** text box. If there is no current password, the **Current** text box is not displayed. Enter the new password in the **New** and **Confirm** text boxes. Tap **Save**.

To change an existing password, enter the current password in the **Current** text box and enter the new password in the **New**: and **Confirm**: text boxes. Tap **Save**.

To delete the password, enter the current password in the **Current**: text box and leave the **New**: and **Confirm**: text boxes empty. Tap **Save**.

**NOTE**  Passwords are case sensitive and can not exceed 63 characters.

---

### Export

**NOTE**  For Windows CE 5.0 devices, exporting options enables settings to persists after cold boot. For Mobile 5.0 devices, exporting options enables settings to persists after clean boot. See *Chapter 11, Persistence* for more information.

Use **Export** to export all profiles to a registry file, and to export the options to a registry file.

**Figure 7-7**  *Options - Export Dialog Box*

To export options:

1. Tap **Export Options**. The **Save As** dialog box displays.
2. Enter a filename in the **Name:** field. The default filename is WCS_OPTIONS.REG.

3. Select the desired folder.

4. Tap **Save**.

To export all profiles:

1. Tap **Export All Profiles**. The **Save As** dialog box displays.

2. Enter a filename in the **Name:** field. The default filename is WCS_PROFILES.REG.

3. In the **Folder:** drop-down list, select the desired folder.

4. Tap **Save**.

Selecting **Export All Profiles** also saves an indication of the current profile. This information is used to determine which profile to connect with after a warm boot or cold boot.
Chapter 8 Wireless Status Application

Introduction

To open the Wireless Status window, tap the Signal Strength icon > Wireless Status. The Wireless Status window displays information about the wireless connection.

![Wireless Status Window](image)

**Figure 8-1  Wireless Status Window**

The Wireless Status window contains the following options. Tap the option to display the option window.

- Signal Strength - provides information about the connection status of the current wireless profile.
- Current Profile - displays basic information about the current profile and connection settings.
- IPv4 Status - displays the current IP address, subnet, and other IP related information assigned to the mobile computer.
- Wireless Log - displays a log of important recent activity, such as authentication, association, and DHCP renewal completion, in time order.
- Versions - displays software, firmware, and hardware version numbers.
- Quit - exits the Wireless Status window.

Each option window contains a back button to return to the main Wireless Status window.
Signal Strength Window

The **Signal Strength** window provides information about the connection status of the current wireless profile including signal quality, missed beacons, and other statistics described below. The BSSID address (shown as AP MAC Address) displays the AP currently associated with the connection. In Ad-Hoc mode, the AP MAC Address shows the BSSID of the Ad-Hoc network. Information in this window updates every 2 seconds.

To open the **Signal Status** window, tap **Signal Strength** in the **Wireless Status** window.

![Signal Strength Window](image)

**Figure 8-2  Signal Strength Window**

After viewing the **Signal Strength** window, tap the back button to return to the **Wireless Status** window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signal</td>
<td>Displays the Relative Signal Strength Indicator (RSSI) of the signal transmitted between the AP and mobile computer. As long as the Signal Quality icon is green the AP association is not jeopardized. If the icon is red (poor signal), an association with a different AP could be warranted to improve the signal. The signal strength icon changes depending on the signal strength.</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Excellent Signal" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Very Good Signal" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Good Signal" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Fair Signal" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Poor Signal" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Out of Range (no signal)" /></td>
</tr>
<tr>
<td></td>
<td>The radio card is off or there is a problem communicating with the radio card.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates if the mobile computer is associated with the AP.</td>
</tr>
<tr>
<td>Signal Quality</td>
<td>Displays a text format of the Signal icon.</td>
</tr>
<tr>
<td>Tx Retries</td>
<td>Displays a percentage of the number of data packets the mobile computer retransmits. The fewer transmit retries, the more efficient the wireless network is.</td>
</tr>
</tbody>
</table>
The Current Profile window displays basic information about the current profile and connection settings. This window updates every two seconds.

To open the Current Profile window, tap Current Profile in the Wireless Status window.

---

**Table 8-1  Signal Strength Status (Continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Missed Beacons</td>
<td>Displays a percentage of the amount of beacons the mobile computer missed. The fewer missed beacons, the more efficient the wireless network is. Beacons are uniform system packets broadcast by the AP to keep the network synchronized.</td>
</tr>
<tr>
<td>Signal Level</td>
<td>The AP signal level in decibels per milliwatt (dBm).</td>
</tr>
<tr>
<td>Noise Level</td>
<td>The background interference (noise) level in decibels per milliwatt (dBm).</td>
</tr>
<tr>
<td>SNR</td>
<td>The access point/mobile computer Signal to Noise Ratio (SNR) of signal strength to noise (interference) in decibels per milliwatt (dBm).</td>
</tr>
<tr>
<td>Association Count</td>
<td>Displays the number of times the mobile computer has roamed from one AP to another.</td>
</tr>
<tr>
<td>AP MAC Address</td>
<td>Displays the MAC address of the AP to which the mobile computer is connected.</td>
</tr>
<tr>
<td>Transmit Rate</td>
<td>Displays the current rate of the data transmission.</td>
</tr>
</tbody>
</table>

**Current Profile Window**

The Current Profile window displays basic information about the current profile and connection settings. This window updates every two seconds.

To open the Current Profile window, tap Current Profile in the Wireless Status window.

---

**Table 8-2  Current Profile Window**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>Displays the name of the profile that the mobile computer is currently using to communicate with the AP.</td>
</tr>
<tr>
<td>ESSID</td>
<td>Displays the current profile’s ESSID.</td>
</tr>
<tr>
<td>Mode</td>
<td>Displays the current profile’s mode, either Infrastructure or Ad-Hoc.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Displays the current profile’s authentication type.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Displays the current profile’s encryption type.</td>
</tr>
</tbody>
</table>
IPv4 Status Window

The IPv4 Status window displays the current IP address, subnet, and other IP related information assigned to the mobile computer. It also allows renewing the IP address if the profile is using DHCP to obtain the IP information. Tap Renew to initiate the IP address renewal process. The IPv4 Status window updates automatically when the IP address changes.

To open the IPv4 Status window, tap IPv4 Status in the Wireless Status window.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel</td>
<td>Displays the channel currently being used to communicate with the AP.</td>
</tr>
<tr>
<td>Country</td>
<td>Displays the country setting currently being used.</td>
</tr>
<tr>
<td>Transmit Power</td>
<td>Displays the current radio transmission power level.</td>
</tr>
</tbody>
</table>

Table 8-3 IPv4 Status Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Type</td>
<td>Displays the IP address assignment method used for the current profile: DHCP or Static. If the IP Type is DHCP, the IP Address and other information shown is obtained from the DHCP server. In this case, the DHCP Server address and the Lease information will also be shown. If the IP Type is Static, the IP Address and other information shown are those that were entered in the profile.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Displays the mobile computer’s IP address. The Internet is a collection of networks with users that communicate with each other. Each communication carries the address of the source and destination networks and the particular machine within the network associated with the user or host computer at each end. This address is called the IP address. Each node on the IP network must be assigned a unique IP address that is made up of a network identifier and a host identifier. The IP address is shown in dotted-decimal notation with the decimal value of each octet separated by a period, for example, 192.168.7.27.</td>
</tr>
</tbody>
</table>
The Wireless Log window displays a log of recent activity, such as authentication, association, and DHCP renewal completion, in time order. Save the log to a file or clear the log. The auto-scroll feature automatically scrolls down when new items are added to the log.

To open the Wireless Log window, tap Wireless Log in the Wireless Status window. The Wireless Log window displays.

![Wireless Log Window](image)

**Figure 8-5  Wireless Log Window**

**Saving a Log**

To save a Wireless Log:

**Table 8-3  IPv4 Status Fields (Continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnet</td>
<td>Displays the mobile computer's subnet mask. Most TCP/IP networks use subnets to manage routed IP addresses. All IP addresses have a network part and a host part. The network part specifies a physical network. The host part specifies a host on that physical network. The subnet mask allows a network administrator to use some of the bits that are normally used to specify the host to instead specify physical sub-networks within an organization. This helps organize and simplify routing between physical networks.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Displays the gateway address. A gateway forwards IP packets to and from a remote destination.</td>
</tr>
<tr>
<td>DCHP Server</td>
<td>Displays the IP address of the DHCP server.</td>
</tr>
<tr>
<td>Lease Obtained</td>
<td>Displays the date and time that the IP address was obtained.</td>
</tr>
<tr>
<td>Lease Expires</td>
<td>Displays the date and time that the IP address expires.</td>
</tr>
<tr>
<td>DNS</td>
<td>Displays the IP address of the DNS server.</td>
</tr>
<tr>
<td>WINS</td>
<td>WINS is a Microsoft Net BIOS name server. WINS eliminates the broadcasts needed to resolve computer names to IP addresses by providing a cache or database of translations.</td>
</tr>
<tr>
<td>MAC</td>
<td>The IEEE 48-bit address is assigned to the mobile computer at the factory to uniquely identify the adapter at the physical layer.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Displays the name of the mobile computer.</td>
</tr>
</tbody>
</table>
1. Tap the Save button. The Save As dialog box displays.
2. Navigate to the desired folder.
3. In the Name field, enter a file name and then tap OK. The Wireless Log is saved as a text file in the selected folder.

**Clearing the Log**

To clear the log, tap Clear.

**Versions Window**

The Versions window displays software, firmware, and hardware version numbers.

To open the Versions window, tap Versions in the Wireless Status window.

![Versions Window](image)

**Figure 8-6  Versions Window**

- The window displays Fusion software version numbers as well as application and middleware version information.
Chapter 9 Wireless Diagnostics Application

Introduction

The **Wireless Diagnostics** application window provides links to perform ICMP Ping, Trace Routing, and Known APs functions. To open the **Wireless Diagnostics** window, tap the **Signal Strength** icon > **Wireless Diagnostics**.

![Figure 9-1 Wireless Diagnostics Window](image)

The **Wireless Diagnostics** window contains the following options. Tap the option to display the option window.

- **ICMP Ping** - tests the wireless network connection.
- **Trace Route** - tests a connection at the network layer between the mobile computer and any place on the network.
- **Known APs** - displays the APs in range using the same ESSID as the mobile computer.
- **Quit** - Exits the **Wireless Diagnostics** window.

Option windows contain a back button 🔵 to return to the **Wireless Diagnostics** window.

**ICMP Ping Window**

The **ICMP Ping** window allows testing of a connection at the network layer (part of the IP protocol) between the mobile computer and any other device on the network. Ping tests only stop when the **Stop Test** button is selected,
the Wireless Diagnostics application is closed, or if the mobile computer switches between infrastructure and ad-hoc modes.

To open the ICMP Ping window, tap ICMP Ping in the Wireless Diagnostics window.

![ICMP Ping Window](image)

**Figure 9-2  ICMP Ping Window**

To perform an ICMP ping:

1. In the **IP** field, enter an IP address or select an IP address from the drop-down list.
2. From the **Size** drop-down list, select a size value.
3. Tap **Start Test**. The ICMP Ping test starts. Information of the ping test displays in the appropriate fields.

The following statistics appear on the page:

- **Signal** - The current signal strength, measured in dBm, is provided both as a numerical value and as a histogram.
- **Noise** - The current noise level, measured in dBm, is provided both as a numerical value and as a histogram.
- **SNR** - The current signal to noise ratio, measured in dBm, is provided both as a numerical value and as a histogram.
- **Total Tx** - The total number of pings sent is displayed numerically.
- **Total Rx** - The total number of valid ping responses received is displayed numerically.
- **Lost** - The total number of pings that were lost is displayed numerically.
- **RT Times** - Four round trip times: Last, Average, Minimum, and Maximum are displayed in milliseconds.
- **% Rates** - For each of the 12 data rates, the number of times that rate was used to transmit the ping is displayed as a percentage.

**Graphs**

A real time graph of any of the above statistics can be displayed by double tapping on that statistic.
Trace Route Window

**Trace Route** traces a packet from a computer to a host, showing how many hops the packet requires to reach the host and how long each hop takes. The **Trace Route** utility identifies where the longest delays occur.

The **Trace Route** window allows testing a connection at the network layer (part of the IP protocol) between the mobile computer and any other device on the network.

To open the **Trace Route** window, tap **Trace Route** in the **Wireless Diagnostics** window.

In the IP combo box, enter an IP address or choose one from the drop-down list, or enter a DNS Name and tap **Start Test**. When starting a test, the trace route attempts to find all routers between the mobile computer and the destination. The Round Trip Time (RTT) between the mobile computer and each router appears, along with the total test time. The total test time may be longer than all RTTs added together because it does not only include time on the network.

**Known APs Window**

The **Known APs** window displays the APs in range using the same ESSID as the mobile computer. This window is only available in **Infrastructure** mode. To open the **Known APs** window, tap **Known APs** in the **Wireless Diagnostics** window.
Tap and hold on an AP to display a pop-up menu with the following options: Set Mandatory and Set Roaming.

Select Set Mandatory to prohibit the mobile computer from associating with a different AP. The letter M displays on top of the icon. The mobile computer connects to the selected AP and never roams until:

- Set Roaming is selected.
- Set Mandatory is selected on a different AP.
- Manually connecting to a profile from the Manage Profiles page.
- The mobile computer roams to a new profile.
- The mobile computer resumes after being suspended.
- The mobile computer resets (warm or cold).

Select Set Roaming to allow the mobile computer to roam to any AP with a better signal. These settings are temporary and never saved to the registry.

Tap Refresh to update the list of the APs with the same ESSID.
Chapter 10 Log On/Off Application

Introduction

When the user launches the Log On/Off application, the mobile computer may be in one of two states; the user may be logged onto the mobile computer by already entering credentials through the login box, or there is no user logged on. Each of these states has a separate set of use cases and a different look to the dialog box.

User Already Logged In

If already logged into the mobile computer, the user can launch the login dialog box for the following reasons:

• Connect to a different profile.
• Connect to and re-enable a cancelled profile. To do this:
  • Launch the Log On/Off dialog.
  • Select the cancelled profile from the profile drop-down list.
  • Login to the profile.

✓ NOTE A cancelled profile can also be re-enabled by using the Manage Profile window to connect to the cancelled profile.

• Log off the mobile computer to prevent another user from accessing the current users network privileges.
• Switch mobile computer users to quickly logoff the mobile computer and allow another user to log into the mobile computer.

No User Logged In

If no user is logged into the mobile computer, launch the login dialog box and log in to access user profiles.

The Login dialog box varies if it is:

• Launched by WCS, because the service is connecting to a new profile that needs credentials.
• Launched by WCS, because the service is trying to verify the credentials due to credential caching rules.
• Launched by a user, when a user is logged in.
• Launched by a user, when no user is logged in.

Tapping **OK** sends the credentials to the WCS. If there are no credentials entered, a dialog box displays asking the user to fill in all required fields.

The **Log Off** button only displays when a user is already logged on. When the **Log Off** button is tapped, the user is prompted with three options: Log Off, Switch Users, and Cancel. Switching users logs off the current user and re-initialize the login dialog box to be displayed for when there is no user logged on. Logging off logs off the current user and close the login dialog box. Tapping **Cancel** closes the Log Off dialog box and returns to the Login dialog box.

When the user is logged off, the mobile computer only roams to profiles that do not require credentials or to profiles that were created with the credentials entered into the profile.

The **Cancel** button closes the dialog without logging into the network. If the login dialog was launched by the WCS and not by the user, tapping **Cancel** first causes a message box to display a warning that the cancel will disable the current profile. If the user still chooses to cancel the login at this point, the profile is cancelled.

Once a profile is cancelled, the profile is suppressed until a user actively re-enables it or a new user logs onto the mobile computer.

### Table 10-1 Log On/Off Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Profile Field</td>
<td>When launching the login application, the Wireless Profile field has available all the wireless profiles that require credentials. This includes profiles that use EAP TLS, PEAP, LEAP, EAP-TTLS or EAP-FAST.</td>
</tr>
<tr>
<td>Profile Status Icon</td>
<td>The profile status icon (next to the profile name) shows one of the following states: The selected profile is cancelled. The selected profile is enabled but is not the current profile. The profile is the current profile (always the case for WCS Launched).</td>
</tr>
<tr>
<td>Username, Password, and Domain Name Fields</td>
<td>The <strong>Username</strong>, <strong>Password</strong>, and <strong>Domain Name</strong> fields are used as credentials for the profile selected in the Wireless Profile field. The <strong>Password</strong> fields is limited to 63 characters. The <strong>Username</strong> and <strong>Domain Name</strong> fields combined are limited to 63 characters. Note if any of the above field labels are red, then entry is mandatory; if the field labels are black, then entry is optional.</td>
</tr>
<tr>
<td>Mask Password Checkbox</td>
<td>The <strong>Mask Password</strong> checkbox determines whether the password field is masked (i.e., displays only the ‘*’ character) or unmasked (i.e., displays the entered text). Check the box to unmask the password. Uncheck the box to mask the password (the default).</td>
</tr>
<tr>
<td>Status Field</td>
<td>The status field indicates the reason the dialog is open.</td>
</tr>
</tbody>
</table>
Export options and profiles to provide cold boot persistence for Windows CE 5.0 devices and clean boot persistence for Mobile 5.0 devices. Save the exported registry files in the **Application** folder to use them on a cold boot or clean boot to automatically restore previous profile and option settings.

To save server certificates for persistence, save the certificate files in the folder **Application\RootCerts** to install the certificates automatically on a cold or clean boot.

User certificates that are installed into the Microsoft Certificate Store by the user, either through the Profile Editor Wizard or through the Fusion Certificate Manager application, are automatically saved in a special format to files in the **Application\UserCerts** folder. On a cold or clean boot, the user certificates will be automatically restored.
Chapter 12 Configuration Examples

Introduction

This chapter provides example procedures for configuring specific authentication and encryption types.

EAP–FAST/MS Chap v2 Authentication

To configure EAP-FAST and MS Chap v2 authentication:

1. Tap the Signal Strength icon to display the Wireless Applications menu.

2. Select Options. The Options window appears.

3. In the drop-down list, select Auto PAC Settings. The Auto PAC Settings window appears.
4. In the **Allow Provisioning** drop-down list, select **Yes**.
5. In the **Allow Refreshing** drop-down list, select **Yes**.
6. Tap **Save**.
7. Tap **ok**.
8. Tap the **Signal Strength** icon to display the **Wireless Applications** menu.
9. Select **Manage Profiles**. The **Manage Profiles** window appears.
10. Tap and hold in the window and select **Add** from the pop-up menu. The **Profile Editor** window appears.
11. In the **Profile Name** text box enter a name for the profile.
12. In the **ESSID** text box enter the ESSID.
13. Tap **Next**. The **Operating Mode** dialog box displays.
14. In the **Operating Mode** drop-down list, select **Infrastructure**.
15. In the **Country** drop-down list, select the country that the device is in.
16. Tap **Next**. The **Security Mode** dialog box displays.
17. In the **Security Mode** drop-down list, select **WPA2-Enterprise**.

![Authentication Dialog Box](image1)

**Figure 12-5 Authentication Dialog Box**

18. In the **Authentication** drop-down list, select **EAP-FAST**.

19. Tap **Next**. The **Tunneled Authentication Type** dialog box displays.

20. In the **Tunneled Authentication Type** drop-down list, select **MS CHAP v2**.

![Tunneled Authentication Dialog Box](image2)

**Figure 12-6 Tunneled Authentication Dialog Box**

21. Select the **Provide User Certificate** check box if a certificate is required.

22. Tap **Next**. The **Installed User Certificates** dialog box appears.

![Installed User Certificates Dialog Box](image3)

**Figure 12-7 Installed User Certificates Dialog Box**

23. Select a certificate from the drop-down list of currently installed certificates before proceeding. The selected certificate’s name appears in the drop-down list.

If the required certificate is not in the list, tap **Install Certificate**. See *User Certificate Installation on page 4-9* for information on installing User Certificates.

24. Tap **Next**. The **Install Server Certificate** dialog box appears.
25. Select a certificate from the drop-down list of currently installed certificates. The selected certificate’s name appears in the drop-down list.

If the required certificate is not in the list, tap **Install Certificate**. See *Server Certificate Installation on page 4-11* for information on installing Server Certificates.

26. Tap **Next**. The **User Name** dialog box appears.

The user name and password can be entered (but is not required) when the profile is created. If the username and password are not entered in the profile, then when attempting to connect, the user is be prompted to supply them. The entered information (credentials) will be saved (cached) for future reconnections.

27. Tap **Next**. The **Password** dialog box appears.

28. In the **Enter Password** text box, enter a password. Note that if a username was entered and no password is entered, Fusion assumes that no password is a valid password.

29. Select the **Advanced ID** check box, if advanced identification is desired.

30. Tap **Next**.

   If the **Advanced ID** is not selected, the **Prompt for Login** dialog box appears. Go to step XX.

   The **Advanced ID** dialog box appears.
31. Use the **Advanced ID** dialog box to enter the 802.1X identity to supply to the authenticator. This value can be 63 characters long and is case sensitive. In TTLS and PEAP, it is recommended entering the identity *anonymous* (rather than a true identity) plus any desired realm (e.g., anonymous@myrealm). A user ID is required before proceeding.

![Figure 12-11  Advanced Identity Dialog Box](image)

32. Tap **Next**. The **Prompt for Login** dialog box displays. See *Credential Cache Options on page 4-14* for detailed information on configuring Login settings.

![Figure 12-12  Prompt for Login at Dialog Box](image)

33. Tap **Next**. The **Encryption** dialog box displays.

34. In the **Encryption Type** drop-down list, select **AES**.

![Figure 12-13  Encryption Dialog Box](image)

35. Tap **Next**. The **IP Address Type** dialog box displays.

![Figure 12-14  IP Address Entry Dialog Box](image)
36. In the **IP Address Type** drop-down list, select **DHCP**.

37. Tap **Next**. The **Transmit Power** dialog box displays.

38. In the **Transmit Power** drop-down list select a power mode.

![Figure 12-15  Transmit Power Dialog Box](image)

39. Tap **Next**. The **Battery Usage** dialog box appears.

40. In the **Battery Usage Mode** dialog box select a power consumption option.

![Figure 12-16  Battery Usage Dialog Box](image)

41. Tap **Save**.
Glossary

A

API. An interface by means of which one software component communicates with or controls another. Usually used to refer to services provided by one software component to another, usually via software interrupts or function calls.

C

Clean Boot. See Cold Boot.

Cold Boot. A cold boot restarts the mobile computer and erases all user stored records and entries. The operating system is reloaded; files not stored in "protected" folders are erased; the registry is erased and reloaded from "REG" files saved in protected folders.

CCX. Cisco Compatible Extensions. A proprietary set of specified requirements that are used to improve the connectivity of mobile devices.

CCKM. Cisco's Central Key Management. Part of CCX, a proprietary methodology to enhance the connectivity during AP to AP roaming.

Cradle. A cradle is used for charging the terminal battery and for communicating with a host compute. It also provides a storage place for the terminal when not in use.

H

Hard Reset. See Cold Boot.

Host Computer. A computer that serves other terminals in a network, providing such services as computation, database access, supervisory programs and network control.
I

IEEE Address. See MAC Address.

I/O Ports. interface The connection between two devices, defined by common physical characteristics, signal characteristics, and signal meanings. Types of interfaces include RS-232 and PCMCIA.

Input/Output Ports. I/O ports are primarily dedicated to passing information into or out of the terminal’s memory. Series 9000 mobile computers include Serial and USB ports.

IP. Internet Protocol. The IP part of the TCP/IP communications protocol. IP implements the network layer (layer 3) of the protocol, which contains a network address and is used to route a message to a different network or subnetwork. IP accepts “packets” from the layer 4 transport protocol (TCP or UDP), adds its own header to it and delivers a “datagram” to the layer 2 data link protocol. It may also break the packet into fragments to support the maximum transmission unit (MTU) of the network.

IP Address. (Internet Protocol address) The address of a computer attached to an IP network. Every client and server station must have a unique IP address. A 32-bit address used by a computer on a IP network. Client workstations have either a permanent address or one that is dynamically assigned to them each session. IP addresses are written as four sets of numbers separated by periods; for example, 204.171.64.2.

K

Key. A key is the specific code used by the algorithm to encrypt or decrypt the data. Also see, Encryption and Decrypting.

M

MC. Mobile Computer.

MDN. Mobile Directory Number. The directory listing telephone number that is dialed (generally using POTS) to reach a mobile unit. The MDN is usually associated with a MIN in a cellular telephone -- in the US and Canada, the MDN and MIN are the same value for voice cellular users. International roaming considerations often result in the MDN being different from the MIN.

MIN. Mobile Identification Number. The unique account number associated with a cellular device. It is broadcast by the cellular device when accessing the cellular system.

Mobile Computer. In this text, mobile computer refers to a Zebra hand-held computer. It can be set up to run as a stand-alone device, or it can be set up to communicate with a network, using wireless radio technology.

O

Open System Authentication. Open System authentication is a null authentication algorithm.
**P**

**PAN.** Personal area network. Using Bluetooth wireless technology, PANs enable devices to communicate wirelessly. Generally, a wireless PAN consists of a dynamic group of less than 255 devices that communicate within about a 33-foot range. Only devices within this limited area typically participate in the network.

**Parameter.** A variable that can have different values assigned to it.

**PING.** (Packet Internet Groper) An Internet utility used to determine whether a particular IP address is online. It is used to test and debug a network by sending out a packet and waiting for a response.

---

**Q**

**QWERTY.** A standard keyboard commonly used on North American and some European PC keyboards. “QWERTY” refers to the arrangement of keys on the left side of the third row of keys.

---

**R**

**RAM.** Random Access Memory. Data in RAM can be accessed in random order, and quickly written and read.

**RF.** Radio Frequency.

**Router.** A device that connects networks and supports the required protocols for packet filtering. Routers are typically used to extend the range of cabling and to organize the topology of a network into subnets. See **Subnet**.

---

**S**

**Shared Key.** Shared Key authentication is an algorithm where both the AP and the MU share an authentication key.

**SID.** System Identification code. An identifier issued by the FCC for each market. It is also broadcast by the cellular carriers to allow cellular devices to distinguish between the home and roaming service.

**Soft Reset.** See **Warm Boot**.

**Subnet.** A subset of nodes on a network that are serviced by the same router. See **Router**.

**Subnet Mask.** A 32-bit number used to separate the network and host sections of an IP address. A custom subnet mask subdivides an IP network into smaller subsections. The mask is a binary pattern that is matched up with the IP address to turn part of the host ID address field into a field for subnets. Default is often 255.255.255.0.
**T**

TCP/IP. (Transmission Control Protocol/Internet Protocol) A communications protocol used to internetwork dissimilar systems. This standard is the protocol of the Internet and has become the global standard for communications. TCP provides transport functions, which ensures that the total amount of bytes sent is received correctly at the other end. UDP is an alternate transport that does not guarantee delivery. It is widely used for real-time voice and video transmissions where erroneous packets are not retransmitted. IP provides the routing mechanism. TCP/IP is a routable protocol, which means that all messages contain not only the address of the destination station, but the address of a destination network. This allows TCP/IP messages to be sent to multiple networks within an organization or around the world, hence its use in the worldwide Internet. Every client and server in a TCP/IP network requires an IP address, which is either permanently assigned or dynamically assigned at startup.

**Terminal.** See Mobile Computer.

**TFTP.** (Trivial File Transfer Protocol) A version of the TCP/IP FTP (File Transfer Protocol) protocol that has no directory or password capability. It is the protocol used for upgrading firmware, downloading software and remote booting of diskless devices.

**U**

UDP. User Datagram Protocol. A protocol within the IP protocol suite that is used in place of TCP when a reliable delivery is not required. For example, UDP is used for real-time audio and video traffic where lost packets are simply ignored, because there is no time to retransmit. If UDP is used and a reliable delivery is required, packet sequence checking and error notification must be written into the applications.

**W**

**Warm Boot.** A warm boot restarts the mobile computer and closes all running programs. All data that is not saved to flash memory is lost.
# Index

## Numerics

802.11 ESSID ............................................. 4-1

## A

ad-hoc ............................................... 4-2
ad-hoc networks .................................. 7-2
AES .................................................. 4-18
AP networks ....................................... 7-2
authentication
  EAP-TLS ........................................... 4-6
  LEAP ............................................. 4-7
  none ............................................. 4-6
  PEAP ............................................ 4-7

## B

bluetooth
  ad-hoc mode .................................... 4-2
bullets ............................................ x

## C

conventions
  notational ...................................... x
country code .................................... 4-2

## D

DCP .................................................. x
default gateway .................................. 4-21
Device Configuration Package .................. x
DNS .................................................. 4-21, 4-22

## E

EAP-TLS ............................................ 4-6
EMDK for C .......................................... x
encryption
  open system .................................... 4-17, 4-21
  TKIP (WPA) ...................................... 4-18
Enterprise Mobility Developer Kit for C .......... x

## G

gateway ............................................. 4-22

## I

information, service ................................ xi
infrastructure ..................................... 4-2
IP address ......................................... 4-22
IP config
  DNS ............................................ 4-22
gateway .......................................... 4-22
IP address ......................................... 4-22
subnet mask ....................................... 4-22
WINS ............................................... 4-22

## L

LEAP .................................................. 4-7

## M

mode
  802.11 ESSID .................................... 4-1
  ad-hoc .......................................... 4-2
country .......................................... 4-2
infrastructure .................................... 4-2
operating ......................................... 4-2
profile name ............................. 4-1

N
notational conventions .................... x

O
open system ............................. 4-17, 4-21
operating mode .......................... 4-2

P
PEAP .................................... 4-7
profile
  create new ............................ 3-3
  delete ................................. 3-4
  edit .................................. 3-3
  name .................................. 4-1

S
service information ......................... xi
signal strength ........................... 8-2
static .................................. 4-21
subnet mask .............................. 4-22

T
TKIP (WPA) ............................. 4-18

W
WINS .................................... 4-21, 4-22