© 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>-02 Rev. A</td>
<td>03/2015</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

Chapter 1: Getting Started
Introduction ........................................................................................................................................ 1-1
Configuring the Infrastructure ................................................................................................ .............. 1-1
Fusion Overview ................................................................................................................ 1-1
   Windows Mobile Home Screen ............................................................................................... 1-2
   Windows Classic Today Screen ............................................................................................. 1-2
Fusion Signal Strength Icon ................................................................................................................. 1-3
Fusion Functions .............................................................................................................. 1-4
   Enable/Disable Radio ...................................................................................................... 1-6
   Hide Menu ....................................................................................................................... 1-6
   Exit ............................................................................................................................... 1-7
   Fusion Help .................................................................................................................... 1-7
   Switching Between Fusion and WZC .............................................................................. 1-7
   More Information on WZC ............................................................................................. 1-7
Minimum Setup .................................................................................................................................... 1-8

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

Chapter 3: Manage Profiles Application
Introduction .................................................................................................................. 3-1
Connect to a Profile ........................................................................................................... 3-2
About This Guide

Introduction

This guide provides information about using the Fusion Wireless Companion software on a Zebra mobile computer.

NOTE Screens and windows pictured in this guide are samples and can differ from actual screens. This guide describes the functionality using Windows Mobile operating system. Functionality for the Windows CE operating system may differ.

Chapter Descriptions

Topics covered in this guide are as follows:

- Chapter 1, Getting Started provides an overview of the Fusion Wireless Companion software.
- 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 Fusion options.
- Chapter 8, Wireless Status Application describes how to get status about the wireless connection.
- Chapter 9, Wireless Diagnostics Application describes tools to help diagnose problems with 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 persist Fusion data and settings across a clean/cold boot.
- Chapter 12, Registry Controlled Features describes Fusion features that are controlled by registry settings.
- Chapter 13, Configuration Examples provides examples for setting up profiles with various authentication and encryption types.
Notational Conventions

The following conventions are used in this document:

- *Italics* are 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


For the latest version of this guide and all guides, go to: [http://www.zebra.com/support](http://www.zebra.com/support).
Chapter 1 Getting Started

Introduction

Each Zebra mobile computer has a wireless local area network (WLAN) interface. This WLAN interface is managed either by Fusion Wireless Companion or Windows Wireless Zero Config (WZC) application. The software allows the user to configure and control the wireless radio in order to securely connect to the WLAN infrastructure. This guide enables the user to configure the mobile computer so that it can connect properly to a WLAN. This guide describes how to use the Fusion software.

NOTE Fusion 3.20 does not support Zebra Value Added features.

- The following Fusion 3.00 features are not supported in Fusion 3.20:
  - WZC mode only supports a limited number of Fusion applications.

Configuring the Infrastructure

WLANs allow mobile computers to communicate wirelessly. Before using the mobile computer on a WLAN, the facility must be set up with the required hardware to run the WLAN (sometimes known as infrastructure). The infrastructure and the mobile computer must both be properly configured to enable this communication.

Refer to the documentation provided with the infrastructure (access points (APs), access ports, switches, Radius servers, etc.) for instructions on how to set up the infrastructure.

Once you have set up the infrastructure to enforce your chosen WLAN security scheme, use the Fusion or WZC software to configure the mobile computer to match.

Fusion Overview

The Fusion software contains applications with which to create wireless profiles. Each profile specifies the security parameters to use for connecting to a particular WLAN as identified by its ESSID. The Fusion software also allows the user to control which profile out of a set of profiles is used to connect. Other Fusion applications allow the user to monitor the status of the current WLAN connection and to invoke diagnostic tools for troubleshooting.
The Fusion applications are accessed differently depending upon the operating system configuration, Windows Mobile 6.5, by default, supports a Windows Home screen as well as the classic Mobile 6.1 Today screen. Devices may also contain an Enterprise Home screen that replaces the Windows Home screen.

**Windows Mobile Home Screen**

When the Windows Mobile Home screen is configured and Fusion is managing the WLAN, a Fusion plug-in displays on the Home screen to provide information about signal strength and profile name.

![Image of Windows Mobile Home Screen with Fusion Plug-in](image1)

**Figure 1-1** *Windows Mobile Home Screen with Fusion Plug-in*

When the Windows Mobile Home screen is configured and Windows is managing the WLAN, a Wireless Zero Config plug-in displays on the Home screen to provide information about signal strength and profile name.

![Image of Windows Mobile Home Screen with Wireless Zero Config Plug-in](image2)

**Figure 1-2** *Windows Mobile Home Screen with Wireless Zero Config Plug-in*

Tap the **Fusion Menu** tile to open the **Wireless Launcher** window.

**Windows Classic Today Screen**

When the Windows Mobile Classic Today screen is configured and Fusion is managing the WLAN, a Fusion signal strength icon appears in the Task tray.
When the Windows Mobile Classic Today screen is configured and Windows is managing the WLAN, a signal strength icon appears in the Task tray.

Tap the WZC Signal Strength icon to display the Wireless Launcher menu.

---

**Fusion Signal Strength Icon**

The shape and color of the **Signal Strength** icon provides information about the received wireless signal strength for the WLAN connection. *Table 1-1* describes the different icons and their meanings.

<table>
<thead>
<tr>
<th>Fusion Icon</th>
<th>WZC Icon</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Fusion Icon" /></td>
<td><img src="image2.png" alt="WZC Icon" /></td>
<td>Excellent signal strength</td>
<td>WLAN network is ready to use.</td>
</tr>
<tr>
<td><img src="image3.png" alt="Fusion Icon" /></td>
<td><img src="image4.png" alt="WZC Icon" /></td>
<td>Very good signal strength</td>
<td>WLAN network is ready to use.</td>
</tr>
<tr>
<td><img src="image5.png" alt="Fusion Icon" /></td>
<td><img src="image6.png" alt="WZC Icon" /></td>
<td>Good signal strength</td>
<td>WLAN network is ready to use.</td>
</tr>
</tbody>
</table>
Table 1-1  *Signal Strength Icon Descriptions (Continued)*

<table>
<thead>
<tr>
<th>Fusion Icon</th>
<th>WZC Icon</th>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Fusion Icon" /></td>
<td><img src="image2.png" alt="WZC Icon" /></td>
<td>Fair signal strength</td>
<td>WLAN network is ready to use. Notify the network administrator that the signal strength is only “Fair”.</td>
</tr>
<tr>
<td><img src="image3.png" alt="Fusion Icon" /></td>
<td><img src="image4.png" alt="WZC Icon" /></td>
<td>Poor signal strength</td>
<td>WLAN network is ready to use. Performance may not be optimum. Notify the network administrator that the signal strength is “Poor”.</td>
</tr>
<tr>
<td><img src="image5.png" alt="Fusion Icon" /></td>
<td><img src="image6.png" alt="WZC Icon" /></td>
<td>Out-of-network range (not associated)</td>
<td>No WLAN network connection. Notify the network administrator.</td>
</tr>
<tr>
<td><img src="image7.png" alt="Fusion Icon" /></td>
<td><img src="image8.png" alt="WZC Icon" /></td>
<td>The WLAN radio is disabled.</td>
<td>The WLAN radio is disabled. To enable, choose Enable Radio from the Wireless Applications menu.</td>
</tr>
<tr>
<td>None</td>
<td>None</td>
<td>The Wireless Launcher application was exited.</td>
<td>The Wireless Launcher application has been closed. See the Fusion Functions paragraphs below for how to restart the Wireless Launcher.</td>
</tr>
</tbody>
</table>

**Fusion Functions**

Tap the Signal Strength icon or tap Start > Wireless Companion > Wireless Launcher icon to display the Wireless Launcher menu.

![Wireless Launcher Menu](image9.png)

*Figure 1-5  Wireless Launcher Menu with Fusion Managing the WLAN*
Figure 1-6  *Wireless Launcher Menu with Windows Managing the WLAN*

Many of the items in the menu invoke one of the Fusion applications. These menu items and their corresponding applications are summarized in *Table 1-2*.

**Table 1-2  Supported Applications**

<table>
<thead>
<tr>
<th>Application</th>
<th>Description</th>
<th>Fusion Support</th>
<th>WZC Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Find WLANs</td>
<td>Invokes the Find WLANs application which displays a list of the WLANs available in your area.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Manage Profiles</td>
<td>Invokes the Manage Profiles application (which includes the Profile Editor Wizard) to manage and edit your list of WLAN profiles.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Wireless Zero Config</td>
<td>Invokes the Wireless Zero Config application list and configure the WLAN.</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Manage Certs</td>
<td>Invokes the Certificate Manager application which allows you to manage certificates used for authentication.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Manage PACs</td>
<td>Invokes the PAC Manager application which helps you manage the list of Protected Access Credentials used with EAP-FAST authentication.</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Options</td>
<td>Invokes the Options application which allows you to configure the Fusion option settings.</td>
<td>Yes</td>
<td>Yes*</td>
</tr>
<tr>
<td>Wireless Status</td>
<td>Invokes the Wireless Status application which allows you to view the status of the current wireless connection.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Wireless Diagnostics</td>
<td>Invokes the Wireless Diagnostics application which provides tools with which to diagnose problems with the wireless connection.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Log On/Off</td>
<td>Invokes the Network Login dialog which allows you to log on to a particular profile or to log off from the currently active profile</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

* Not all options and links are supported in WZC mode.
Each of the applications, except for WZC, has a chapter devoted to it in this guide.

Additional **Wireless Launcher** menu entries include:

- Enable/Disable Radio
- Hide Menu
- Exit.

### Enable/Disable Radio

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

![Classic Home Screen](image1.png) ![Windows Mobile Home Screen](image2.png)

**Figure 1-7  Disable Radio**

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

![Classic Home Screen](image3.png) ![Windows Mobile Home Screen](image4.png)

**Figure 1-8  Enable Radio**

Also note that the radio may be enabled or disabled using the **Wireless Manager** screen.

### Hide Menu

To hide the menu tap **Hide** in the menu.
Exit

Tap **Exit** to close the menu and exit the **Wireless Launcher** application. A dialog appears to confirm exiting the Wireless Launcher application. Tap **Yes** to exit. This closes the **Wireless Launcher** application and removes the **Signal Strength** icon from the screen.

To restart the **Wireless Launcher** application and redisplay the **Signal Strength** icon:

1. Tap **Start** > **Programs** > **Wireless Companion** icon > **Wireless Launch** icon.
2. Tap **ok** twice to close the windows.
3. The **Signal Strength** icon appears on the screen.

Fusion Help

To access the on-device Fusion Help tap **Start** > **Wireless Companion** > **Fusion Help**.

Switching Between Fusion and WZC

To switch from Fusion to WZC:

1. Tap **Start** > **Wireless Companion** > **Wireless Launch**.
2. Select **Options**.
3. Select **WLAN Management** from the drop-down list.
4. Select **Windows Manages WLAN** radio button.
5. Tap **Save**.
6. Tap **OK**.
7. Perform a reboot. Refer to the device’s User Guide for instructions.

To switch from WZC to Fusion:

1. Tap **Start** > **Wireless Companion** > **Wireless Launch**.
2. Select **Options**.
3. Select **WLAN Management** from the drop-down list.
4. Select **Fusion Manages WLAN** radio button.
5. Tap **Save**.
6. Tap **OK**.

More Information on WZC

For more information on Microsoft Wireless Zero Config, see the Microsoft Software Developer Network (MSDN) at http://msdn.microsoft.com.
Minimum Setup

Below is a list of the minimum effort to achieve a wireless connection. Note that there are many discrete nuances that may affect the performance of your wireless connection that might be missed if you do not consider them carefully.

You will need to create a profile. It is recommended that you read the profile editor chapter.

1. Find out from your IT administrator what the connection settings should be (Extended Service Set Identifier (ESSID), Enterprise or Personal, authentication type, tunnel type, certificate requirements, Protected Access Credentials (PAC) requirements). Note that not all of the items listed may be relevant.

2. Create the profile using the information provided by the IT administrator.

3. Enter the Manage Profile screen, select the profile (press and hold), and select the Connect option in the context menu that appears.
Chapter 2 Find WLAN Application

Introduction

**NOTE** Find WLAN application is available only when Fusion Manages WLAN is enabled in the Options application.

Use the Find WLANs application to discover available networks in the vicinity of your 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

The Find WLANs list displays:

- **WLAN Networks** - Available wireless networks, (both infrastructure and Ad-hoc) with icons that indicate signal strength and encryption. 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/Ad-hoc peer is transmitting.

- **Signal Strength** - The signal strength of the signal from the AP/Ad-hoc peer.
Tap-and-hold on a WLAN network to open a pop-up menu which provides three options: Connect to, Create profile and Refresh.

Select Connect to to view the list of existing profiles matching the select ESSID. The mobile computer connects to the given profile upon selection.

**NOTE** The number of WLANs (ESSIDs) that can be detected by the wireless radio at one time is limited. If you have a large number of WLANs active in your area, the Find WLANs window may not display them all.

If you do not see your ESSID, try a Refresh. If your ESSID is still not displayed and you wish to create or connect to a profile for it, you will need to use the Manage Profiles application.

### Table 2-1 Signal Strength Icon

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Icon" /></td>
<td>Excellent signal</td>
</tr>
<tr>
<td><img src="image2" alt="Icon" /></td>
<td>Very good signal</td>
</tr>
<tr>
<td><img src="image3" alt="Icon" /></td>
<td>Good signal</td>
</tr>
<tr>
<td><img src="image4" alt="Icon" /></td>
<td>Fair signal</td>
</tr>
<tr>
<td><img src="image5" alt="Icon" /></td>
<td>Poor signal</td>
</tr>
<tr>
<td><img src="image6" alt="Icon" /></td>
<td>Out of range or no signal</td>
</tr>
</tbody>
</table>

### Table 2-2 Encryption Icon

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image7" alt="Icon" /></td>
<td>No encryption. WLAN is an infrastructure network.</td>
</tr>
<tr>
<td><img src="image8" alt="Icon" /></td>
<td>WLAN is an Ad-hoc network.</td>
</tr>
<tr>
<td><img src="image9" alt="Icon" /></td>
<td>WLAN uses encryption. WLAN is an infrastructure network.</td>
</tr>
</tbody>
</table>

Figure 2-2 Find WLANs Menu.
Select **Create profile** to create a new WLAN profile for that network. This starts the **Profile Editor Wizard** which allows you to configure the security parameters that your mobile computer will use for the selected network. After editing the profile, the mobile computer automatically connects to this new profile.

![Figure 2-3 Warning Notice](image)

**NOTE** A warning displays when connecting to an unsecure (or open) network via the **Find WLANs** application. For open WLANs, the profile's settings will take on automatically generated default values. If you wish to manually configure the settings, uncheck the **Use Default configuration** checkbox.

Select **Refresh** to refresh the WLAN list.
Chapter 3 Manage Profiles Application

Introduction

**NOTE** Manage Profiles application is available only when Fusion Manages WLAN is enabled in the Options application.

A profile is a set of operating parameters that define how the mobile computer will connect to a specific WLAN. Create different profiles for use in different network environments. The Manage Profiles application displays the list of user-created wireless profiles. You may have a maximum of 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](image)

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>No Icon</td>
<td>Profile is not selected, but enabled.</td>
</tr>
<tr>
<td>Error</td>
<td>Profile is disabled.</td>
</tr>
</tbody>
</table>

Table 3-1 Profile Icons
You can perform various operations on the profiles in the list. To operate on an existing profile, tap and hold it 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.)

![Manage Profiles Context Menu](image)

**Figure 3-2**  *Manage Profiles Context Menu*

### Connect to a Profile

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 settings configured in the profile (i.e., authentication, encryption, ESSID, IP Config, power consumption, etc.) to connect to a WLAN.

**Editing a Profile**

Tap and hold a profile and select *Edit* from the pop-up menu. This will invoke the *Profile Wizard* where the profile settings are configured.

**Creating a New Profile**

To create a new profile tap and hold anywhere in the *Manage Profiles* window and select *Add* from the pop-up menu.

Selecting *Add* invokes 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.
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

The profiles are listed in priority order for use by the automatic Profile Roaming feature (see Profile Roaming below). Change the order by moving profiles up or down. Tap and hold a profile from the list and select Move Up or Move Down from the pop-up menu.

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.

Profile Roaming

Profile Roaming attempts to automatically select and connect to a profile from the profile list displayed in the Manage Profiles window. The Profile Roaming algorithm uses the order of the profiles in the profile list to determine the order in which profiles are tried.

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

The Profile Roaming algorithm makes two passes through the profile list. The first pass attempts to connect only to profiles that specify ESSIDs that can be detected by the wireless radio. If no connection is made, a second pass through the list is performed attempting to connect to those profiles that were not tried in the first pass. The Profile
Roaming algorithm will only attempt to connect to a profile for which it is not necessary to prompt the user for credentials (i.e., username and password). This includes:

- A profile that does not require credentials.
- A device profile. A device profile is one in which the username and password have been pre-entered directly into the profile. (A profile with the username specified but with the password field left empty is still considered a device profile since an empty password is considered a valid password.)
- A user profile with cached credentials. A user profile is one in which the username and password have not been pre-entered into the profile. A profile has cached credentials if the user has entered credentials for the profile via the Network Login dialog. When a profile has cached credentials, the user is said to have logged on to the profile. See Chapter 10, Log On/Off Application for more information.

The Profile Roaming algorithm will not attempt to connect to:

- A profile that specifies EAP-GTC for its Tunnel Authentication Type and Token (as opposed to Static) for its password type. See Tunneled Authentication on page 4-5 for more information.
- A user profile without cached credentials.
- A user profile that has cached credentials but that also has the At-Connect option enabled. See Credential Cache Options on page 4-13 for more information.
- A device profile that has cached credentials because the user has logged on to it (called a user-override profile), but that also has the At-Connect option enabled.
- A profile that has been disabled.
- A profile that has been cancelled.
- A profile whose Country setting does not allow the profile to be used in the country in which the mobile computer is being operated. See Operating Mode on page 4-2 for more information.

The Profile Roaming algorithm is invoked whenever the mobile computer becomes disconnected (disassociated) from the current WLAN.
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. An indicator in the bottom left corner tracks the number of pages traversed and total number of pages required to complete the current profile configuration. Tap X or the Cancel button 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 Name

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

![Profile Name Dialog Box](image-url)

Figure 4-1 Profile Name Dialog Box
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 4-1  Profile Name Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>The user-friendly name you wish to give the profile. The profile name is limited to 64 characters. Example: The Public LAN.</td>
</tr>
<tr>
<td>ESSID</td>
<td>The ESSID is the 802.11 extended service set identifier. The ESSID is a 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>

**NOTE**  Two profiles with the same user friendly name are acceptable but not recommended.

Tap Next. The Operating Mode dialog box displays.

**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.

![Ad-hoc Channel Selection Dialog Box](image)

**Figure 4-3**  Ad-hoc Channel Selection Dialog Box

<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>
</tbody>
</table>

**Table 4-3**  Ad-hoc Channels

2. Tap **Next**. The **Encryption** dialog box displays. See *Encryption on page 4-16* for encryption options.

---

**Security Mode**

*NOTE* Security Mode dialog box only appears when **Infrastructure** mode is selected in the **Operating Mode** dialog box.

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-104; and 802.1X authentications that use WEP-104 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 TKIP or Advanced Encryption Standard (AES) encryption method.

- **WPA - Enterprise** - This mode allows the user to configure profiles with 802.1X Authentication that uses WPA with TKIP encryption method.

- **WPA2 - Enterprise** - This mode allows the user to configure profiles with 802.1X Authentication that uses WPA2 with TKIP or AES encryption method.

**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)</td>
<td>Enabled for Authentication Type “None.” User input required with pass-phrase/hex key configuration. Disabled for all other Authentication Types. No user input required for encryption key.</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>TKIP 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>TKIP 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>
<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 Protected Access Credential (PAC) 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 and the RADIUS server settings, require a user certificate and the validation of a server certificate.</td>
</tr>
<tr>
<td>PEAP</td>
<td>Select this option to enable PEAP authentication. This type establishes a tunnel and then based on the tunnel type, uses a user certificate and/or a username/password. Validating the server certificate is optional.</td>
</tr>
<tr>
<td>LEAP</td>
<td>Select this option to enable LEAP authentication. This type does not establish a tunnel. It requires a username and password.</td>
</tr>
<tr>
<td>TTLS</td>
<td>Select this option to enable TTLS authentication. This type establishes a tunnel in which the username/password are verified. A user certificate may optionally be used. Validating the server certificate is also optional.</td>
</tr>
</tbody>
</table>

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 Provide 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>CHAP</td>
<td>PEAP: X</td>
<td>Challenge Handshake Authentication Protocol (CHAP) is one of the two main authentication protocols used to verify the user name and password for Point-to-Point (PPP) Internet connections. CHAP is more secure than Password Authentication Protocol (PAP) because it performs a three way handshake during the initial link establishment between the home and remote machines. It can also repeat the authentication anytime after the link is established.</td>
</tr>
<tr>
<td></td>
<td>TTLS: X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EAP-FAST: X</td>
<td></td>
</tr>
<tr>
<td>EAP-GTC</td>
<td>PEAP: X</td>
<td>Extensible Authentication Protocol-Generic Token Card (EAP-GTC) is used during phase 2 of the authentication process. This method uses a time-synchronized hardware or software token generator, often in conjunction with a user PIN, to create a one-time password.</td>
</tr>
<tr>
<td></td>
<td>TTLS: X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EAP-FAST: X</td>
<td></td>
</tr>
<tr>
<td>MD5</td>
<td>PEAP: X</td>
<td>Message Digest-5 (MD5) is an authentication algorithm developed by RSA. MD5 generates a 128-bit message digest using a 128-bit key, IPSec truncates the message digest to 96 bits.</td>
</tr>
<tr>
<td>MS CHAP</td>
<td>PEAP: X</td>
<td>Microsoft Challenge Handshake Authentication Protocol (MS CHAP) is an implementation of the CHAP protocol that Microsoft created to authenticate remote Windows workstations. MS CHAP is identical to CHAP, except that MS CHAP is based on the encryption and hashing algorithms used by Windows networks, and the MS CHAP response to a challenge is in a format optimized for compatibility with Windows operating systems.</td>
</tr>
</tbody>
</table>
User Certificate Selection

If the user checked the Provide 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

NOTE User Certificates can also be installed using the Manage Certificates Application. See Chapter 5, Manage Certificates Application for more information.

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 .pfx file that has been manually placed on the device.

To install a user certificate from the CA:

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

![Figure 4-7 Import Certificate Dialog Box](image)

2. Select Import User Cert from Server and tap OK. The Install from Server dialog box appears.

![Figure 4-8 Install from Server Dialog Box](image)

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 from a server, the mobile computer must already be connected to a network from which that server is accessible.

To install a user certificate from a .pfx file:

1. Tap Install Certificate. The Import Certificate dialog box appears.
2. Choose **Import from File** and tap **OK**.  

   The **Open** dialog box appears.

3. In the **Type** drop-down list, select **Certificates (.cer, .pfx)**.

   ✓  **NOTE** Installing a user certificate from a file requires that the file be of type *.pfx*.

4. Browse to the desired .pfx file and tap **OK**.  

   The **Personal Certificate** dialog box appears.

5. If the .pfx file is password protected, enter the appropriate password; else leave the password fields empty.  

   Deselect the **Hide Password** check box to see the password characters as they are entered.

6. Tap **OK**. The certificate(s) are imported.
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 hourglass may appear as the wizard populates the existing certificate list. If the required certificate is not listed, install it.

![Installed Server Certificates Dialog Box](image)

Figure 4-12 Installed Server Certificates Dialog Box

Server Certificate Installation

> **NOTE** Server Certificates can also be installed using the Manage Certificates Application. See Chapter 5, Manage Certificates Application for more information.

A server certificate can only be installed from either a .cer file or a .pfx file that has been loaded onto the device. The certificate file can be loaded either manually or via a web-browser-based interface to the Certificate Authority (CA).

> **NOTE** To successfully install a server certificate from a CA using a web-browser, the mobile computer must already be connected to a network from which that CA is accessible. The procedure you should follow to download the server certificate from the CA is beyond the scope of this guide.

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 Certificate Dialog Box](image)

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.

**User Name**

The user name and password can optionally be entered when the profile is created (called a device profile) or they can be left empty (called a user profile). 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 a profile is a device or a user profile affects how the profile is treated during a Profile Roaming operation (see Profile Roaming on page 3-4). Profiles are excluded from profile roaming 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 Encryption on page 4-16), 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).

If the Static radio button is selected, 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.

---

**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. For TTLS,EAP-FAST, and PEAP authentication types, it is recommended entering the identity anonymous (rather than a true identity). You can optionally enter a fully qualified domain (e.g., mydomain.local) and it will automatically be combined with the 802.1x identity (i.e., anonymous@mydomain.local) before being sent to the RADIUS server.

Entering an 802.11x Identity is required before proceeding.

![Advanced Identity Dialog Box](image)

**Figure 4-19 Advanced Identity Dialog Box**

Tap Next. The Encryption dialog box displays.

---

**Credential Cache Options**

When connecting to a password-based user profile for the first time, Fusion will prompt the user to enter credentials. After the credentials have been entered, they are cached. These cached credentials will normally be used, without prompting the user, whenever Fusion reconnects to that profile. The credential caching options allow the administrator to specify additional circumstances under which Fusion will prompt the user to re-enter the credentials even though it already has cached credentials for the given profile. Requiring the user to re-enter credentials can help ensure that only an authorized user is using the device.

The credential caching options are at connection, on each resume, or at a specified time.
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 the mobile computer prompt for credentials each time it tries to connect. 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 entered credentials. If the infrastructure has implemented a fast reconnect technology such as Fast Session Resume, or PMKID caching then selecting this option will prevent that technology from working properly by prompting the user for credentials when attempting to reconnect.</td>
</tr>
<tr>
<td>On Resume</td>
<td>Select this option to cause an authenticated user to be reauthenticated when a suspend/resume occurs. The mobile computer uses the cached credentials to authenticate. Once authenticated, the user is prompted for credentials. If the user does not enter matching credentials within three attempts, the user is disconnected from the network. This option only applies when the user has previously entered credentials. If the infrastructure has implemented a fast reconnect technology such as Fast Session Resume, or PMKID caching then selecting this option will prevent that technology from working properly by prompting the user for credentials when attempting to reconnect.</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 entered credentials.</td>
</tr>
</tbody>
</table>
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 may be prompted for credentials even when credentials have already been entered and cached for that profile.

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 mode are Open, WEP-40 and WEP-104.

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 only includes encryption methods available for the selected security mode and authentication type.

![Encryption Dialog Box]

Based on the encryption method and the authentication type, the user may have to manually enter pre-shared encryption keys (or a pass 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. This encryption method is only available for the Legacy security mode with Authentication Type set to None. Note: This is alternately referred to as WEP-64.</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. This encryption method is available for the Legacy security mode. Note: This is alternately referred to as WEP-128.</td>
</tr>
</tbody>
</table>
For all Encryption types other than Open, if authentication is set to None, then the wizard displays additional controls for entering pre-shared keys (see Figure 4-23 on page 4-16). This includes Personal security modes, which default to authentication None and exclude Enterprise security modes, which require an authentication type to be specified.

- Select the Pass-phrase or Hexadecimal Keys radio button to indicate whether a pass-phrase or hexadecimal keys will be entered on the next page.
- Select the For added security - Mask characters entered check box to hide characters entered. Deselect this to show characters entered.

<table>
<thead>
<tr>
<th>Encryption</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TKIP</td>
<td>Select TKIP for the adapter to use the Temporal Key Integrity Protocol (TKIP) encryption method. This encryption method is available for all security modes other than Legacy. When TKIP is selected, Mixed Mode support is automatically enabled. The Allow Mixed Mode checkbox is enabled and grayed out. This is true for all security modes that allow TKIP as an encryption method. This means that the mobile computer will operate in an environment in which TKIP is used for encrypting the unicast traffic, and either TKIP or WEP-104 is used for encrypting multicast/broadcast traffic. This allows the mobile computer to operate with an AP that is set up to support both WPA and legacy mobile computers simultaneously.</td>
</tr>
<tr>
<td>AES</td>
<td>Select AES for the adapter to use the Advanced Encryption Standard (AES) encryption method. This encryption method is available for the WPA2 - Enterprise and WPA2 - Personal security modes. When AES is selected, Mixed Mode support is automatically enabled. The Allow Mixed Mode checkbox is enabled and grayed out. This means that the mobile computer will use only AES encryption for unicast traffic, but allows it to use either AES, TKIP, or WEP-104 encryption for broadcast traffic. This allows the mobile computer to operate with an AP that is set up to support legacy and/or WPA and WPA2 mobile computers simultaneously.</td>
</tr>
</tbody>
</table>

For all Encryption types other than Open, if authentication is set to None, then the wizard displays additional controls for entering pre-shared keys (see Figure 4-23 on page 4-16). This includes Personal security modes, which default to authentication None and exclude Enterprise security modes, which require an authentication type to be specified.

- Select the Pass-phrase or Hexadecimal Keys radio button to indicate whether a pass-phrase or hexadecimal keys will be entered on the next page.
- Select the For added security - Mask characters entered check box to hide characters entered. Deselect this to show characters entered.

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Encryption / Authentication Matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open</td>
<td>WEP</td>
</tr>
<tr>
<td>Legacy (Pre-WPA)</td>
<td>Yes</td>
</tr>
<tr>
<td>EAP-TLS</td>
<td>WEP-104</td>
</tr>
<tr>
<td>EAP-FAST</td>
<td>WEP-104</td>
</tr>
<tr>
<td>PEAP</td>
<td>WEP-104</td>
</tr>
<tr>
<td>LEAP</td>
<td>WEP-104</td>
</tr>
<tr>
<td>TTLS</td>
<td>WEP-104</td>
</tr>
</tbody>
</table>
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** 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 **IPv4 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 IPv4 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.

To enter a pass-phrase key without characters hidden:

1. Tap Next.

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 field, re-enter the key. When the keys match, a message appears indicating that the keys match.

5. Tap Next. The IPv4 Address Entry dialog box displays.
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 **IPv4 Address Entry** dialog box displays.

---

**IPv4 Address Entry**

Use the **IPv4 Address Entry** dialog box to configure network address parameters: IP address, subnet mask, gateway, DNS, and WINS.

---

**Table 4-10** IPv4 Address Entry

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtain Device IP Address</td>
<td>Check to obtain a leased IP address and network configuration information from a remote automatically</td>
</tr>
<tr>
<td>Address Automatically</td>
<td>Uncheck to manually assign IP, subnet mask and default gateway addresses the mobile computer profile uses.</td>
</tr>
<tr>
<td>Ad-hoc mode does not support DHCP. Use only Static IP address assignment.</td>
<td></td>
</tr>
</tbody>
</table>
Select all three check boxes to automatically obtain addresses from a remote server. Tap Next. The **Transmit Power** dialog box displays.

Uncheck the **Obtain Device IP Address Automatically** to manually assign IP, subnet mask and default gateway addresses the mobile computer profile uses. Tap **Next**. The **Static IP Address** dialog box appears.

![Figure 4-29](image)  
**Static IP Address Entry Dialog Box**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IPv4 Address</strong></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><strong>Subnet Mask</strong></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>
<tr>
<td><strong>Gateway</strong></td>
<td>The default gateway forwards IP packets to and from a remote destination.</td>
</tr>
</tbody>
</table>
Select the Set Static DNS Address or Set static WINS address check box, then tap Next to display the DNS/WINS Address Entry dialog box. Enter the DNS and/or WINS addresses here. Tap Next without selecting the Set Static DNS Address or Set static WINS Address check box to display the Transmit Power dialog box.

Table 4-11  Static IP Address Entry Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Static DNS Address (Optional)</td>
<td>Check to manually assign DNS server addresses.</td>
</tr>
<tr>
<td>Set Static WINS Address (Optional)</td>
<td>Check to manually assign WINS server addresses.</td>
</tr>
</tbody>
</table>

Select the Set Static DNS Address or Set static WINS address check box, then tap Next to display the DNS/WINS Address Entry dialog box. Enter the DNS and/or WINS addresses here. Tap Next without selecting the Set Static DNS Address or Set static WINS Address check box to display the Transmit Power dialog box.

The IP information entered in the profile is only used if the Enable IPv4 Mgmt check box in the Options > System Options dialog box was selected (System Options on page 7-2). If not selected, the IP information in the profile is ignored and the IP information entered in the Microsoft interface applies.

Table 4-12  DNS/WINS Address Entry Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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. The Alternate DNS server address will be used if the Preferred DNS server is unavailable.</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. The Alternate WINS server address will be used if the Preferred WINS server is unavailable.</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.
Figure 4-31  Transmit Power Dialog Box (Ad-hoc Mode)

Table 4-13  Power Transmit Options (Ad-hoc Mode)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full</td>
<td>Select Full power for the highest transmission power level. Select Full 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 30 mW 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 15 mW to set the maximum transmit power level to 15 mW. The radio transmits at the minimum power required.</td>
</tr>
<tr>
<td>5 mW</td>
<td>Select 5 mW to set the maximum transmit power level to 5 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 and options are disabled (grayed-out).

Figure 4-32  Battery Usage Dialog Box

NOTE  Power consumption is also related to the transmit power settings.
When the AP that the mobile computer associates to is configured to use WMM Power Save mode, the mobile computer will ignore the Battery Usage Mode setting – assuming it’s not set to CAM – and will use the WMM protocol instead. While the use of WMM Power Save mode can maximize battery life, it can also decrease network performance.

**NOTE** WMM Power Save mode will override Fast Power Save and MAX Power Save mode and cannot be disabled.
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.

![Certificate Manager Window](image)

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.
Figure 5-2  Certificate Type Options

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.

Figure 5-3  Command Buttons and Context Menu

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.
Figure 5-4  Certificate Properties Window

Tap ok, Escape, or X button to exit (depending on the mobile computer).

Import a Certificate

Import certificates from either files or from a server machine:

- .CER file - DER encrypted Root/Server certificates.

   ✓  In order to validate a server certificate for an Intermediate CA during authentication, it is only necessary to import the certificate from the associated Root CA and then specify the Root CA in the profile.

- .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.

   ✓  It is possible to import and successfully use a user certificate issued by an Intermediate CA; however, this may require additional infrastructure setup. For example, it may be necessary to supply the RADIUS server with certificates for both the Intermediate CA and for the Root CA. Infrastructure setup is beyond the scope of this guide.

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

Figure 5-5  Import Certificate Dialog Box

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  Certificate Dialog Box - Delete Certificate

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.

Figure 6-1  PAC Manager Window

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, Import and Delete commands.

NOTE  Manage PACs application is available only when Fusion Manages WLAN is enabled in the Options application.
You can always sort by A-ID, sort by I-ID, view buttons and hide buttons in the pop-up menu.

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

**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 display in the lower list of the window.

![Figure 6-3 PAC Properties Popup](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.
Import PAC

Usually PACs are automatically provisioned to the mobile computer over the air the first time EAP-FAST authentication occurs. For increased security, an administrator may choose to manually provision the mobile computer with a PAC instead. In this case, the administrator must generate an appropriate PAC file manually using commands on the PAC Authority. Once the PAC file is generated, it must be manually transferred to the mobile computer’s file system before it can be imported by the Manage PACs application.

To import a PAC, tap the **Import** button. A dialog displays asking you to select the PAC file to be imported.

Navigate to the file to be imported and choose it. The **Import PAC** dialog displays.

If the PAC file is password protected, enter the password in the **Password** field. If you uncheck the **Hide Password** checkbox, the password will be displayed in clear text as you type it. To hide the password as you type it, leave the **Hide Password** checkbox checked. If you wish to overwrite any existing PAC in the Fusion PAC Store without being prompted for verification, check the **Overwrite PAC if Exists** checkbox. Tap the **Ok** button to import the PAC. Tap the **Cancel** button to abort the import operation.

If you have tapped **Ok** and the PAC already exists in the PAC Store, a verification dialog box may appear. Tap **Yes** to continue the import operation or tap **No** to abort the operation. If you have tapped **Yes**, an informational dialog box appears listing the attributes (A-ID and I-ID) of the imported PAC.
Figure 6-6  *Import PAC File Dialog Box*

Tap **ok** to close the dialog box. You will be returned to the main **PAC Manager** window with the tree list of PACs. The newly-imported PAC should appear in the list.
Chapter 7 Options

Introduction

Use the wireless Option dialog box to select one of the following operation options from the drop-down list. The options listed vary depending upon if Fusion or Windows manages the WLAN:

- Op Mode Filtering (Fusion manages WLAN)
- System Options (Fusion manages WLAN)
- Auto PAC Settings (Fusion manages WLAN)
- IPv6 (Fusion manages WLAN)
- WLAN Management
- Change Password
- Export.

Change the option settings as you desire and then tap SAVE to save your changes. Until you tap the SAVE button, no changes are saved. To close the dialog, tap ok. If you tap ok and you have made changes without saving them, a dialog will display asking if you want to quit without saving.

Op (Operating) Mode Filtering

NOTE  Op Mode Filtering option is available only when Fusion Manages WLAN is enabled.

The Op 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.

Table 7-1  OP Mode Filtering Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP Networks</td>
<td>Select the AP Networks check box to display available AP networks and their signal strength within the Available WLAN Networks (see Chapter 2, Find WLAN Application). These are the APs in the vicinity available to the mobile computer for association. If this option was previously disabled, refresh the Available WLAN Networks window to display the AP networks available to the mobile computer. Default: Enabled.</td>
</tr>
<tr>
<td>AD-Hoc Networks</td>
<td>Select the Ad-Hoc Networks check box to display available peer (adapter) networks and their signal strength within the Available WLAN Networks. These are peer networks in the vicinity that are available to the mobile computer for association. If this option was previously disabled, refresh the Available WLAN Networks window to display the Ad Hoc networks available to the mobile computer. Default: Enabled</td>
</tr>
</tbody>
</table>

System Options

*NOTE* System option is available only when Fusion Manages WLAN is enabled.

Use System Options to set miscellaneous system setting.

Figure 7-2  System Options Dialog Box
Table 7-2  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. Default: Enabled</td>
</tr>
<tr>
<td>Enable IPv4 Mgmt</td>
<td>Enables the Wireless Companion Services to handle IPv4 address management. The Wireless Companion Service configures the IP based on what is configured in the network profile. Deselect this to manually configure the IP in the standard Windows IP window. Default: Enabled</td>
</tr>
</tbody>
</table>

Auto PAC Settings

- **NOTE**  Auto PAC Settings option is available only when **Fusion Manages WLAN** is enabled.

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

![Auto PAC Settings Dialog Box](image)

Table 7-3  Auto PAC Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Provisioning</td>
<td>Select <strong>Yes</strong> from the drop down list to allow the mobile computer to be automatically provisioned with a PAC when using the EAP-FAST authentication protocol. Select <strong>No</strong> to disallow automatic PAC provisioning. Default: No</td>
</tr>
<tr>
<td>Allow Refreshing</td>
<td>Select <strong>Yes</strong> from the drop down list to allow an existing PAC on the mobile computer to be automatically refreshed when using the EAP-FAST authentication protocol. Select <strong>No</strong> to disallow automatic PAC refreshing. Default: No</td>
</tr>
</tbody>
</table>

If the master key on the PAC Authority has expired then the PAC on the mobile computer that was generated with this expired key will have to be manually deleted and a new PAC provisioned even when **Allow Refreshing** is set to **Yes**.
IPv6

**NOTE** IPv6 option is available only when Fusion Manages WLAN is enabled. When Windows Manages WLAN is enabled, IPv6 is always enabled.

Use the IPv6 options to enable or disable IPv6 for WLAN.

![IPv6 Options Dialog Box](image)

**Table 7-4 IPv6 Options**

<table>
<thead>
<tr>
<th>Enable IPv6</th>
<th>Select the Enable IPv6 check box to enable IPv6 for WLAN. Default: Disabled</th>
</tr>
</thead>
</table>

**WLAN Management**

Use WLAN Management to select which WLAN software will manage the WLAN.

![WLAN Management Window](image)

Select Fusion Manages WLAN to allow the Fusion application to manage the WLAN.

Select Windows Manages WLAN to allow the Microsoft Zero Config application to manage the WLAN and then tap Save.

A dialog box displays indicating that the device has to be re-booted. Tap OK.

The WLAN Management options are then disabled.

After changing the WLAN Management option, a reset of the device is required.

**Change Password**

Use Change Password to require that a user enter a password before being allowed to access certain Fusion functions. The functions that are password protected include:
• Find WLANs
• Manage Profiles
• Manage Certs
• Manage PACs
• Options.

Having a password prohibits an un-trusted user from, for example, creating or editing a profile or changing 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.

![Change Password Window](image)

**Figure 7-6 Change Password Window**

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 devices, exporting options enables settings to persists after cold boot. For Windows Mobile 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.

![Options - Export Dialog Box](image)

**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:

![Figure 7-8 Export Options Save As Dialog Box](image)

**NOTE** Export Profile is available only when **Fusion Manages WLAN** is enabled.

To export only one profile, see *Export a Profile on page 3-4* for more information.

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

![Figure 7-9 Export All Profiles Save As Dialog Box](image)

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.

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.
- IPv6 Status – displays IPv6 status and IPv6 related information assigned to the WLAN interface of the mobile computer.
- Wireless Log - displays a log of important recent activity, such as authentication, association, and DHCP renewal completion, in time order.
- Logos & Certification – Displays logos and certificates
- 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)

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

### Table 8-1 Signal Strength Status

<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>![Out of Range (no signal)]</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="The radio card is off or there is a problem communicating with the radio card." /></td>
</tr>
<tr>
<td>Profile Name</td>
<td>Displays the name of the current profile.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates if the mobile computer is associated with the AP.</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>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>
<tr>
<td>Signal Level</td>
<td>The AP signal level 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 (available only when Fusion manages WLAN).</td>
</tr>
<tr>
<td>Mode</td>
<td>Displays the current profile’s mode, either Infrastructure or Ad-hoc. See Table 4-2 on page 4-2.(available only when Fusion manages WLAN).</td>
</tr>
<tr>
<td>Security Mode</td>
<td>Displays the current profile’s security mode. See Table 4-4 on page 4-4.(available only when Fusion manages WLAN).</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. Tap Export to export IPv4 status information to a text file. 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.

![IPv4 Status Window](image)
The IPv6 Status window displays IPv6 status, current IPv6 addresses and other IPv6 related information assigned to the WLAN interface. It also allows resetting the IPv6 address. The IPv6 Status window updates automatically when the IPv6 address changes.

Tap Reset to initiate IPv6 reset. Reset forces the TCP/IPv6 stack to re-bind to the WLAN interface. During re-bind, IPv6 stack discards its current IPv6 configuration and starts a fresh address auto configuration.

Tap Export to export IPv6 status information to a text file.

To open the IPv6 Status window, tap IPv6 Status in the Wireless Status window.
Double tap on a device **IPv6 Addresses** or **Temporary IPv6 address** to get more detailed information.

![IPv6 Status Window](image)

**Figure 8-5  IPv6 Status Window**

**Table 8-4  IPv6 Status Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
<td>Indicates whether IPv6 is enabled or disabled for the WLAN interface. You can enable or disable IPv6 from <strong>Options &gt; Enable IPv6</strong>, see IPv6 on page 7-4.</td>
</tr>
<tr>
<td><strong>IPv6 Addresses</strong></td>
<td>Displays the mobile computer’s IPv6 addresses assigned to WLAN interface. Displays all IPv6 addresses except Temporary IPv6 address. For each IPv6 address, it shows the scope (link local/site local/global/unknown) and remaining valid lifetime of the address.</td>
</tr>
<tr>
<td><strong>Temporary IPv6 Address</strong></td>
<td>Displays the mobile computer's Temporary IPv6 address assigned to WLAN interface. It displays the scope and remaining valid lifetime of the address. Temporary IPv6 addresses are based on random interface identifiers and are generated for public address prefixes that use stateless address auto configuration.</td>
</tr>
<tr>
<td><strong>Gateway</strong></td>
<td>Displays the IPv6 address of the gateway. A gateway forwards IP packets to and from a remote destination.</td>
</tr>
<tr>
<td><strong>DNS</strong></td>
<td>Displays the IPv6 address of the DNS server.</td>
</tr>
<tr>
<td><strong>MAC</strong></td>
<td>The IEEE 48-bit address is assigned to the network adapter at the factory to uniquely identify the adapter at the physical layer.</td>
</tr>
<tr>
<td><strong>Host Name</strong></td>
<td>Displays the name of the mobile computer.</td>
</tr>
</tbody>
</table>
Wireless Log Window

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.

### Table 8-5  IPv6 Address Details Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 Address</td>
<td>Displays the IPv6 address for which details are displayed.</td>
</tr>
<tr>
<td>Prefix origin</td>
<td>Displays the prefix origin for the IPv6 address. Possible values are Router Advertisement, Well-known, Manual, DHCPv6 or Unknown source.</td>
</tr>
<tr>
<td>Suffix origin</td>
<td>Displays the suffix origin for the IPv6 address. Possible values are Link layer address, Random, Well-known, Manual, DHCPv6 or Unknown source.</td>
</tr>
<tr>
<td>DAD state</td>
<td>Displays the Duplicate Address Detection state for the IPv6 address. Possible values are Preferred, Tentative, Deprecated, Duplicate or Invalid.</td>
</tr>
<tr>
<td>Preferred Lifetime (Remaining)</td>
<td>Displays the amount of time this address will remain in the Preferred state.</td>
</tr>
</tbody>
</table>
Saving a Log

To save a Wireless Log:

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**.

Logos & Certifications Window

The **Logos & Certifications** window displays a list of logos and compliance standards supported by this device, such as Wi-Fi Interoperability and Cisco Compatible Extensions. Select an item in the list to view the corresponding certificate. For a list of supported standards, see *Table 8-6 on page 8-9*.

![Logos & Certifications Window](Image)

**Figure 8-8** Logos & Certifications Window

- When viewing the certificate, controls to adjust the zoom and scroll are available.
- For certain certificates a link is available to view the certificate in a browser, if an internet connection is available.
- Supported standards are as follows:
The **Versions** window displays software, firmware, and hardware version numbers.

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

- The window displays Fusion software version numbers as well as application and middleware version information.
- Tap **Export** to export version information to a text file.
- Tap **Export FusionPublicApi.h** to export the current version of the FusionPublicAPI.h header file to the specified location.

### Table 8-6  Logos & Certifications

<table>
<thead>
<tr>
<th>Certification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wi-Fi Association</td>
<td>This certificate indicates the device has passed Wi-Fi Alliance interoperability tests.</td>
</tr>
<tr>
<td>Windows Mobile Logo</td>
<td>This certificate indicates the device has passed the Windows Mobile Logo test.</td>
</tr>
</tbody>
</table>

### Versions Window

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

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

- The window displays Fusion software version numbers as well as application and middleware version information.
- Tap **Export** to export version information to a text file.
- Tap **Export FusionPublicApi.h** to export the current version of the FusionPublicAPI.h header file to the specified location.

### Table 8-7  Version Sub-categories

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>Version information for Wireless Fusion Enterprise Mobility Suite applications.</td>
</tr>
<tr>
<td>Middleware</td>
<td>Version information for Wireless Fusion Enterprise Mobility Suite middleware components.</td>
</tr>
<tr>
<td>WLAN Adapters</td>
<td>Version and type information for WLAN adapters and the corresponding firmware and drivers.</td>
</tr>
<tr>
<td>Interface</td>
<td>Version and type information for the device’s interface to the WLAN adapter and the corresponding firmware.</td>
</tr>
<tr>
<td>Device</td>
<td>Device model and identification numbers.</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System version information.</td>
</tr>
</tbody>
</table>
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

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](image1)

**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:

- IPv4 Address or IPv6 Address – Target IP address.
- Signal - The current signal strength, 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.

Use the **DNS Lookup Options** button to select the name resolution priority. Select the option and tap **OK** button. If a name is entered in the IP field, DNS Lookup Options setting will decide whether to use IPv4 or IPv6 address for the test. By default, this is set to IPv4 then IPv6, which indicates that it will try to resolve the name to an IPv4 address; if this fails and if IPv6 is enabled, it will try to resolve the name to an IPv6 address.

![DNS Lookup Options Window](image2)

**Figure 9-3  DNS Lookup Options Window**
Graphs

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

![Graph Example](image)

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.

![Trace Route Window](image)

In the **IP** drop-down list, 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.

Use the **DNS Lookup Options** button to select the name resolution priority. Select the option and tap **OK** button. If a name is entered in the IP field, DNS Lookup Options setting will decide whether to use IPv4 or IPv6 address for the test. By default, this is set to IPv4 then IPv6, which indicates that it will try to resolve the name to an IPv4 address; if this fails and if IPv6 is enabled, it will try to resolve the name to an IPv6 address.
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.

See Table 9-1 for the definitions of the icons next to the AP.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Symbol]</td>
<td>The AP is the associated access point.</td>
</tr>
<tr>
<td>![Symbol]</td>
<td>The mobile computer is not associated to this AP.</td>
</tr>
</tbody>
</table>

Select Set Roaming to allow it to roam to any AP with a better signal.
Chapter 10 Log On/Off Application

Introduction

There are two ways a user can connect to a profile when the profile requires credentials: either by using the Manage Profiles window, or by using the Network Login application. In the first case, Fusion automatically launches the Network Login window to allow the user to enter credentials when they are needed. In the second case, the user explicitly launches the Network Login window and supplies the credentials ahead of time and then tells the system to use them to connect. In either case, once the user has given the credentials, the user is said to have logged on (or in) to the profile. When the user has logged on to a profile, the system saves those credentials and the profile is said to have cached credentials.

When the user launches the Network Login application, the mobile computer may be in one of two states; the user may be logged onto one or more profiles, by having already entered credentials through the login window, or the user is not logged on to any profile. Each of these states has a separate set of use cases and a different look to the dialog box.

![Network Login In Window](image)

Figure 10-1  Network Login In Window

**NOTE** Log On/Off application is available only when Fusion Manages WLAN is enabled in the Options application.
Logging On

If not already logged on to any profile, the user can launch the Network Login window in order to select a profile to log on to.

If already logged into one or more profiles, the user can launch the Network Login window to perform any of these functions:

- Connect to a different profile.
- Connect to and re-enable a cancelled profile. To do this:
  - Launch the Network Login window.
  - Select the cancelled profile from the Wireless 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 from all profiles simultaneously to prevent another user from accessing the current users network privileges.
- Switch mobile computer users. This is equivalent to performing a log off followed by a log on.

The appearance of the Network Login dialog box varies if it is:

- Launched by Fusion, because the service is connecting to a new profile that needs credentials.
- Launched by Fusion, 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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Profile</td>
<td>When launching the login application, the Wireless Profile field lists 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:</td>
</tr>
<tr>
<td>✓</td>
<td>The profile is the current profile (always the case for Fusion Launched).</td>
</tr>
<tr>
<td>✓</td>
<td>The selected profile is enabled but is not the current profile.</td>
</tr>
<tr>
<td>❌</td>
<td>The selected profile is cancelled.</td>
</tr>
<tr>
<td>Username</td>
<td>Used to obtain secure access on the selected Wireless profile. The Username and Domain Name fields combined are limited to 63 characters. If the field label is red, then entry is mandatory; if black, then the entry is optional.</td>
</tr>
</tbody>
</table>
Tap OK to send the credentials to Fusion. If one or more of the required fields is left blank, a dialog box displays requesting the user to fill in all required fields.

### Logging Off

The user can log off from all profiles simultaneously by launching the Network Login window and tapping the Log Off button. The Log Off button only displays when a user has cached credentials for one or more profiles. When the Log Off button is selected, the user is prompted with three options: Log Off, Switch Users, and Cancel. Switching users logs off the current user and re-initializes the Network Login window to be displayed for when there is no user logged on. Logging off logs off the current user from all profiles and closes 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.

Tap the Cancel button to close the Network Login window without logging into the network. If the Network Login window was launched by Fusion 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-connects to it.

> **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.

### Table 10-1  **Network Login Options (Continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Along with the username, required to gain access to the network with the selected Wireless profile. The Password field is limited to 63 characters. If the field label is red, then entry is mandatory; if black, then the entry is optional.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Use to specify the network domain of the security server used for authentication. If the field label is red, then entry is mandatory; if black, then the entry is optional.</td>
</tr>
<tr>
<td>Mask Password checkbox</td>
<td>The Mask Password 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>
Chapter 11 Persistence

Introduction

As you configure the Fusion settings (i.e., profiles, options, user and root certificates, and PACs), they are saved either in the Microsoft registry or in files in the file system. This allows the Fusion settings to persist across a warm boot. However, the registry and the volatile parts of the file system are lost after a cold boot on Windows CE devices and after a clean boot on Windows Mobile devices. So that the Fusion settings won’t be lost, Fusion provides a mechanism for persisting the Fusion settings across a clean/cold boot. Part of this mechanism is automatically implemented by Fusion, and part of it must be performed manually by the user.

This chapter discusses how to:

- make sure your Fusion settings, persist across a clean/cold boot.
- return the Fusion settings to their factory default values.

Persisting Fusion Settings

The Fusion settings that are saved in the registry include:

- Profiles.
- Options.

The Fusion settings that are saved in the file system include:

- User certificates.
- Root (server) certificates.
- PACs.

Fusion automatically persists user certificates, root certificates imported from .pfx files, and PACs. This data is stored in files in subfolders of the Application folder. The Application folder is part of the non-volatile file system and is not lost on a clean/cold boot. After the clean/cold boot, Fusion automatically reads the data back in from the files that have been saved under the Application folder and restores the settings.

Fusion relies on the user to help manually with persistence for profiles, options, and root certificates that are imported from .cer files. Since the profiles and options are stored in the registry, the user must export them to files
under the Application folder before performing the clean/cold boot. You can use the Export function from the Options application. See xxx. When you import a root certificate from a .cer file, place the .cer file in \Application\RootCerts. This allows Fusion to find the .cer file after a clean/cold boot and re-install the root cert that it contains.

When you install a user certificate, be sure to install it either through the Profile Editor Wizard or through the Fusion Certificate Manager application. This allows Fusion to automatically save the data for the user certificate in a special format to files in the Application\UserCerts folder.

---

**Returning to Factory Default Settings**

To return the Fusion settings to their factory default values, you must remove all files in which the Fusion settings are stored. Delete the following files from the mobile computer:

- The file that stores your Fusion profiles. This file will have been created manually and is usually named \Application\WCS_PROFILES.REG.
- The file that stores your Fusion option settings. This file will have been created manually and is usually named \Application\WCS_OPTIONS.REG.
- All files in \Application\RootCerts. For backward compatibility with previous versions, Fusion also searches, after a clean/cold boot, in \Application for persisted root certificates stored in files with the extension .cer. If you have manually placed any .cer files in \Application, remove them as well,
- All files in \Application\UserCerts.
- All files in \Application\Pacstore.

After you delete the files specified above, perform the clean/cold boot. The Fusion settings should be restored to their factory default values.
Chapter 12 Registry Controlled Features

This chapter is devoted to features of Fusion that can be turned on and off but do not have a standard Fusion user interface. Instead, these features are controlled by registry settings, and can be very useful. The following is a list of features that are described in this chapter:

• NPCS.

**NPCS**

Network Policy Configuration Service (NPCS) is a Microsoft feature. As far as Fusion is concerned it makes a decision as to whether or not Fusion should be disabled. The logic used to determine this is to apply a wireless LAN policy on the mobile computer using Open Mobile Alliance (OMA) Device Management (DM). This policy, when applied, modifies a registry key to indicate whether or not Fusion should be disabled.

If the registry key is set then:

• The wireless radio must be powered off;
• Users must not be able to scan or connect to WLAN access points.
• Users must not be able to send or receive data over a WLAN.
• WLAN-related UI must be disabled, hidden or grayed out.
• If the wireless LAN stack exposes any WLAN API’s for third party applications they must be disabled.

A WLAN can be re-enabled if the registry key is properly modified.

The registry key monitored is:

[HKEY_LOCAL_MACHINE\Comm\NetworkPolicy\WiFi]

Edit the following key:

“Disabled”=dword:0

where:

dword:0 (or key not present) = disabled. Allow WLAN to function normally.
dword:1 (or greater) = enabled. Enforce the policy by disabling the radio and all the WLAN related User Interfaces.
Chapter 13 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:


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. Tap **Next**. The **Security Mode** dialog box displays.

16. In the **Security Mode** drop-down list, select **WPA2-Enterprise**.
17. In the Authentication drop-down list, select EAP-FAST.

18. Tap Next. The Tunneled Authentication Type dialog box displays.

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

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

21. Tap Next. The Installed User Certificates dialog box appears.

22. 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 4-8 for information on installing User Certificates.

23. Tap Next. The Install Server Certificate dialog box appears.
24. 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 4-10** for information on installing Server Certificates.

25. 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.

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

27. 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.

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

29. 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.
30. 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.

![Advanced Identity Dialog Box](image1)

**Figure 13-11** Advanced Identity Dialog Box

31. Tap **Next**. The **Prompt for Login** dialog box displays. See *Credential Cache Options on page 4-13* for detailed information on configuring Login settings.

![Prompt for Login at Dialog Box](image2)

**Figure 13-12** Prompt for Login at Dialog Box

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

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

![Encryption Dialog Box](image3)

**Figure 13-13** Encryption Dialog Box

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

![IP Address Entry Dialog Box](image4)

**Figure 13-14** IP Address Entry Dialog Box
35. Ensure that all three check boxes are selected.

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

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

![Battery Usage Dialog Box](image)

**Figure 13-15  Battery Usage Dialog Box**

38. Tap **Save**.

### Switching Between Fusion and WZC

To switch from Fusion to WZC:

1. Tap **Start > Wireless Companion > Wireless Launch**.

![Wireless Launcher Menu](image)

**Figure 13-16  Wireless Launcher Menu**

2. Select **Options**.

3. Select **WLAN Management** from the drop-down list.

![WLAN Management Window](image)

**Figure 13-17  WLAN Management Window**

4. Select **Windows Manages WLAN** radio button.
To switch from WZC to Fusion:


![Wireless Launcher Window](image13-18)

Figure 13-18  Wireless Launcher Window

2. Select Options.

3. Select WLAN Management from the drop-down list.

![WLAN Management Window](image13-19)

Figure 13-19  WLAN Management Window

4. Select Fusion Manages WLAN radio button.

5. Tap Save.

6. Tap OK.

7. Perform a warm boot. Refer to the device’s User Guide for instructions.
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.

Cradle. A cradle is used for charging the terminal battery and for communicating with a host computer. 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.

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

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.

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

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.

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.
**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.

**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.

**WZC. Wireless Zero Config.** Microsoft application used to configure wireless 802.11 radio.
Index

Numerics

802.11 ESSID . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-2

A

ad-hoc . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-2
ad-hoc channel . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-2
ad-hoc networks . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7-2
advanced ID . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-13
AES . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .4-17, 4-18
AP networks . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 7-2
at connect . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-14
at time . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-14
authentication
   EAP-FAST . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-5
   EAP-TLS . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-5
   LEAP . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-5
   none . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-5
   PEAP . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-5
   TTLS . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-5
authentication type . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-5

B

battery usage . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-23
CAM . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-24
MAX power save . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-24
bluetooth
   ad-hoc mode . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-2
bullets . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . x

C

channel . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2-1, 4-3
conventions
   notational . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . x
create profile . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2-3

D

DCP . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . x
Device Configuration Package . . . . . . . . . . . . . . . . . . . . . . x

E

EAP-TLS . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-5
EMDK for C . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . x
encryption . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-16
   AES . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-17
   open . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-16
   open system . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-16
   TKIP . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-17
   WEP-104 (104/24) . . . . . . . . . . . . . . . . . . . . . . 4-16
   WEP-40 (40/24) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-16
Enterprise Mobility Developer Kit for C . . . . . . . . . . . . . . . . x
ESSID . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-1, 4-2
export profile . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3-4
Extensible Authentication Protocol-Generic Token Card . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . x

F

Find WLANs application . . . . . . . . . . . . . . . . . . . . . . . . . . 2-1

G

gateway . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-21

H

hexadecimal keys . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4-17
<table>
<thead>
<tr>
<th>I</th>
<th>page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>infrastructure</td>
<td>4-2</td>
</tr>
<tr>
<td>IP address</td>
<td>4-21</td>
</tr>
<tr>
<td>IP config</td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td>4-21</td>
</tr>
<tr>
<td>subnet mask</td>
<td>4-21</td>
</tr>
<tr>
<td>WINS</td>
<td>4-22</td>
</tr>
<tr>
<td>IPv4 address entry</td>
<td>4-20</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>L</th>
<th>page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>LEAP</td>
<td>4-5</td>
</tr>
<tr>
<td>Legacy (Pre - WPA)</td>
<td>4-4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>M</th>
<th>page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Profile application</td>
<td>3-1</td>
</tr>
<tr>
<td>masked characters</td>
<td>4-17</td>
</tr>
<tr>
<td>MD5</td>
<td>4-6</td>
</tr>
<tr>
<td>Message Digest-5</td>
<td>4-6</td>
</tr>
<tr>
<td>Microsoft Challenge Handshake Authentication Protocol version 2</td>
<td>4-7</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>S</th>
<th>page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>security mode</td>
<td>4-3</td>
</tr>
<tr>
<td>server certificate install</td>
<td>4-10</td>
</tr>
<tr>
<td>set static DNS address</td>
<td>4-22</td>
</tr>
<tr>
<td>set static WINS address</td>
<td>4-22</td>
</tr>
<tr>
<td>signal strength</td>
<td>2-1, 8-2</td>
</tr>
<tr>
<td>subnet mask</td>
<td>4-21</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>T</th>
<th>page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TKIP</td>
<td>4-17, 4-18</td>
</tr>
<tr>
<td>transmit power</td>
<td>4-22</td>
</tr>
<tr>
<td>tunneled authentication</td>
<td>4-5</td>
</tr>
<tr>
<td>CHAP</td>
<td>4-6</td>
</tr>
<tr>
<td>EAP-GTC</td>
<td>4-6</td>
</tr>
<tr>
<td>MD5</td>
<td>4-6</td>
</tr>
<tr>
<td>MS CHAP</td>
<td>4-6</td>
</tr>
<tr>
<td>MS CHAP v2</td>
<td>4-7</td>
</tr>
<tr>
<td>PAP</td>
<td>4-7</td>
</tr>
<tr>
<td>TLS</td>
<td>4-7</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>U</th>
<th>page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>user certificate install</td>
<td>4-7</td>
</tr>
<tr>
<td>user name</td>
<td>4-11</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>W</th>
<th>page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEP-104</td>
<td>4-18</td>
</tr>
<tr>
<td>WEP-40</td>
<td>4-18</td>
</tr>
<tr>
<td>WINS</td>
<td>4-22</td>
</tr>
<tr>
<td>Wireless Launcher</td>
<td>1-7</td>
</tr>
<tr>
<td>exit</td>
<td>1-7</td>
</tr>
<tr>
<td>Wireless Launcher menu</td>
<td>1-6</td>
</tr>
<tr>
<td>hide</td>
<td>1-6</td>
</tr>
<tr>
<td>WPA - Enterprise</td>
<td>4-4</td>
</tr>
<tr>
<td>WPA - Personal</td>
<td>4-4</td>
</tr>
<tr>
<td>WPA2 - Enterprise</td>
<td>4-4</td>
</tr>
<tr>
<td>WPA2 - Personal</td>
<td>4-4</td>
</tr>
</tbody>
</table>