CHAPTER 4

Using the Cisco Unified Wireless IP Phone 7921G Web Pages

You can use the Cisco Unified Wireless IP Phone 7921G web pages to set up and configure settings for the phone.

This chapter describes how to set up your PC to initially configure a Cisco Unified Wireless IP Phone 7921G through a USB connection and how to remotely access a configured phone over the WLAN.

After you have initially configured phones, you can make adjustments to network settings on the phone by using the Settings menu and Network Profile menu options. For more information, see Chapter 5, "Configuring Settings on the Cisco Unified Wireless IP Phone."

This chapter includes these topics:

Using the USB Connection for Initial Phone Configuration

To setup new phones for deployment to users, use your PC to enter the initial configuration for the wireless network settings and network profiles. To save time during initial deployment, you can create a standard network profile template and export it to several phones. For more information, see the "Backup Settings for Phone Configuration" section on page 4-47.

See these sections for information about initial phone configuration:

- Setting Up Your PC to Configure the Cisco Unified Wireless IP Phone 7921G, page 4-2
- Accessing the Phone Web Page, page 4-5
- Setting Configuration Privileges for the Phone Web Page, page 4-7
- Accessing the Configuration Web Page for a Phone, page 4-7

Setting Up Your PC to Configure the Cisco Unified Wireless IP Phone 7921G

Before you can configure phones using the USB connection, you must install drivers and set up the USB ports on the phone and PC.

To interface with the phone and web pages using the USB cable, the PC must run one of these operating systems:

- Windows 2000 Professional
- Windows XP

These sections provide information about setting up your PC:

- Installing the USB Drivers, page 4-3
- Configuring the USB LAN on the PC, page 4-4
- Using the USB Cable to Configure Phones, page 4-6

Installing the USB Drivers

To install the drivers on your PC, follow these steps:

Procedure

Step 1 Download the installation package and "read me" file for the USB drivers from this location:

http://www.cisco.com/cgi-bin/tablebuild.pl/ip-7900ser-crypto

Note Before proceeding, review the "read me" file for specific instructions for your PC operating system.

Step 2 Double-click on the **USB-Install-7921.1-0-1.exe** file to start the installation program.

Step 3 Follow the prompts in the InstallShield Wizard.

Note If you receive a Hardware Installation warning message stating that the software has not passed Microsoft Windows Logo testing, click **Continue**.

Step 4 The driver installation is complete when you see the Finished screen. You can close the wizard.

Step 5 Plug the USB cable into the USB port on the PC and into the USB connector on the phone.

The Found New Hardware Wizard dialog opens.

Step 6 To update the new software, click the button next to **Yes, this time only** and click **Next**.

Step 7 Click the button next to **Install the Software automatically (Recommended)**.

After 2-3 minutes, the software installs and a message appears on the task bar stating "Found New Hardware - Software installed and ready to use."

Step 8 Click **Finish** when the installation is complete.

The phone briefly displays "USB Connected" on the status line.

Configuring the USB LAN on the PC

To configure the USB LAN connection on your PC, follow these steps:

Procedure

Step 1 To setup the USB LAN connection, do one of the following:

- For Windows XP—Click **Start > Control Panel > Network Connections**.
- For Windows 2000—Click **Start > Settings > Control Panel > Network and Dial Up Connections**.

Step 2 Locate and double-click the new LAN connection to open the Local Area Connection Status window, then click **Properties**.

Step 3 Scroll to the **Internet Protocol (TCP/IP)** component and click **Properties**.

Step 4 In the Internet Protocol (TCP/IP) Properties window, choose **Use the following IP address:**

Step 5 In the IP address field, enter a static IP address for the PC: **192.168.1. (1-254** -except 100), for example: *192.168.1.11*

Note

- By default, the Cisco Unified Wireless IP Phone 7921G is configured with 192.168.1.100 so you cannot use this IP address for the PC.
- Make sure to use an IP address that is not in use on any other interface on the PC.

Step 6 Enter the subnet mask: **255.255.255.0**

Step 7 Click **OK** to make the changes.

Related Topics

- Accessing the Phone Web Page, page 4-5

- Setting Configuration Privileges for the Phone Web Page, page 4-7
- Accessing the Configuration Web Page for a Phone, page 4-7

Accessing the Phone Web Page

After setting up the USB interface on the PC, you are ready to use the USB cable connection to the phone.

To access the phone web page, follow these steps:

Procedure

Step 1 Open a Windows browser.

Step 2 In the address field, enter **https://192.168.1.100** to locate the wireless IP phone web page.

Note When the Security Alert dialog box displays a notice to accept the Trust Certificate, click **Yes** or **Always** to accept the application.

The Summary web page for the phone displays. See Table 4-1 for details about this web page.

Step 3 Use the hyperlinks in the left column of the web page to configure settings for the phones. For information, see these sections:

- Configuring Network Profiles, page 4-10
- Configuring USB Settings, page 4-37
- Configuring Trace Settings, page 4-38
- Configuring Wavelink Settings, page 4-41
- Configuring the Phone Book, page 4-42
- Using System Settings, page 4-46

Step 4 After entering the new settings, disconnect the USB cable from the phone. The settings are active immediately.

Step 5 Check that the phone can access the network successfully.

Using the USB Cable to Configure Phones

You are ready to use the USB cable to set up other phones. Before plugging the USB cable into another phone, wait approximately 12-15 seconds for the USB interface on the PC to shut down.

To connect to another phone, follow these steps:

Procedure

Step 1 Plug the USB cable into a Cisco Unified Wireless IP Phone 7921G.

The phone briefly displays "USB Connected" on the status line.

Step 2 Access the web page for the new phone by following the steps in "Accessing the Phone Web Page" section on page 4-5.

Related Topics

- Installing the USB Drivers, page 4-3
- Configuring the USB LAN on the PC, page 4-4
- Using the USB Cable to Configure Phones, page 4-6
- Accessing the Phone Web Page, page 4-5

Updating Phones Remotely

You might have to update settings on a Cisco Unified Wireless IP Phone 7921G that is already configured and in use. You can use the wireless LAN to remotely access and configure these phones.

Use these sections for information about remotely updating phones:

- Setting Configuration Privileges for the Phone Web Page, page 4-7
- Accessing the Configuration Web Page for a Phone, page 4-7

Setting Configuration Privileges for the Phone Web Page

To make changes to the phone by using the web page, you must use Cisco Unified Communications Manager Administration to enable Web Access and Phone Book Web Access.

To allow configuration privileges, follow these steps:

Procedure

Step 1 Log into Cisco Unified Communications Manager Administration.

Step 2 Search for the phone in Cisco Unified Communications Manager by choosing **Devices > Phones** and enter search information such as the directory number.

Step 3 Open the Phone Configuration page, scroll down to Product Specific Configuration, and enable these privileges:

- In the Web Access field, select **Full** from the drop-down menu.
- In the Phone Book Web Access field, select **Allow Admin**.

Step 4 Click **Save** to make the change.

Step 5 You must reset the phone to enable configuration privileges on the web pages for this phone.

Accessing the Configuration Web Page for a Phone

You can access the web page for any Cisco Unified Wireless IP Phone 7921G that is connected to the WLAN. Be sure the phone is powered on and connected.

To access the web page for the Cisco Unified Wireless IP Phone 7921G follow these steps:

Procedure

Step 1 Obtain the IP address of the Cisco Unified Wireless IP Phone 7921G using one of these methods:

- Search for the phone in Cisco Unified Communications Manager by choosing **Devices > Phones**. Phones registered with Cisco Unified Communications Manager display the IP address on the Find and List Phones web page and at the top of the Phone Configuration web page.
- On the Cisco Unified Wireless IP Phone 7921G, press **Settings > Device Information > Network Configuration** and then scroll to the IP Address option.

Step 2 Open a web browser and enter the following URL, where *IP_address* is the IP address of the Cisco Unified IP Phone:

https://<*IP_address*>

Note When the Security Alert dialog box displays a notice to accept the Trust Certificate, click **Yes** or **Always** to accept the application.

Step 3 Log in to the web pages with username: **admin** and enter the password: **Cisco** for the phone web pages.

The Summary web page for the phone displays. See Table 4-1 for details about this web page.

Step 4 Make changes to configurable pages as needed. For information, see these sections:

- Configuring Network Profiles, page 4-10
- Configuring USB Settings, page 4-37
- Configuring Trace Settings, page 4-38
- Configuring Wavelink Settings, page 4-41
- Configuring the Phone Book, page 4-42
- Using System Settings, page 4-46

Step 5 Return to the Phone Configuration web page in Cisco Unified Communications Manager Administration and set the Web Access field back to **ReadOnly** or **Disabled**.

Step 6 Reset the phone from Cisco Unified Communications Manager to disable full access to the web pages.

Be sure to change the Web Access privileges and reset the phone to prevent users from making configuration changes on the phone web pages.

Note If a wireless IP phone was previously registered to Cisco Unified CallManager Release 4.x, and then registers to Cisco Unified Communications Manager 5.x or later, the Phone Configuration web page password might be reset to "Cisco."

Summary Information Web Page

The Summary Information area on a phone's web page displays device settings and related information for the phone. Table 4-1 describes these items.

Table 4-1 Summary Information Area Items

Item	Description
Phone DN	Directory number assigned to this phone
Wireless Information	
Active Network Profile	Name of the profile that the phone is currently using
SSID	SSID that the phone is currently using
Access Point	Name of the access point to which the phone is associated
MAC Address	Media Access Control (MAC) address of the phone
Network Information	
IP Address	Internet Protocol (IP) address of the phone
Subnet Mask	Subnet mask used by the phone

Table 4-1 Summary Information Area Items (continued)

Item	Description
Default Router	IP address for the default gateway that the phone is using
TFTP Server	IP address for the Primary Trivial File Transfer Protocol (TFTP) server that the phone is using
Communications Manager Information	
Active Communications Manager	IP address for the Cisco Unified Communications Manager server to which the phone is registered
Directory Number	Primary directory number for the phone

Related Topics

- Accessing the Phone Web Page, page 4-5
- Configuring Network Profiles, page 4-10
- Configuring USB Settings, page 4-37
- Configuring Trace Settings, page 4-38
- Configuring the Phone Book, page 4-42
- Using System Settings, page 4-46

Configuring Network Profiles

You can configure up to four different profiles for a phone to take advantage of different WLAN environments. You can add names to the profiles and enable one or more of the profiles for the phone to use. The Network Profiles area displays this information about each profile:

- Enabled Profile—A check mark designates an enabled profile
- Name—Lists the name for the profile
- SSID—Lists the SSID used by this profile
- Status—Identifies which profile the phone is using

To display the Network Profiles list, access the web page for the phone as described in the "Accessing the Phone Web Page" section on page 4-5, and then click the **Network Profiles** hyperlink.

For more information about configuring network profiles, see these sections:

- Network Profile Settings, page 4-11
- Configuring Wireless Settings in a Network Profile, page 4-17
- Configuring Wireless LAN Security, page 4-18
- Configuring IP Network Settings, page 4-33
- Configuring the Alternate TFTP Server, page 4-35
- Configuring Advanced Settings, page 4-36

Network Profile Settings

You can configure the settings for a profile by using this web page area. You can also modify or view configured profiles from this web page area. Table 4-2 describes these items and provides references for more information.

To display Network Profile(1-4) Settings, access the web page for the phone as described in the "Accessing the Phone Web Page" section on page 4-5, and then click the **Profile (1-4)** hyperlink.

Table 4-2 Network Profile Settings Items

Item	Description	For More Information, See...
Wireless		
Profile Name	Provides a name for the profile to make it easy to identify; up to 63 alphanumeric characters.	Configuring Wireless Settings in a Network Profile, page 4-17
SSID	Assigns the Service Set Identifier (SSID) to this profile. You must assign the same SSID to the phone that is also assigned to access points in the wireless network.	Connecting to the Wireless Network, page 2-4

Table 4-2 Network Profile Settings Items (continued)

Item	Description	For More Information, See...
Single Access Point	Determines scanning frequency: True—Minimizes the scanning for APs False—Frequent scanning of all access points within range for best match	Roaming in a Wireless Network, page 2-14
Call Power Save Mode	Set for the type of power saving mode used in the WLAN. Options are: • U-APSD/PS-Poll • None	The 802.11 Standards for Wireless LAN Communications, page 2-3
802.11 Mode	Determines the signal mode or priority for selecting signal modes available in the WLAN. Options are: • 802.11 b/g—Use only 2.4 GHz band • 802.11a—Use only 5 GHz band • Auto, 802.11b/g preferred over 802.11a (dual band) • Auto, 802.11a preferred over 802.11b/g (dual band) **Note** The preferred band, if available, will be used at power-on, but the phone may switch to the less preferred 2.4 GHz band, if available, and the preferred band is lost. Once the phone has connected to the less preferred band, it will not scan for the preferred band if the current band is acceptable, and may remain connected to the less preferred band. • Auto, signal strength (RSSI)—Use strongest signal in dual band environment	The 802.11 Standards for Wireless LAN Communications, page 2-3

Table 4-2 Network Profile Settings Items (continued)

Item	Description	For More Information, See...
WLAN Security		
Authentication Mode	Sets the authentication and encryption methods for this profile: • Open—Open access to APs • Open+WEP—Open access with WEP encryption (requires an encryption key) • Shared Key+WEP—Shared key authentication with WEP (requires an encryption key) • LEAP—Cisco proprietary authentication and encryption using a RADIUS server (requires a username and password) • EAP-FAST—Authentication and encryption using TLS and RADIUS server (requires a username and password) • EAP-TLS—Uses Public Key Certificates (PKI) to secure communication to the RADIUS authentication server. A dynamic session-based key is derived from the Cisco Unified Wireless IP Phone 7921G and RADIUS server to encrypt data using a client certificate for authentication.	Configuring Wireless LAN Security, page 4-18 Configuring the Authentication Mode, page 4-20

Table 4-2 Network Profile Settings Items (continued)

Item	Description	For More Information, See...
Authentication Mode (continued)	- PEAP—This method uses name and password authentication based on Microsoft MSCHAP V2 authentication. - Auto (AKM)—Automatic authenticated key management using: – WPA, WPA2 (requires a username and password) – WPA-Pre-shared key, WPA2-Pre-shared key (requires a passphrase/pre-shared key) – CCKM (requires a username and password)	
Export Security Credentials	Controls whether the wireless security credential data can be exported in the configuration file. - True—Allows exporting the data - False—Blocks exporting the data	Backup Settings for Phone Configuration, page 4-47
Wireless Security Credentials	Required for LEAP, EAP-FAST, and Auto (AKM) authentication methods	
Username	Assigns the network authentication username for this profile	Configuring the Username and Password, page 4-21
Password	Assigns the network authentication password for this profile	
WPA Pre-shared Key Credentials	Sets the Pre-shared key for this profile	
Pre-shared Key Type	Determines the key type: **Hex** or **ASCII**	Configuring the Pre-shared Key, page 4-22
Pre-shared Key	Identifies the key	

Table 4-2 Network Profile Settings Items (continued)

Item	Description	For More Information, See...
Wireless Encryption	Required for Open+WEP and Shared+WEP authentication methods	
Key Type	Determines the encryption key type: **Hex** or **ASCII**	Setting Wireless Encryption, page 4-23
Encryption Key 1-4	Identifies the Transmit Key: • Encryption Key character string • Key Size of **40** or **128** characters	
Authentication Certificate	Required for EAP-TLS authentication mode.	
EAP-TLS Certificate	Determines the certificate used for authentication: • Manufacturing issued • User installed	Installing Authentication Certificates for EAP-TLS Authentication, page 4-24
IP Network Configuration		
Obtain IP address and DNS servers automatically	Enables DHCP	Configuring IP Network Settings, page 4-33
Use the following IP address and DNS servers	Disables DHCP and uses these static settings: • IP Address • Subnet Mask • Default Router • Primary DNS • Secondary DNS • Domain Name	
TFTP		
Obtain TFTP servers automatically	Determines whether DHCP assigns the TFTP server	Configuring the Alternate TFTP Server, page 4-35
Use the following TFTP servers	Assigns static TFTP server IP addresses for: • TFTP Server 1 • TFTP Server 2	

Table 4-2 Network Profile Settings Items (continued)

Item	Description	For More Information, See...
Network Profile Advanced Settings		
TSPEC Settings		Configuring Advanced Settings, page 4-36
Minimum PHY Rate	Minimum data rate that outbound traffic uses	
Surplus Bandwidth	Excess bandwidth beyond application requirements	
Antenna Settings		
Antenna Selection for 802.11A	• Vertical • Horizontal • Diversity	
Antenna Selection for 802.11B	• Vertical • Horizontal • Diversity	
802.11G Power Settings	Enabled—Identifies enabled channels in WLAN to improve scanning for the phone Max Tx Power—Sets the maximum transmit power for the phone	
802.11A Power Settings	Enabled—Identifies enabled channels in WLAN to improve scanning for the phone Max Tx Power—Sets the maximum transmit power for the phone	

Note If you uncheck all channels in the 802.11 G Power Settings or 802.11 A Power Settings, the phone will not be able to access the WLAN.

Related Topics

- Accessing the Phone Web Page, page 4-5
- Configuring Wireless Settings in a Network Profile, page 4-17
- Configuring Wireless LAN Security, page 4-18

- Setting the Wireless Security Credentials, page 4-21
- Setting Wireless Encryption, page 4-23

Configuring Wireless Settings in a Network Profile

You must configure wireless settings in a profile to enable the phone to access the wireless network.

To configure the wireless settings, refer to Table 4-2 and follow these steps:

Procedure

Step 1 Choose the network profile that you want to configure.

Step 2 To give the profile a recognizable name, in the Profile Name field, enter a name up to 63 characters and numbers in length.

Step 3 To identify the SSID that the phone uses to associate with access points, in the SSID field, enter an SSID that is already configured in the WLAN.

Note The SSID is case sensitive; you must enter it exactly as configured in the network.

Step 4 To determine the scanning frequency of the phone, in the Single Access Point field, choose **True** (less frequent scanning) or **False** (more frequent scanning).

Step 5 To conserve battery power, in the Call Power Save Mode, choose the type (U-APSD or PS-Poll) and option that is being used in the WLAN.

Step 6 Choose the signal mode or priority of signal modes in the 802.11 Mode field that is used by your WLAN,

Configuring Wireless LAN Security

The Cisco Unified Wireless IP Phone 7921G supports many types of authentication. Authentication methods might require a specific encryption method or you can choose between several encryption methods. When configuring a network profile, you can choose one of these authentication methods:

- Open—Provides access to all access points without WEP Key authentication/encryption.
- Open plus WEP—Provides access to all access points and authentication through the use of one or more WEP Keys at the local access point.
- Shared Key plus WEP—Provides shared key authentication through the use of WEP Keys at the local access point.
- LEAP— Exchanges a username and cryptographically secure password with a RADIUS server for authentication in the network. LEAP is a Cisco proprietary version of EAP.
- EAP-FAST—Exchanges a username and password and with a RADIUS server for authentication in the network.
- EAP-TLS—Uses a dynamic session-based WEP key derived from the client adapter and RADIUS server to encrypt data and a client certificate for authentication. It uses PKI to secure communication to the RADIUS authentication server.
- PEAP (EAP-MSCHAP V2)—Performs mutual authentication, but does not require a client certificate on the phone. This method uses name and password authentication based on Microsoft MSCHAP V2 authentication.
- Auto (AKM)—Automatic authenticated key management in which the phone selects the AP and type of key management scheme, which includes WPA, WPA2, WPA-Pre-shared key, WPA2-Pre-shared key, or CCKM (which uses a wireless domain server (WDS)).

Note When set to AKM mode, the phone uses LEAP for 802.1x type authentication methods (non-Pre-shared key such as WPA, WPA2, or CCKM). AKM mode supports only authenticated key-management types (WPA, WPA2, WPA-PSK, WPA2-PSK, CCKM).

The type of authentication and encryption schemes that you are using with your WLAN determine how you set up the authentication, security, and encryption options in the network profiles for the Cisco Unified Wireless IP Phones. Table 4-3 provides a list of supported authentication and encryption schemes that you can configure on the Cisco Unified Wireless IP Phone 7921G.

Table 4-3 Authentication and Encryption Configuration Options

Authentication Mode	Wireless Encryption	Wireless Security Credentials
Open	None	None—access to all APs
Open plus WEP	Static WEP Requires WEP Key	None—access to all APs
Shared Key plus WEP	Static WEP Requires WEP Key	Uses shared-key with AP
LEAP (with optional CCKM)	Uses WEP	Requires Username and Password
EAP-FAST (with optional CCKM)	Uses WEP or TKIP	Requires Username and Password
EAP-TLS	Uses WEP, TKIP, or AES	Requires Username and Password Requires server and client certificates.
PEAP	Uses WEP, TKIP, or AES	Requires Username and Password Requires server side certificate.
Auto (AKM) with CCKM	Uses TKIP or AES	Requires Username and Password
Auto (AKM) with WPA (with optional CCKM)	Uses TKIP	Requires Username and Password

Table 4-3 Authentication and Encryption Configuration Options (continued)

Authentication Mode	Wireless Encryption	Wireless Security Credentials
Auto (AKM) with WPA2 (with optional CCKM)	Uses AES	Requires Username and Password
Auto (AKM) with WPA Pre-Shared Key	Uses TKIP	Requires Passphrase
Auto (AKM) with WPA2 Pre-Shared Key	Uses AES	Requires Passphrase

Note Beginning with Cisco Wireless IP Phone 7921G firmware release 1.1, CCKM is operational with the WPA authentication mode using AES encryption.

Configuring the Authentication Mode

To select the Authentication Mode for this profile, follow these steps:

Procedure

Step 1 Choose the network profile that you want to configure.

Step 2 Choose the authentication mode.

Note Depending on what you selected, you must configure additional options in Wireless Security or Wireless Encryption. See Table 4-3 for more information.

Step 3 Click **Save** to make the change.

Setting the Wireless Security Credentials

When your network uses EAP-FAST, LEAP, EAP-TLS, PEAP, or Auto (AKM) with WPA, WPA2, CCKM for user authentication, you must configure both the username and a password on the Access Control Server (ACS) and the phone.

Note If you use domains within your network, you must enter the username with the domain name, in this format: *domain\username*.

For information about setting security credentials, see these topics:

- Configuring the Username and Password, page 4-21
- Configuring the Pre-shared Key, page 4-22
- Setting Wireless Encryption, page 4-23

Configuring the Username and Password

To enter or change the username or password for the network profile, you must use the same username and the same password string that is configured in the RADIUS server. The maximum length of the username or password entry is 32 characters.

To set up the username and password in Wireless Security Credentials, follow these steps:

Procedure

Step 1 Choose the network profile.

Step 2 In the Username field, enter the network username for this profile.

Step 3 In the Password field, enter the network password string for this profile.

Step 4 Click **Save** to make the change.

Configuring the Pre-shared Key

When using Auto (AKM) with WPA Pre-shared key or WPA2 with Pre-shared key for authentication, you must configure a Passphrase/Pre-shared key in the Wireless Security Credentials area.

Pre-shared Key Formats

The Cisco Unified Wireless IP Phone 7921G supports ASCII and hexadecimal formats. You must use one of these formats when setting up a WPA Pre-shared key:

Hexadecimal

For hexadecimal keys, you must enter 64 hex digits (0-9 and/or A-F); for example, AB123456789CD01234567890EFAB123456789CD01234567890EF3456789C

ASCII

For ASCII keys, you must enter a character string that uses 0-9, A-Z (upper and lower case), including symbols and is from 8 to 63 characters in length; for example, GREG12356789ZXYW

To set up a Pre-shared key in the Wireless Credentials area, follow these steps:

Procedure

Step 1 Choose the network profile that uses Auto (AKM) to enable the WPA Pre-shared key or WPA2 Pre-shared key.

Step 2 In the Key Type area, choose one of these character formats:

- **Hex**
- **ASCII**

Step 3 Enter an ASCII string or Hex digits in the Passphrase/Pre-shared key field**.** See "Pre-shared Key Formats" section on page 4-22.

Step 4 Click **Save** to make the change.

Setting Wireless Encryption

If your wireless network uses WEP encryption, and you have set the Authentication Mode as Open + WEP or Shared Key + WEP, you must enter an ASCII or hexadecimal WEP Key.

The WEP Keys for the phone must match the WEP Keys assigned to the access point. Cisco Unified Wireless IP Phone 7921G and Cisco Aironet Access Points support both 40-bit and 128-bit encryption keys.

WEP Key Formats

You must use one of these formats when setting up a WEP key:

Hexadecimal

For hexadecimal keys, you can use one of the following key sizes:

- 40-bit—You must enter a 10-digit encryption key string that uses the hex digits (0-9 and/or A-F); or example, ABCD123456.
- 128-bit—You must enter a 26-digit encryption key string that uses the hex digits (0-9 and/or A-F); or example, AB123456789CD01234567890EF.

ASCII

For ASCII keys, you must enter a character string that uses 0-9, A-Z (upper and lower case), and all symbols.

- 40-bit—You must enter a 5-character string; for example, GREG5.
- 128-bit—You must enter a 13-character string; for example, GREGSSECRET13.

Entering Wireless Encryption Keys

To set up WEP keys, follow these steps:

Procedure

Step 1 Choose the network profile that uses Open+WEP or Shared+WEP.

Step 2 In the Key Type area, choose one of these character formats:

- **Hex**
- **ASCII**

Step 3 For Encryption Key 1, click **Transmit Key**.

Step 4 In the Key Size area, choose one of these character string lengths:

- **40**
- **128**

Step 5 In the Encryption Key field, enter the appropriate key string based on the selected Key Type and Key Size. See the "WEP Key Formats" section on page 4-23.

Step 6 Click **Save** to make the change.

Related Topics

- Configuring IP Network Settings, page 4-33
- Configuring the Alternate TFTP Server, page 4-35
- Configuring Advanced Settings, page 4-36

Installing Authentication Certificates for EAP-TLS Authentication

EAP-TLS is a certificate based authentication that requires a trust relationship between two or more entities. Each entity has a certificate proving its identity and is signed by a trusted authority. These certificates are exchanged and verified during EAP-TLS authentication.

Note The EAP-TLS certificate based authentication requires that the internal clock on the Cisco Unified Wireless IP Phone 7921G be set correctly. Use the phone web page to set the clock on the phone before using EAP-TLS authentication.

To use EAP-TLS, both the Cisco Unified Wireless IP Phone 7921G and the Cisco Secure Access Control Server (ACS) must have certificates installed and configured properly. If your wireless network uses EAP-TLS for authentication, you can use the Manufacturing Installed Certificate (MIC) or a user installed certificate for authentication on the phone.

Manufacturing Installed Certificate

Cisco has included a Manufacturing Installed Certificate (MIC) in the phone at the factory.

During EAP-TLS authentication the ACS server needs to verify the trust of the phone and the phone needs to verify the trust of the ACS server.

To verify the MIC, the Manufacturing Root Certificate and Manufacturing Certificate Authority (CA) Certificate must be exported from a Cisco Unified Wireless IP Phone 7921G and installed on the Cisco ACS server. These two certificates are part of the trusted certificate chain used to verify the MIC by the Cisco ACS server.

To verify the Cisco ACS certificate, a trusted subordinate certificate (if any) and root certificate (created from a CA) on the Cisco ACS server must be exported and installed on the phone. These certificate(s) are part of the trusted certificate chain used to verify the trust of the certificate from the ACS server.

User Installed Certificate

To use a user installed certificate, a Certificate Signing Request (CSR) must be generated on the phone, sent to the CA for approval, and the approved certificate installed on the Cisco Unified Wireless IP Phone 7921G.

During EAP-TLS authentication, the ACS server needs to verify the trust of the phone and the phone needs to verify the trust of the ACS server.

To verify the authenticity of the user installed certificate, a trusted subordinate certificate (if any) and root certificate from the CA that approved the user certificate must be installed on the Cisco ACS server. These certificate(s) are part of the trusted certificate chain used to verify the trust of the user installed certificate.

To verify the Cisco ACS certificate, a trusted subordinate certificate (if any) and root certificate (created from a CA) on the Cisco ACS server must be exported and installed on the phone. These certificate(s) are part of the trusted certificate chain used to verify the trust of the certificate from the ACS server.

To install authentication certificates for EAP-TLS, perform the tasks listed in Table 4-4:

Table 4-4 Installing the Certificate for EAP-TLS

Task	From	For more information, see...
1. Set the Cisco Unified Communications Manager date and time on the phone.	Cisco Unified Wireless IP Phone 7921G web page	Setting the Date and Time, page 4-27
2. If using the Manufacturing Installed Certificate (MIC): **a.** Export the CA root certificate and manufacturing CA certificate. **b.** Install certificates on the Cisco ACS server and edit the trust list. **c.** Export the CA certificate from the ACS server and import it to the phone.	• Cisco Unified Wireless IP Phone 7921G web page • Internet Explorer • Microsoft Certificate Services	Exporting and Installing the Certificates on the ACS, page 4-28 Exporting the CA Certificate from the ACS Using Microsoft Certificate Services, page 4-29

Table 4-4 Installing the Certificate for EAP-TLS (continued)

Task	From	For more information, see...
3. If using a user installed certificate: **a.** Generate the Certificate Signing Request (CSR). **b.** Send the CSR to CA to sign. **c.** Import the certificate. **d.** Install certificate on the Cisco ACS server and edit the trust list. **e.** Download the CA certificate from the ACS server and import it into the 7921G.	Cisco Unified Wireless IP Phone 7921G web page	Requesting and Importing the User Installed Certificate, page 4-30
4. Set up the user account.	ACS configuration tool	Configuring the ACS Server Setup, page 4-31 *User Guide for Cisco Secure ACS for Windows*

Setting the Date and Time

EAP-TLS uses certificate based authentication that requires the internal clock on the Cisco Unified Wireless IP Phone 7921G to be set correctly. The date and time on the phone might change when it is registered to Cisco Unified Communications Manager.

Note If a new server authentication certicate is being requested and the local time is behind the Greenwich Mean Time (GMT), the authentication certificate validation might fail. It is recommended that you set the local date and time ahead of the GMT.

To set the phone to the correct local date and time, follow these steps:

Procedure

Step 1 Select **Date & Time** from the left navigation pane.

Step 2 If the setting in the Current Phone Date & Time field is different from the Local Date & Time field, click **Set Phone to Local Date & Time**.

Step 3 Click **Phone Restart**, then click **OK**.

Exporting and Installing the Certificates on the ACS

To use the MIC, the Manufacturing Root Certificate and Manufacturing CA Certificate must be exported and installed onto the Cisco ACS server.

To export the manufacturing root certificate and manufacturing CA certificate to the ACS server, follow these steps:

Procedure

Step 1 From the phone web page, choose Certificates. Click Export next to the Manufacturing Root Certificate.

Step 2 Save the certificate and copy it to the ACS server.

Step 3 Repeat Steps 1 and 2 for the Manufacturing CA certificate.

Step 4 From the ACS Server System Configuration page, enter the file path for each certificate and install the certificates.

Note For more information about using the ACS configuration tool, see the ACS online help or the *User Guide for Cisco Secure ACS for Windows*.

Step 5 Use the Edit the Certificate Trust List (CTL) page to add the certificates to be trusted by ACS.

Exporting Certificates from the ACS

Depending on the type of certificate you export from the ACS, use one of the following methods:

- To export the CA certificate from the ACS server that signed the user installed certificate or ACS certificate, see Exporting the CA Certificate from the ACS Using Microsoft Certificate Services, page 4-29.
- To export the CA certificate from the ACS server that uses a self-signed certificate, see Exporting Certificates from the ACS Server Using Internet Explorer, page 4-29.

Exporting the CA Certificate from the ACS Using Microsoft Certificate Services

Use this method for exporting the CA certificate from the ACS server that signed the user installed certificate or ACS certificate.

To export the CA certificate using the Microsoft Certificate Services web page, follow these steps:

Procedure

Step 1 From the Microsoft Certificate Services web page, select Download a CA certificate, certificate chain or CRL.

Step 2 At the next page, highlight the current CA certificate in the text box, choose DER under Encoding Method, then click Download CA certificate.

Step 3 Save the CA certificate.

Exporting Certificates from the ACS Server Using Internet Explorer

Use this method for exporting the CA certificate from the ACS server that uses a self-signed certificate.

To export certificates from the ACS server using Internet Explorer, follow these steps:

Procedure

Step 1 From Internet Explorer, choose Tools > Internet Options, then click the Content tab.

Step 2 Under Certificates, click **Certificates...**, then click the Trusted Root Certification Authorities tab.

Step 3 Highlight the root certificate and click **Export...**. The Certificate Export Wizard appears. Click **Next**.

Step 4 At the next window, select **DER encoded binary X.509 (.CER)**, and click **Next**.

Step 5 Specify a name for the certificate and click **Next**.

Step 6 Save the CA certificate to be installed on the phone.

Requesting and Importing the User Installed Certificate

To request and install the certificate on the phone, follow these steps:

Procedure

Step 1 From the phone web page, choose the network profile using EAP-TLS, and select **User Installed** in the EAP-TLS Certificate field.

Step 2 Click **Certificates**. On the User Certificate Installation page, the Common Name field should match the user name in the ACS server.

Note You can edit the Common Name field if you wish. Make sure that it matches the user name in the ACS server. See "Configuring the ACS Server Setup" section on page 4-31.

Enter the information to be displayed on the certificate, and click **Submit** to generate the Certificate Signing Request (CSR).

Step 3 In the next screen, select and copy the entire contents of the text box. Send this data to the CA administrator for signing.

The CSR text is encoded and should be sent to the Certificate Authority for signing. The CSR text can be sent by e-mail or another method determined by your CA administrator. The following steps describe the basic CSR approval process on the CA web page.

Step 4 From the Microsoft Certificate Services Request a Certificate page, select **Advanced certificate request** to initiate the signing request.

Step 5 At the Advanced Certificate Request page, select **Submit a certificate request by using a base-64-encoded PKCS CMC**.

Step 6 Copy the certificate data from the Cisco Unified Wireless IP Phone 7921G and paste it in the Saved Request text box, then click **Submit**.

Step 7 Once the CSR is approved, the certificate must be exported in a DER encoded format and sent to the original requestor.

Step 8 Return to the phone web page and choose **Certificates** to import the signed certificate.

Step 9 On the Certificates page, locate the User Installed certificate line, and click **Import**. Browse to the certificate on your PC to import to the phone.

Installing the Authentication Server Root Certificate

The Authentication Server Root Certificate must be installed on the Cisco Unified Wireless IP Phone 7921G.

To install the certificate, follow these steps:

Step 1 Export the Authentication Server Root Certificate from the ACS. See Exporting Certificates from the ACS, page 4-29.

Step 2 Go to the phone web page and choose **Certificates**.

Step 3 Click **Import** next to the Authentication Server Root certificate.

Step 4 Restart the phone.

Configuring the ACS Server Setup

To set up the user account name and install the MIC root certificate for the phone on the ACS, follow these steps:

Note For more information about using the ACS configuration tool, see the ACS online help or the *User Guide for Cisco Secure ACS for Windows*.

Procedure

Step 1 From the ACS configuration tool User Setup page, create a phone user account name if it is not already set up. Typically, the user name includes the phone MAC address at the end (for example, CP-7921G-SEPxxxxxxxxxxxx). No password is necessary for EAP-TLS.

Note Make sure the user name matches the Common Name field in the User Certificate Installation page. See "Requesting and Importing the User Installed Certificate" section on page 4-30.

Step 2 On the System Configuration page, in the EAP-TLS section, enable these fields:

- Allow EAP-TLS
- Certificate CN comparison.

Step 3 On the ACS Certification Authority Setup page, add the Manufacturing Root Certificate and Manufacturing CA Certificate to the ACS server.

Step 4 Enable both the Manufacturing Root Certificate and Manufacturing CA Certificate in the ACS Certificate Trust List.

Configuring PEAP

Protected Extensible Authentication Protocol (PEAP) uses server-side public key certificates to authenticate clients by creating an encrypted SSL/TLS tunnel between the client and the authentication server.

Before You Begin

Before you configure PEAP authentication for the phone, make sure these Cisco Secure ACS requirements are met:

- The ACS root certificate must be installed
- Enable the Allow EAP-MSCHAPv2 setting
- User account and password must be configured
- For password authentication, you can use the local ACS database or an external one (such as Windows or LDAP)

Enabling PEAP Authentication

To enable PEAP authentication on the phone, follow these steps:

Procedure

Step 1 From the phone configuration web page, choose PEAP as the authentication mode. See Configuring the Authentication Mode, page 4-20.

Step 2 Enter a user name and password.

Configuring IP Network Settings

The Cisco Unified IP Phones enable DHCP, by default, to automatically assign IP addresses to devices when you connect them to the network. If you do not use DHCP in your network, then you must disable DHCP and manually enter network configuration information. For more information, see "Interacting with the DHCP Server" section on page 2-26.

When DHCP is disabled in the network, you must configure the following settings in the Static Settings menu:

- IP address
- Subnet mask
- Default Router
- DNS server 1 and 2
- TFTP server 1

Use these guidelines when manually configuring the IP settings:

- Ensure the TFTP server has an IP address.
- Ensure the default router IP address is on the same subnet as the host IP address.

Enabling DHCP

To enable the use of DHCP in the Network Profile, follow these steps:

Procedure

Step 1 Choose the network profile that you want to configure.

Step 2 Under the IP Network Configuration area, choose this option:

Obtain IP address and DNS servers automatically

Step 3 Click **Save** to make the change.

Disabling DHCP

To disable the use of DHCP in the Network Profile, follow these steps:

Procedure

Step 1 Choose the network profile that you want to configure.

Step 2 Under the IP Network Configuration area, choose this option:

Use the following IP addresses and DNS servers

Step 3 You must enter these required IP addresses. See Table 4-5 for descriptions of these fields.

Step 4 Click **Save** to make the change.

Table 4-5 Static IP Addresses When DHCP is Disabled

Static Setting	Description
IP Address	Internet Protocol (IP) address of the phone
Subnet Mask	Subnet mask used by the phone
Default Router 1	Primary gateway used by the phone
DNS Server 1	Primary DNS server used by the phone
DNS Server 2	Optional backup DNS server used by the phone

Table 4-5 Static IP Addresses When DHCP is Disabled (continued)

Static Setting	Description
TFTP Server 1 TFTP Server 2	Primary TFTP server used by the phone. Optional backup TFTP server used by the phone
Domain Name	Name of the Domain Name System (DNS) domain in which the phone resides

Configuring the Alternate TFTP Server

If you use DHCP to direct the Cisco Unified IP Phones to a TFTP server, you can also assign an alternative TFTP server to some phones instead of the one assigned by DHCP.

Note If you disable DHCP, then you must use these steps to set up the TFTP server for the phone.

To assign an alternate TFTP server to a phone, follow these steps:

Procedure

Step 1 Choose the network profile that you want to configure.

Step 2 Under the TFTP area, choose this option:

Use the following TFTP servers

Step 3 You must enter the required IP addresses. See Table 4-5 for descriptions of these fields.

Step 4 Click **Save** to make the change.

Configuring Advanced Settings

The network profiles provide a web page for setting QoS, bandwidth, and power settings. The Traffic Specification (TSPEC) parameters are used to advertise information about generated traffic for Call Admission Control (CAC) to the AP.

Minimum PHY rate—Lowest rate that outbound traffic is expected to use before the phone roams to another AP

Surplus Bandwidth Allowance—Fractional number that specifies the excess allocation of time and bandwidth above application rates required to transport a MAC service data unit (MSDU) in a TSPEC frame.

Note If your wireless LAN has access points that use 802.11b and you plan to use Call Admission Control (CAC) with TSPEC, then you need to modify the PHY rate to a supported rate for your 802.11b access points.

To make changes to the advanced settings, follow these steps:

Procedure

Step 1 Choose the network profile that you want to configure.

Step 2 Click the Advanced Profile link at the top of the page.

Step 3 In the TSPEC Setting area, keep the Minimum PHY Rate: **12 Mbps**

Note If you are using 802.11b APs and plan to use Call Admission Control (CAC) with TSPEC, then set the PHY Rate to a rate that the APs support such as 11 Mbps.

Step 4 In the Surplus Bandwidth field, enter the appropriate values.

Step 5 In the 802.11G Power Settings area, check only the channels that are used in your WLAN. By doing this, the phone scans for only those channels.

In the Max Tx Power field, keep the default value.

Step 6 In the 802.11A Power Settings area, check only the channels that are used in your WLAN. By doing this, the phone scans for only those channels.

In the Max Tx Power field, keep the default value.

⚠ **Caution** You must check at least one channel after using "Clear All," to enable the phone to access the WLAN.

Step 7 Click **Save** to make the change.

Related Topics

- Accessing the Configuration Web Page for a Phone, page 4-7
- Network Profile Settings, page 4-11
- Configuring Wireless Settings in a Network Profile, page 4-17
- Configuring Wireless LAN Security, page 4-18
- Setting the Wireless Security Credentials, page 4-21
- Configuring the Pre-shared Key, page 4-22
- Configuring IP Network Settings, page 4-33
- Configuring the Alternate TFTP Server, page 4-35

Configuring USB Settings

To use the USB cable from your PC to a phone, you must configure the USB settings to work with the USB port on the PC. The phone has a default USB IP address of 192.168.1.100. You can change the USB port configuration on the phone in these ways:

- To obtain the IP address automatically, by getting an IP address from the PC that has DHCP set up.
- To use the IP address and subnet mask assigned in this area.

To display the USB Settings area, access the web page for the phone as described in the "Accessing the Phone Web Page" section on page 4-5, and then click the **USB Settings** hyperlink.

To change the USB port settings for the phone, follow these steps:

Procedure

Step 1 On the phone's web page, choose the USB Settings hyperlink.

Step 2 Choose one of the following options:

- Obtain IP address automatically
- Use the following IP address

Step 3 To change the static IP address, in the IP Address field, enter a new IP address that is not assigned on the subnet.

Step 4 To change the subnet for the new IP address, in the Subnet Mask field, enter the appropriate subnet address.

Step 5 Click **Save** to make the change.

Related Topics

- Accessing the Phone Web Page, page 4-5
- Configuring Network Profiles, page 4-10
- Configuring Trace Settings, page 4-38
- Using System Settings, page 4-46

Configuring Trace Settings

You can use the Trace Settings area on the web page to configure how the phone creates and saves trace files. Because trace files are stored in the memory of the phone, you can control the number of files and the data that you want to collect. Table 4-6 describes these configurable items.

Note When preserving trace logs, choose only the logs that need to be saved after the phone is powered off and powered on to avoid using up phone memory.

To display the Trace Settings area, access the web page for the phone as described in the "Accessing the Phone Web Page" section on page 4-5, and then click the **Trace Settings** hyperlink under Setup.

To change the trace settings for the phone, follow these steps:

Procedure

Step 1 On the phone's web page, choose the Trace Settings hyperlink.

Step 2 In the Number of Files field, choose the number of trace files to save, from 2 to 10.

Step 3 In the Remote Syslog Server area, check the box to enable a server to collect the trace files.

Step 4 If you enabled the syslog server, then you must complete these fields:

- IP Address—Enter server IP address
- Port—Enter a port number (514, 1024-65535)

Step 5 In the Module Trace Level area, check only the modules for which you want data:

- Kernel
- Configuration
- Call Control
- Network Services
- Security Subsystem
- User Interface
- Wireless
- Audio System
- System

Step 6 In the Advanced Trace Settings area, in the Preserve Logs field, choose one of the following:

- True—Save the trace logs to flash memory on the phone.
- False—Save the trace logs to RAM.

Note

- When set to False, the trace logs are lost when the phone is powered off.
- When the phone is powered off, then powered back on, the Preserve Logs field is reset to False, the default value.

Step 7 Click **Save** to make the change.

Table 4-6 Trace Settings Area Items

Item	Description
General	
Number of Files	Choose the number of trace files that the phone saves, from 2-10 files.
File Size	Choose the File size for the trace file that is saved. The file size range is 50K to 250K.
Remote Syslog Server	
Enable Remote Syslog	Set up a remote server to store trace logs IP Address—Enter server IP address Port—Enter a port number (514, 1024-65535)
Module Trace Level	
Kernel	Operating System data
Configuration	Phone configuration data
Call Control	Cisco Unified Communications Manager data
Network Services	DHCP, TFTP, CDP data
Security Subsystem	Application level security data
User Interface	Key strokes, softkeys, MMI data
Wireless	Channel scanning, authentication data
Audio System	RTP, SRTP, RTCP, DSP data
System	Firmware, upgrade data

Table 4-6 Trace Settings Area Items (continued)

Item	Description
Advanced Trace Settings	
Preserve Logs	True—Save trace logs after powering off the phone False—Delete trace logs
Reset Trace Settings upon Reboot	You may enable debugging by configuring various settings on the Trace Configuration. These options determine how trace settings are handled when you reboot: • Yes—Default value. Settings will be reset to the default values upon reboot. • No—Trace settings will not reset upon reboot.

Related Topics

- Accessing the Phone Web Page, page 4-5
- Configuring Network Profiles, page 4-10
- Configuring USB Settings, page 4-37
- Using System Settings, page 4-46

Configuring Wavelink Settings

The Cisco Unified Wireless IP Phone 7921G supports the use of the Wavelink Avalanche server to configure the phone, which can be set up as a Wavelink Avalanche client device. The Cisco Unified Wireless IP Phone 7921 Configuration Utility can be installed on the Wavelink Avalanche server to configure a single phone or multiple phones with common settings. For more information, see Configuring the Phone Using the Wavelink Avalanche Server, page 6-1.

You can use the phone web page to assign attributes to the phone that can be used to distinguish it from other mobile devices connected to the Wavelink server. These attributes can be used as search criteria for locating phones on the Wavelink server. For example, the predefined ModelName parameter with a value of “CP7921G” will identify a device as the Cisco Unified Wireless IP Phone 7921G.

By default, the following parameters are configured as follows:

- ModelName = CP7921
- EnablerVer = 3.11-01

To configure Wavelink parameters using the phone web page, follow these steps:

Procedure

Step 1 From the phone web page, choose **Wavelink Settings**.

Step 2 In the Wavelink Custom Parameters section, enter values for each parameter in the Name and Value fields. You can define up to four pairs of custom parameters.

Note Do not use spaces in the Name field.

Note For more information about using the Wavelink Avalanche server, see Configuring the Phone Using the Wavelink Avalanche Server, page 6-1.

Configuring the Phone Book

Cisco Unified Wireless IP Phone 7921G users can store up to 100 contacts in the Phone Book on their phone. As the administrator, you can configure the Phone Book for these phones from the phone web page.

Note Before you can configure the Phone Book from the web, you must first enable the Phone Book Web Access privilege from Cisco Unified Communications Administration. For more information, see Setting Configuration Privileges for the Phone Web Page, page 4-7.

You can perform the following tasks for the Phone Book:

- Import or export a file from/to the Phone Book—See Importing and Exporting Contacts, page 4-43

- Search the Phone Book for a contact—See Searching the Phone Book Information, page 4-43
- Update the Phone Book contact information—See Updating Phone Book Information, page 4-44
- Assign a speed dial to contact phone number—See Assigning A Speed-Dial Hot Key to a Contact Number, page 4-45

Importing and Exporting Contacts

To import contact information from a file, follow these steps:

Procedure

Step 1 From the phone web page, choose **Phone Book > Import/Export** from the left pane.

Step 2 At the Phone Book Import & Export page, do one of the following:

- To import a file, browse to it on your PC. Choose one of the following options, then click **Import**:
  - Delete all current contacts before importing
  - Delete only the current contacts that have the same IDs
  - Merge current contacts with imported data
- To export a file, click **Export**. A file with your contact information is displayed. Save this file to your PC or another storage device.

Searching the Phone Book Information

You can search for contacts in the Phone Book by first name, last name, nickname, or company name.

To perform a search, follow these steps:

Procedure

Step 1 From the phone web page, choose **Phone Book** from the left pane.

Step 2 At the Phone Book page, enter a search string in the text box and click **Search**.

The contact records containing a match will be displayed.

Updating Phone Book Information

You can update the information for Phone Book from the phone web page. You can perform the following tasks:

- Add a contact—See Adding a Contact, page 4-44
- Delete contacts—See Deleting Contacts, page 4-45
- Edit the information for a contact—See Editing Contact Information, page 4-45

Note When entering phone numbers, only numeric characters and the symbols # and * are stored and displayed.

Adding a Contact

To add a contact to the Phone Book, follow these steps:

Procedure

Step 1 From the phone web page, choose **Phone Book** from the left pane.

Step 2 At the Phone Book page, click New. The Phone Book (New Contact) page appears.

Step 3 Enter information for this contact. If you wish to assign speed dials, see Assigning A Speed-Dial Hot Key to a Contact Number, page 4-45.

Step 4 When finished, click **Save**.

Deleting Contacts

To delete contacts from the Phone Book, follow these steps:

Procedure

Step 1 From the phone web page, choose **Phone Book** from the left pane.

Step 2 At the Phone Book page, select the contacts to delete, and click **Delete**.

To delete all contacts, click **DeleteAll**.

Editing Contact Information

To edit information for a contact, follow these steps:

Procedure

Step 1 From the phone web page, choose **Phone Book** from the left pane.

Step 2 At the Phone Book page, select a contact. The Phone Book (Edit Contact) page appears.

Step 3 Change or enter information for this contact. If you wish to assign speed dials, see Assigning A Speed-Dial Hot Key to a Contact Number, page 4-45.

Step 4 When finished, click **Save**.

Assigning A Speed-Dial Hot Key to a Contact Number

You can assign a speed-dial hot key to any contact phone number in the Phone Book.

To assign a speed-dial hot key to a contact number, follow these steps:

Procedure

Step 1 From the phone web page, add a new contact or select a contact record to edit. For more information, see Adding a Contact, page 4-44 or Editing Contact Information, page 4-45.

Step 2 At the Phone Book (Edit Contact) page or the Phone Book (New Contact) page, click the speed dial icon next to the phone number you wish to assign.

Step 3 At the Phone Book (Speed Dial List) window, click an unassigned speed dial. The speed dial you selected is assigned to the contact number, and the speed dial code number appears next to the contact number.

Step 4 Click **Save**. To change a speed dial assignment, click the speed dial icon again and repeat Step 3.

Using System Settings

In addition to phone settings, the web page includes these areas for system management:

- Trace Logs—See Viewing Trace Logs, page 4-47
- Backup Settings—See Backup Settings for Phone Configuration, page 4-47
- Phone Upgrade—See Upgrading Phone Firmware, page 4-51
- Change Password—See Changing the Admin Password, page 4-52
- Site Survey—See Viewing the Site Survey Report on the Web, page 4-53
- Date and Time—See Setting the Date and Time, page 4-27

For information about the remaining web page topics, see the Chapter 9, "Monitoring the Cisco Unified Wireless IP Phone Remotely."

Viewing Trace Logs

You can use the Trace Logs area on the web page to view and manage trace files. System trace logs appear in a list on this page. You define how many messages are saved in the Trace Settings area.

To view a trace log, click on the "Message.<n>" link. The trace log appears in ASCII text. You can save the text file in a directory or on a disk to send to TAC for troubleshooting purposes.

To download a trace log, click **Download**. All the trace logs on the phone are then collected into a file named SEP<MAC-ADDRESS-OF-PHONE>_LOGS.tar.gz for a downloading and saving.

Note Trace logs are erased when the phone is powered off. To preserve trace logs, see the "Configuring Trace Settings" section on page 4-38.

To display the Trace Logs area, access the web page for the phone as described in the "Setting Up Your PC to Configure the Cisco Unified Wireless IP Phone 7921G" section on page 4-2, and then click the **Trace Logs** hyperlink.

Related Topics

- Using System Settings, page 4-46
- Backup Settings for Phone Configuration, page 4-47
- Upgrading Phone Firmware, page 4-51
- Changing the Admin Password, page 4-52

Backup Settings for Phone Configuration

You can use the Backup Settings area on the web page to export the phone configuration. You must set up an encryption key that encrypts the phone settings to keep them secure. When you export a configuration, all the settings in the network profiles, phone settings, USB settings, and trace are copied. None of the statistics or information fields are copied from the web pages.

Note To import a file to a phone, you must enter the same encryption key that was used to export the file.

To display the Backup Settings area, access the web page for the phone as described in the "Accessing the Configuration Web Page for a Phone" section on page 4-7, and then click the **Backup Settings** hyperlink. Table 4-7 describes the items in this area.

Table 4-7 Backup Settings Area Items

Item	Description
Import Configuration	
Encryption Key	Enter the alphanumeric string up to 8-20 characters for encrypting the phone settings.
Import File	Enter the path and filename or use the Browse button to locate the file.
Import button	Click the button to import the phone settings file into the phone.
Export Configuration	
Encryption Key	Enter the alphanumeric string up to 8-20 characters for encrypting the phone settings.
Export button	Click the button to export the phone settings file to a location on your PC or to a disc.

Using Network Profile Templates

At initial phone deployment, you can create a typical network profile and export the phone settings to a location that you specify, such as a folder on your PC or your network. Then, you can import the network profile template to several phones to save time.

Creating a Configuration Template

To create a phone configuration template, follow these steps:

Procedure

Step 1 Connect the USB cable to the phone and access the phone's web page using the instructions on "Accessing the Phone Web Page" section on page 4-5.

Step 2 On the phone's web page, choose the **Network Profiles** hyperlink and configure the Network Profile settings for your template configuration.

Note You can leave the Username and Password fields blank so they can be configured individually.

Step 3 Next, configure the USB Settings and Trace Settings for your template configuration.

Step 4 Choose the **Backup Settings** hyperlink, to access the export and import settings.

Step 5 In the Export Configuration area, enter an encryption key of from 8 to 20 characters.

Record this key because you must enter this key to import the configuration template on other phones.

Step 6 Click **Export** and the File Download dialog displays, and then click **Save.**

Step 7 Give your configuration a new file name such as *7921template.cfg*.

Step 8 Choose a location on your PC or on the network for the file and then click **Save**.

Step 9 The encrypted configuration file contains these settings:

- Profile Name
- SSID
- Single Access Point
- Call Power Save Mode
- 802.11 Mode
- WLAN Security
- Authentication Method
- User name
- Password
- Passphrase

- Encryption keys
- Use DHCP to get IP address and DNS servers
- Static Settings (if configured)
  - IP Address
  - Subnet Mask
  - Default Router
  - Primary DNS Server
  - Secondary DNS Server
- Use DHCP to get TFTP Server
- Static TFTP Settings (if configured)
  - TFTP Server 1
  - TFTP Server 2

Advanced Network Profile Settings

- Minimum PHY rate
- Surplus Bandwidth
- 802.11G Power Settings (checked ones)
- 802.11A Power Settings (checked ones)

USB Settings (use one of these)

- Obtain IP address from server

  or
- Static settings (if configured)
  - IP address
  - Subnet Mask

Trace Settings

- Number of Files
- Syslog Server (enabled/disabled)
  - IP address
  - Port

- Modules and error level for collection
- Preserving Logs (true/false)

Importing a Configuration Template

To import a phone configuration template, follow these steps:

Procedure

Step 1 Connect the USB cable to an unconfigured phone and access the phone's web page using the instructions on "Accessing the Phone Web Page" section on page 4-5.

Step 2 On the phone's web page, choose the **Backup Settings** hyperlink.

Step 3 In the Import Configuration area of the page, enter the Encryption Key.

Note You must enter the same key that you used to export the configuration template.

Step 4 Use the Browse button to locate the configuration template and click **Open**.

The configuration file downloads to the phone.

Step 5 You can use the web pages to add missing configuration items such as the username and password or make other changes at this time.

Related Topics

- Using System Settings, page 4-46
- Viewing Trace Logs, page 4-47
- Upgrading Phone Firmware, page 4-51
- Changing the Admin Password, page 4-52

Upgrading Phone Firmware

You can use the Phone Upgrade area on the web page to upgrade firmware files on the phones by using the USB connection or by using the WLAN.

To display the Phone Upgrade area, access the web page for the phone as described in the "Accessing the Configuration Web Page for a Phone" section on page 4-7, and then click the **Phone Upgrade** hyperlink.

To upgrade the phone software, enter the phone software TAR (firmware file name) or use the Browse button to locate the firmware file on the network.

Related Topics

- Using System Settings, page 4-46
- Viewing Trace Logs, page 4-47
- Backup Settings for Phone Configuration, page 4-47
- Changing the Admin Password, page 4-52

Changing the Admin Password

Cisco Unified CallManager 4.1 or Later

If you are running Cisco Unified CallManager 4.1 or later, you can use the Change Password area on the web page to change the administration password for the phone web pages.

To change the password on the web page, you must first enter the old password. Enter the new password and then reenter the new password to confirm the change.

To display the Change Password area, access the web page for the phone as described in the "Accessing the Configuration Web Page for a Phone" section on page 4-7, and then click the **Change Password** hyperlink.

Cisco Unified Communications Manager 5.0 or Later

If you are running Cisco Unified Communications Manager 5.0 or later, you must set the password in Cisco Unified Communications Manager Administration on the Phone Configuration page. The password set in Cisco Unified Communications Manager takes precedence over the password that is set on the web pages.

Caution When setting the Administration Password in the Product Specific Configuration section in Cisco Unified Communications Manager 5.0 Administration, you must enable TFTP encryption. Otherwise, the password appears in readable text in the phone configuration file and can be viewed from any host that has access to TFTP server.

Related Topics

- Using System Settings, page 4-46
- Viewing Trace Logs, page 4-47
- Upgrading Phone Firmware, page 4-51
- Backup Settings for Phone Configuration, page 4-47

Viewing the Site Survey Report on the Web

Before the Site Survey Report is generated for viewing from the phone web page, you must first run the Site Survey utility from the phone. For more information, see Using the Site Survey Utility, page 2-35.

To view the report, go to the phone web page and choose **Site Survey** from the left pane. An HTML report in the form of a neighbor table of APs is displayed.

Note You can also run the Neighbor List utility from the phone to display a list of current APs on the phone. However, this utility will not generate the Site Survey Report that you can access from the phone web page. See also Using the Neighbor List Utility, page 2-34.

The neighbor table provides a matrix of APs observed during the site survey. Depending on the extent of the survey, not all observed APs will be considered a best AP or an immediate neighbor.

The Site Survey Report stores information about each AP until it reaches a limit of 256 APs. For each AP, up to ten neighbors are tracked.

Table 4-8 shows the information shown in the site survey report.

Table 4-8 Site Survey Report Neighbor Table

Information	Description/Indicator
Report title	The SSID used during Site Survey is displayed in the report title.
Best AP	Information displayed in cell with yellow background and where the row heading matches the column heading (for example, 64%-60/-43): • Percentage of time it is the best AP. • RSSI range during the time it is the best AP. **Note** A low number (below -65) may indicate insufficient overlap between the best AP and its neighbors.
Immediate Neighbor	Information may be displayed in the following way: • Pink background— If AP is on the same channel as the best AP. **Note** Being on the same channel as the best AP might indicate a problem with the channel re-use pattern, particularly if the percentage of time the AP is an immediate neighbor is relatively high compared to other immediate neighbors. • Asterisk (*)—Not an immediate neighbor. Information displayed in cell (for example, 27%-61/-39): • Percentage of time it is the immediate neighbor of the best AP. • RSSI range during the time it is the immediate neighbor.

Table 4-9 shows the information shown in the AP details report.

Table 4-9 AP Details Report

Field	Description
AP	Name of the AP if it is CCX-compliant; otherwise, the MAC address is displayed here.
MAC	MAC address of the AP.
Observation Count	Number of sweeps where this AP has been observed.
Channel - Frequency	The last channel and frequency where this AP was observed.
Country	A two-digit country code. Country information might not be displayed if the country information element (IE) is not present in the beacon.
Beacon Interval	Number of time units between beacons. A time unit is 1.024 ms.
DTIM Period	Every *n*th beacon is a DTIM period. After each DTIM beacon, the AP would send any broadcast or multicast packets that may have been queued for power-save devices.
RSSI Range [Lo Hi]	The entire RSSI range in which this AP has been observed.
BSS Lost Count	When a sweep does not discover an AP, the last best AP is flagged with a BSS lost count.
Channel Utilization	The percentage of time, normalized to 255, in which the AP sensed the medium was busy, as indicated by the physical or virtual carrier sense (CS) mechanism.
Station Count	Total number of spanning tree algorithms (STAs) currently associated with this BSS.
Available Admission Capacity	An unsigned integer that specifies the remaining amount of medium time available through explicit admission control, in units of 32 µs/s.
Basic Rates	Data rates required by the AP at which the station must be capable of operating.

Table 4-9 AP Details Report (continued)

Field	Description
Optional Rates	Data rates supported by the AP that are optional for the station to operate at.
Multicast Cipher and Unicast Cipher	For Multicast Cipher, one of the following; for Unicast Cipher, one or more of the following: • None • WEP40 • WEP104 • TKIP • CCMP • CKIP CMIC • CKIP • CMIC
AKM	One or more of the following: • WPA1_1X • WPA_PSK • WPA2_1X • WPA2_PSK • WPA1_CCKM • WPA2_CCKM
Proxy ARP Supported	CCX compliant AP supports responding to IP ARP requests on behalf of the associated station. Thjs feature is critical to standby time on the wireless IP phone.
WMM Supported	Support for WiFi Multi-Media Extensions.
CCX Version Number	Version of CCX if the AP is CCX compliant.

Table 4-9 AP Details Report (continued)

Field	Description
U-APSD Supported	Unscheduled Automatic Power Save Delivery is supported by the AP. May only be available if WMM is supported. This feature is critical to talk time and achieving maximum call density on the wireless IP phone.
Background AC	Access Category information for each AC: • Admission Control Required—If yes, admission control must be used prior to transmission using the access paramters specific for this AC. • AIFSN—Number of slots after an SIFS duration a non-AP STA should defer before invoking a backoff or starting a transmission. • ECWMIN—Encodes value of CWmin in an exponent form to provide the minimum amount of time in a random backoff. • ECWMAX—Encodes value of CWmax in an exponent form to provide the maximum amount of time in a random backoff. • TXOpLimit—Interval of time in which a particular quality of service (QoS) station has the right to initiate frame exhange sequences onto the wireless medium.
Best Effort AC	
Video AC	
Voice AC	
Channels	A list of supported channels (from the country IE).
Power	Maximum transmit power in dBm permitted for that channel.
Warning messages (in red at the bottom)	The first AP in the list (reference AP) is compared against the values recommended by Cisco, the differences are reported as warnings, and warning messages appear at the bottom of this report. All other APs are compared against the reference AP for consistency.