Cisco Wireless IP Phone 8821 and 8821-EX Administration Guide for Cisco Unified Communications Manager

Updated: August 26, 2020

Chapter: Configuration on the Phone

Chapter Contents

Manually Set Up the Phone Network from the Settings Menu

When you are setting up the phone manually, you must set the following fields:

- IP address

- Subnet mask
- Default router
- DNS server 1
- TFTP server 1

After you set up the network configuration, you set up the Wi-Fi connection.

Procedure

Step 1 Access the **Settings** app.

Step 2 Select **Wi-Fi**.

Step 3 Select a profile.

Step 4 (Optional) Set a profile name.

a. Select **Profile name**
b. Enter the name of the profile
c. Press **More** ••• and select **Save**.

Step 5 Select **Network configuration** > **IPv4 Setup**.

Step 6 Select **DHCP** and press **Off**.

Step 7 Enter an IP address for the phone.

a. Select **IP address**.
b. Press the Navigation ring down and press **Select** to enter edit mode.
c. Enter the IP address.
d. Press **Save**.

Step 8 Enter a subnet mask.

a. Select **Subnet mask**.
b. Press the Navigation ring down and press **Select** to enter edit mode.
c. Enter the mask.
d. Press **Save**.

Step 9 Enter a default router.

a. Select **Subnet mask**.
b. Press the Navigation ring down and press **Select** to enter edit mode.
c. Enter the mask.
d. Press **Save**.

Step 10 Enter the primary DNS server.

a. Select **DNS server 1**.
b. Press the Navigation ring down and press **Select** to enter edit mode.
c. Enter the IP address of the DNS server.

d. Press **Save**.

Step 11 Enter the primary TFTP server

a. Select **TFTP server 1**.

b. Press the Navigation ring down and press **Select** to enter edit mode.

c. Enter the IP address of the TFTP server for your Cisco Unified Communications Manager.

d. Press **Save**.

Step 12 Press **Erase** at the Trust list prompt.

When you select **Erase**, the CTL and ITL files are removed from the phone. If you select **Continue**, the files remain but you may not be able to connect to the new Cisco Unified Communications Manager.

- Access the Settings App

Related Tasks

Reset the Network Settings
Access the Settings App

Access the Settings App

You use the **Settings** app to set up, manage, and customize your phone.

Procedure

Step 1 From the Line view screen, press the left arrow of the navigation cluster to view the Applications screen.

Step 2 From the Applications screen, press the left arrow of the navigation cluster to select **Settings** ⚙.

Add the Phone to the Wi-Fi Network

When you enter an IP address, scroll to the field, and press **Select**. The field changes from one field into input boxes. You use the keypad to enter the digits and the navigation ring to move between the fields.

After you configure the phone and save the changes, the phone connects to the Cisco Unified Communications Manager. After the connection is made, the phone downloads the configuration file and, if necessary, upgrades the firmware to a new firmware load.

Before you begin

You need the following information about the Wi-Fi network:

- SSID
- Security type (for example, WEP, EAP)
- PIN or passkey for the selected security type

Procedure

Step 1 Access the **Settings** app.

Step 2 Select **Wi-Fi**.

Step 3 Select a profile.

Step 4 (Optional) Set a profile name.

a. Select **Profile name**.

b. Use the keypad to enter a new name.

- The **Back** ⌫ softkey deletes the character to the left of the cursor.
- Use the Navigation ring to move from left to right in the field.

c. Press **More** ••• and select **Save**.

Step 5 Select **Network configuration** > **IPv4 setup**.

If your network does not support DHCP, perform these steps.

a. Select **DHCP** and press **Off**.

b. Select **IP address** and enter the assigned address of the phone.

c. Select **Subnet mask** and enter the required subnet mask. For example, 255.255.255.0.

d. Select **Default router** and enter the IP address of the Default router.

e. Select **DNS server 1** and enter the IP address of the DNS server.

For all networks,

a. Select Alternate TFTP and set to **On**.

b. Select TFTP Server 1 and enter the TFTP IP address for the Cisco Unified Communications Manager.

c. Press **More** and select **Save**.

d. In the Trust list window, press **More** and select **Erase**.

e. Select **Back** and then select **Back** again.

Step 6 Select **WLAN configuration**.

Step 7 Select **SSID**.

a. Use the keypad to enter the SSID of the access point.

b. Press **More** and select **Save**.

Step 8 Select **Security mode**.

Step 9 Select the type of security that the access point requires.

Step 10 Set the required security fields using the following table:

Security Mode	Configured Field	Description
None	None	When the Security mode is set to None, no other fields are required.
WEP	WEP key	Enter the 40/104 or 64/128 ASCII or Hex WEP key.
PSK	Passphrase	Enter the 8-63 ASCII or 64 Hex Passphrase.
EAP-FAST PEAP-GTC PEAP-MSCHAPV2	User ID Password	Enter the userid. Enter the password

Security Mode	Configured Field	Description
EAP-TLS	User certificate	Select the type of certificate. You may need to give the certificate to your users. For more information, see Certificates.

Step 11 Select **802.11 mode** and select the required mode.

The mode determines the frequency. If you set the mode to Auto, the phone can use either the 5 GHz or 2.4 GHz frequency, with 5 GHz as the preferred frequency.

Step 12 Select **On call power save** and press **Select** to change the setting.

This field should only be set to Disabled if required for troubleshooting.

Step 13 Press **More** and select **Save**.

Step 14 Press **Power/End Call** ☎.

Related Tasks

Access the Settings App

Connect the Phone to the Cisco Unified Communications Manager

Before you begin

- You need the IP address of the Cisco Unified Communications Manager TFTP server.
- The phone must be configured in the Cisco Unified Communications Manager
- The phone must be connected to the Wi-Fi network.

Procedure

Step 1 Access the **Settings** app.

Step 2 Select **Wi-Fi**.

Step 3 Select a profile.

Step 4 Select **Network configuration** > **IPv4**

Step 5 Select Alternate TFTP and set to **On**.

Step 6 Select TFTP Server 1 and enter the TFTP IP address for the Cisco Unified Communications Manager.

Step 7 Press **More** ••• and select **Set**.

Step 8 In the Trust list window, press **More** and select **Erase**.

When you select **Erase**, the CTL and ITL files are removed from the phone. If you select **Continue**, the files remain but you may not be able to connect to the new Cisco Unified Communications Manager.

Step 9 Exit to the home screen.

The phone connects to the Cisco Unified Communications Manager. After the connection is made, the phone downloads the configuration file and, if necessary, upgrades the firmware to a new firmware load.

Related Tasks

Access the Settings App

Cisco IP Phone Administration Page

Cisco phones that support Wi-Fi have special web pages that are different from the pages for other phones. You use these special web pages for phone security configuration when Simple Certificate Enrollment Protocol (SCEP) is not available. Use these pages to manually install security certificates on a phone, to download a security certificate, or to manually configure the phone date and time.

These web pages also show the same information that you see on other phone web pages, including device information, network setup, logs, and statistical information.

You can access the administration pages in these ways:

- wireless connection
- direct USB connection
- USB Ethernet dongle

Configure the Administration Page for Phone

The administration web page is enabled when the phone ships from the factory and the password is set to Cisco. But if a phone registers with Cisco Unified Communications Manager, the administration web page must be enabled and a new password configured.

Enable this web page and set the sign-in credentials before you use the web page for the first time after the phone has registered.

Once enabled, the administration web page is accessible at HTTPS port 8443 (`https://x.x.x.x:8443`, where x.x.x.x is a phone IP address).

Before you begin

Decide on a password before you enable the administration web page. The password can be any combination of letters or numbers, but it must be between 8 and 127 characters in length.

Your username is permanently set to admin.

Procedure

Step 1 From the Cisco Unified Communications Manager Administration, select **Device** > **Phone**.

Step 2 Locate your phone.

Step 3 In the Product Specific Configuration Layout, set the Web Admin parameter to **Enable**.

Step 4 In the Admin Password field, enter a password.

Step 5 Select **Save** and click **OK**.

Step 6 Select **Apply Config** and click **OK**.

Step 7 Restart the phone.

Access the Phone Administration Web Page

When you want to access the administration web pages, you need to specify the administration port.

Procedure

Step 1 Obtain the IP address of the phone:

- In Cisco Unified Communications Manager Administration, select **Device** > **Phone**, and locate the phone. Phones that register with Cisco Unified Communications Manager display the IP address on the Find and List Phones window and at the top of the Phone Configuration window.
- On the phone, access the **Settings** app, choose **Phone Information** > **Network** > **IPv4**, and then scroll to the IP address field.

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

```
https://<IP_address>:8443
```

Step 3 Enter the password in the Password field.

Step 4 Click **Submit**.

Related Tasks

Access the Settings App

Set Up the Phone with the Administration Web Page

You can set the phone parameters from the Administration web page if you need to set up the phone remotely. When you set up the phone this way, you set up the first WLAN profile for the phone.

Procedure

Step 1 From the phone administration web page, select **WLAN**.

Step 2 Click **Profile 1**.

Step 3 Set the fields as described in the following table.

Field Name	Description
Source	Read-only field
Status	Use to enable or disable the profile.
Profile	Enter the name of the profile.
User modifiable	Set the field to enable or disable the user from changing their WLAN profile.
WLAN configuration	
SSID	Enter the SSID of the access point.
Security mode	Select a security mode.

Field Name	Description
WEP key	When the security type is set to WEP, the screen changes to display the **WEP key** field. enter a 40/104 or 64/128 ASCII or Hex WEP key.
Passphrase	When the security type is set to PSK, the screen changes to display the **Passphrase** field. Enter an 8-63 ASCII or 64Hex passphrase.
User ID	When the security type is EAP-Fast, PEAP-GTC, or PEAP-MSCHAPV2, the screen changes to display the **User ID** field. Enter the id of the user.
Password	When the security type is EAP-Fast, PEAP-GTC, or PEAP-MSCHAPV2, the screen changes to display the **Password** field. Enter a password.
User certificate	Select the type of certificate.
802.11 mode	Select the mode required.
On call power save	Select the type of power save mode that the phone uses to save power.
Network configuration	
Domain name	Enter the domain name.
IPv4 setup	
DHCP	Set your DHCP method. If DHCP is off, you have more fields to set up.
IP address	When DHCP is off, assign a static IP address
Subnet mask	When DHCP is off, enter the subnet mask.
Default router	When DHCP is off, enter the IP address of the router.
DNS server 1 DNS server 2 DNS server 3	When DHCP is off, enter the IP address of at least one DNS server.
Alternate TFTP	Set this field to indicate if you use a different TFTP server from the one associated with your Cisco Unified Communications Manager.
TFTP server 1 TFTP server 2	Enter the IP address of the Cisco Unified Communications Manager TFTP server (primary and, if available, secondary).

Step 4 Click **Save**.

Configure Backup Settings from the Phone Administration Web Page

You can use the phone administration web page to backup and restore the phone configuration.

Procedure

Step 1 From the phone administration web page, select **Backup settings**.

Step 2 Perform one of the following options:

- Import a backup file. Browse to the file on your computer, enter the encryption key, and click **Import**.
- Export a backup file. Enter an encryption key and click **Export**. Remember that you will need this key to import the file.

Manually Set the Phone Date and Time

With certificate-based authentication, the phone must display the correct date and time. An authentication server checks the phone date and time against the certificate expiry date. If the phone and the server dates and times don't match, the phone stops working.

Use this procedure to manually set the date and time on the phone if the phone is not receiving the correct information from your network.

Procedure

Step 1 From the phone administration web page, scroll to **Date and time**.

Step 2 Perform one of the following options:

- Click **Set phone to local date and time** to synch the phone to a local server.
- In the **Specify date and time fields**, select the month, day, year, hour, minute, and second using the menus and click **Set phone to specific date and time**.

Local Contacts Management from the Phone Administration Page

Through the phone administration web page, you can:

- Import a comma separated values (CSV) file of contacts into the user's phone.
- Export a user's local contacts list as a CSV file.
- Delete all the local contacts from a user's phone.

The import and export functions can be useful during initial phone setup. You could set up a list of commonly-used phone numbers for your organization on one phone. Then you could export that list and import it to other phones.

If you allow your users to access the phone administration page, make sure that you give them the local contacts import and export instructions.

Recommended Approach for Initial Local Contacts Lists

If you want to create a list to import to multiple phones, this approach is recommended:

1. Create a single entry in the local contacts list of a phone.
2. Export the list from the phone.
3. Edit the list to add the entries.

   You can use a text editor to edit the list.

If you use other tools (for example, document or spreadsheet programs), you need to save the list in one of these formats:

- CSV UTF-8
- Standard CSV

4. Import the list into the phone.
5. Verify that the list is displayed correctly before you import it on other phones.

- Import a User's Local Contacts
- Export a User's Local Contacts
- Delete a User's Local Contacts

Import a User's Local Contacts

You can import a CSV file into a user's phone. You can create this CSV file using a text editor or create the list on one phone and export it (see Export a User's Local Contacts).

You can add up to 200 Local contacts. However, if a Local contacts list already exists on the phone, the number of entries in the CSV file and in the phone can't exceed 200, or the import fails.

Only 49 of the entries can be marked as Favorites, because the first entry in the Favorites list is reserved for voicemail. If a Favorites list already exists on the phone, the number of entries in the CSV file that are marked as favorites and the number in the phone can't exceed 49, or the import fails.

The import does not check to see if the entries already exist in the phone, so duplicated entries are possible. Duplicated entries must be manually deleted.

Before you begin

Create a CSV file in the following format.

Sample CSV file

```
First name, Last name, Nickname, Company, Work number, Home number, Mobile number, Email address, Work prima
Michael,G,,Sample Company,1000,12345678,,test@test.com,true,false,false,2,3,
```

Where:

Field Name	Description	From the Sample
First name	First name as a string	Michael
Last name	Last name as a string, or leave empty	G
Nickname	Short name as a string, or leave empty	(empty)
Company	The company name as a string, or leave empty. **Note** The string cannot contain a comma.	Sample Company

Field Name	Description	From the Sample
Work number	The exact number to be dialed from the phone.	1000
Home number	The exact number to be dialed from the phone.	12345678
Mobile number	The exact number to be dialed from the phone.	(empty)
Email address	An email address, or leave empty	test@test.com
Work primary Home primary Mobile primary	Values—true, false Configure only one of these values to be true, and the other two are configured as false.	Work primary—true Home primary—false Mobile primary—false
Work favorite Home favorite Mobile favorite	Configure the Favorite slot number for any numbers to be added to Favorites. For example, enter 2 in Work favorite to map the Work number to Favorite slot 2. **Note** Favorite slot 1 is reserved for voicemail.	Work favorite—2 Home favorite—3 Mobile favorite—(empty)

Procedure

Step 1 From the phone administration web page, select **Local contacts.**

Step 2 Under **Import local contacts**, click **Browse**.

Step 3 Navigate to the CSV file, click on it, and click **OK.**

Step 4 Click **Upload**.

Step 5 Check on the phone to ensure that the list is displayed correctly.

Export a User's Local Contacts

You can export a phone's local contacts list as a CSV file.

Procedure

Step 1 From the phone administration web page, select **Local contacts.**

Step 2 Under **Export local contacts**, click **Export.**

Step 3 Save the file on your computer.

Delete a User's Local Contacts

You can delete the complete local contacts list from a phone. For example, you might do this before you assign the phone to another user.

Procedure

Step 1 From the phone administration web page, select **Local contacts**.

Step 2 Under **Delete all local contacts**, click **Delete**.

Step 3 In the pop-up window, confirm the deletion.

Step 4 Check that the local contacts list on the phone is empty.

Wireless LAN Security

Cisco phones that support Wi-Fi have more security requirements and require extra configuration. These extra steps include installing certificates and setting up security on the phones and on the Cisco Unified Communications Manager.

For additional information, see *Security Guide for Cisco Unified Communications Manager*.

- Install a User Certificate from the Phone Administration Web Page
- Install an Authentication Server Certificate from the Phone Administration Web Page
- Manually Remove a Security Certificate from the Phone Administration Web Page
- SCEP Setup

Install a User Certificate from the Phone Administration Web Page

You can manually install a user certificate on the phone if Simple Certificate Enrollment Protocol (SCEP) is not available.

The preinstalled Manufacturing Installed Certificate (MIC) can be used as the User Certificate for EAP-TLS.

After the User Certificate installs, you need to add it to the RADIUS server trust list.

Before you begin

Before you can install a User Certificate for a phone, you must have:

- A User Certificate saved on your PC. The certificate must be in PKCS #12 format.
- The certificate's extract password.

Procedure

Step 1 From the phone administration web page, select **Certificates**.

Step 2 Locate the **User installed** field and click **Install.**

Step 3 Browse to the certificate on your PC.

Step 4 In the **Extract password** field, enter the certificate extract password.

Step 5 Click **Upload.**

Step 6 Restart the phone after the upload is complete.

Install an Authentication Server Certificate from the Phone Administration Web Page

You can manually install an Authentication Server certificate on the phone if Simple Certificate Enrollment Protocol (SCEP) is not available.

The root CA certificate that issued the RADIUS server certificate must be installed for EAP-TLS.

Before you begin

Before you can install a certificate on a phone, you must have an Authentication Server Certificate saved on your PC. The certificate must be encoded in PEM (Base-64) or DER.

Procedure

Step 1 From the phone administration web page, select **Certificates**.

Step 2 Locate the **Authentication server CA (Admin webpage)** field and click **Install**.

Step 3 Browse to the certificate on your PC.

Step 4 Click **Upload**.

Step 5 Restart the phone after the upload is complete.

If you are installing more than one certificate, install all of the certificates before restarting the phone.

Manually Remove a Security Certificate from the Phone Administration Web Page

You can manually remove a security certificate from a phone if Simple Certificate Enrollment Protocol (SCEP) is not available.

Procedure

Step 1 From the phone administration web page, select **Certificates**.

Step 2 Locate the certificate on the Certificates page.

Step 3 Click **Delete**.

Step 4 Restart the phone after the deletion process completes.

SCEP Setup

Simple Certificate Enrollment Protocol (SCEP) is the standard for automatically provisioning and renewing certificates. It avoids manual installation of certificates on your phones.

- Configure the SCEP Product Specific Configuration Parameters
- Simple Certificate Enrollment Protocol Server Support

Configure the SCEP Product Specific Configuration Parameters

You must configure the following SCEP parameters on your phone web page

- RA IP address
- SHA-1 or SHA-256 fingerprint of the root CA certificate for the SCEP server

The Cisco IOS Registration Authority (RA) serves as a proxy to the SCEP server. The SCEP client on the phone use the parameters that are downloaded from Cisco Unified Communication Manager. After you configure the parameters, the phone sends a `SCEP getcs` request to the RA and the root CA certificate is validated using the defined fingerprint.

Procedure

Step 1 From the Cisco Unified Communications Manager Administration, select **Device** > **Phone**.

Step 2 Locate the phone.

Step 3 Scroll to the Product Specific Configuration Layout area.

Step 4 Check the **WLAN SCEP Server** check box to activate the SCEP parameter.

Step 5 Check the **WLAN Root CA Fingerprint (SHA256 or SHA1)** check box to activate the SCEP QED parameter.

Simple Certificate Enrollment Protocol Server Support

If you are using a Simple Certificate Enrollment Protocol (SCEP) server, the server can automatically maintain your user and server certificates. On the SCEP server, configure the SCEP Registration Agent (RA) to:

- Act as a PKI trust point
- Act as a PKI RA
- Perform device authentication using a RADIUS server

For more information, see your SCEP server documentation.

Set Up a Phone with the USB Dongle and the Desktop Charger

A USB to Ethernet adapter (dongle) can be inserted into the desktop charger to connect to an Ethernet network for automatic Wi-Fi profile provisioning and certificate enrollment purposes only. Voice calls over the Ethernet network are not supported.

Note The USB Dongle is not intended to be connected to the desktop charger for day-to-day use. It is intended to be only used for initial provisioning purposes.

The native VLAN of the switch port to be used for provisioning must have connectivity to the Cisco Unified Communications Manager and must offer DHCP option 150 pointing it to the Cisco Unified Communications Manager.

The supported USB to Ethernet adapters are:

- Apple USB 2.0 Ethernet Adapter
- Belkin B2B048 USB 3.0 Gigabit Ethernet Adapter
- D-Link DUB-E100 USB 2.0 Fast Ethernet Adapter
- Linksys USB300M USB 2.0 Ethernet Adapter
- Linksys USB3GIG USB 3.0 Gigabit Ethernet Adapter

Before you begin

You need a USB to Ethernet adapter (dongle).

The desktop charger must be connected to the power source using the power adapter.

Procedure

Step 1 In Cisco Unified Communications Manager Administration, check that the WLAN Profile you created is associated to either the correct CUCM device pool (**System** > **Device Pool**), or associated with the wireless phone (**Device** > **Phone**).

Step 2 Connect one end of the dongle into the desktop charger and the other end to an RJ-45 cable connected to the network switch.

Step 3 Put the phone into the desktop charger and wait while the profile downloads.

Step 4 Check that the phone registers to the Cisco Unified Communications Manager.

Step 5 Remove the phone from the desktop charger.

Step 6 Disconnect the dongle from the desktop charger.