Deployment

- Configuration Files, page 1
- Determine MAC Address, page 2
- Cisco Unified Communications Manager Device Addition Methods, page 2
- Cisco Unified Communications Manager User Addition, page 5
- Identify Device Model, page 7
- Configure Line Settings, page 7
- Associate User with Device, page 8
- Survivable Remote Site Telephony, page 9

Configuration Files

The TFTP server stores the device configuration files that define parameters for connection to Cisco Unified Communications Manager. In general, any time you make a change in Cisco Unified communications Manager that requires the device to be reset, a change is automatically made to the configuration file.

Configuration files also contain information about the image load that the device should be running. If this image load differs from the one that is currently loaded on a device, the device contacts the TFTP server to request the required load files. Due to the size of the image loads it is mandatory that TCP port 6970 be open between the device and the TFTP server.

A device accesses a default configuration file, named XmlDefault.cnf.xml, from the TFTP server when the following conditions exist:

- You enable autoregistration in Cisco Unified Communications Manager.
- You have not added the device to the Cisco Unified Communications Manager database.
- The device registers for the first time.

Note If the device security mode in the configuration file is set to Authenticated or Encrypted, but the device has not received a CTL or ITL file, the device makes four attempts to obtain the file so the device can register securely.

If autoregistration is not enabled and the device has not been added to the Cisco Unified Communications Manager database, the registration request will be rejected. The device displays `Out of service` on the screen.

Cisco DX Series devices access the configuration file, SEPmac_address.cnf.xml, where mac_address is the Ethernet MAC address of the device. The device will instead access the configuration file named SEPmac_address.cnf.xml.sgn if a CTL or ITL file is installed. The **Description** field in the **Phone Configuration** window of Cisco Unified Communications Manager Administration is prepopulated when the device is first configured. The MAC address identifies the device uniquely.

Determine MAC Address

You can determine the MAC address of a device in these ways:

- From the device, tap **Applications** > **Settings** > **About device** > **Status** and look at the **Ethernet MAC Address** field.
- Look at the MAC label on the back of the device.
- Display the web page for the device and click the **Device Information** hyperlink.

Cisco Unified Communications Manager Device Addition Methods

Before you install the device, you must choose a method for addition of endpoints to the Cisco Unified Communications Manager database.

The following table provides an overview of the methods for addition of devices to the Cisco Unified Communications Manager database.

Table 1: Methods for Adding Devices to the Cisco Unified Communications Manager

Method	Requires MAC Address?	Notes
Autoregistration	No	Results in automatic assignment of directory numbers.
Autoregistration with Tool for Autoregistered Phones Support (TAPS)	No	Requires autoregistration and the Bulk Administration Tool; updates information in the device and in Cisco Unified Communications Manager Administration.
Cisco Unified Communications Manager Administration	Yes	Requires devices to be added individually.

Method	Requires MAC Address?	Notes
Cisco Unified Communications Manager Bulk Administration Tool	Yes	Allows for simultaneous registration of multiple devices.
Self-Provisioning	No	Allows the user to provision their own device.

Autoregistration

By enabling autoregistration before you begin to install devices, you can:

- Add devices without prior collection of MAC addresses from the devices.
- Automatically add a device to the Cisco Unified Communications Manager database when you physically connect the device to your IP telephony network. During autoregistration, Cisco Unified Communications Manager assigns the next available sequential directory number to the device.
- Quickly enter devices into the Cisco Unified Communications Manager database and modify any settings, such as the directory numbers, from Cisco Unified Communications Manager.
- Move autoregistered devices to new locations and assign them to different device pools without affecting their directory numbers.

Note Cisco recommends that you use autoregistration to add fewer than 100 devices to your network. To add more than 100 devices to your network, use the Bulk Administration Tool.

Autoregistration is disabled by default. In some cases, you might not want to use autoregistration; for example, if you want to assign a specific directory number to the device, or if you want to use a secure connection with Cisco Unified Communications Manager as described in the *Cisco Unified Communications Manager Security Guide*. For information about enabling autoregistration, see the "Autoregistration Setup" section in the *Cisco Unified Communications Manager Security Guide*.

Autoregistration and TAPS

You can add devices with autoregistration and TAPS, the Tool for Autoregistered Phones Support, without prior collection of MAC addresses from devices.

TAPS works with the Bulk Administration Tool to update a batch of devices that were already added to the Cisco Unified Communications Manager database with dummy MAC addresses. Use TAPS to update MAC addresses and to download predefined configurations.

Note Cisco recommends that you use autoregistration and TAPS to add fewer than 100 devices to your network. To add more than 100 devices to your network, use the Bulk Administration Tool.

To implement TAPS, you or the end user dials a TAPS directory number and follows voice prompts. After the process is complete, the device contains the directory number and other settings, and the device is updated in Cisco Unified Communications Manager Administration with the correct MAC address.

Autoregistration must be enabled in Cisco Unified Communications Manager Administration (**System** > **Cisco Unified CM**) for TAPS to function.

Note When you configure the cluster for mixed mode through the Cisco CTL client, autoregistration is automatically disabled. When you configure the cluster for nonsecure mode through the Cisco CTL client, autoregistration is not enabled automatically.

For more information, see the *Cisco Unified Communications Manager Bulk Administration Guide*.

Add Device in Cisco Unified Communications Manager

You can add devices individually to the Cisco Unified Communications Manager database. To do so, you first must obtain the MAC address for each device.

Procedure

Step 1 After you collect MAC addresses, in Cisco Unified Communications Manager Administration, choose **Device** > **Phone**.

Step 2 Click **Add New**.

Step 3 Choose the device type from the **Phone Type** drop-down list box.

Note Depending on the Cisco Unified Communications Manager version, when you add Cisco DX Series devices, you may need to install a Device Enabler before you install the firmware.

Step 4 Click **Next**.

Step 5 Enter the details of device-specific parameters (Device Pool, Device Security Profile, and so on).

Step 6 Click **Save**.
For more information, go to the "System Configuration Overview" chapter in the *Cisco Unified Communications Manager System Guide*.

Add Device with Bulk Administration Tool Phone Template

The Cisco Unified Communications Manager Bulk Administration Tool enables you to perform batch operations, such as registration of multiple devices.

For more information about the Bulk Administration Tool, see the *Cisco Unified Communications Manager Bulk Administration Guide*.

Procedure

Step 1 Obtain the MAC address for each device.

Step 2 From Cisco Unified Communications Manager, choose **Bulk Administration** > **Phones** > **Phone Template**.

Step 3 Click **Add New**.

Step 4 Choose a Phone Type and select **Next**.

Step 5 Enter the details of device-specific parameters, such as Device Pool and Device Security Profile.

Step 6 Click **Save**.

Step 7 From Cisco Unified Communications Manager Administration, choose **Device** > **Phone** > **Add New** to add a device by using an existing Bulk Administration Tool template.

Self-Provisioning

Self-provisioning allows the user to set up their device with less administrator effort. When self-provisioning is enabled, the user enters their credentials during the device setup. The device MAC address and other configuration information is shared with the Cisco Unified Communications Manager server.

Self-provisioning requires Cisco Unified Communications Manager Release 10.0 or later. For more information, see the "Self-Provisioning" chapter of the *Cisco Unified Communications Manager Administration Guide*.

Enable Self-Provisioning

Procedure

Step 1 In Cisco Unified Communications Manager Administration, go to **User Management** > **User Setting** > **User Profile**.

Step 2 Set Self-provisioning to **Enabled**.

Step 3 Go to **User Management** > **End User**.

Step 4 Set the Self-Service User ID.

Step 5 Go to **User Management** > **Self Provisioning** and choose an authentication mode.

Cisco Unified Communications Manager User Addition

This section describes steps for adding a user to Cisco Unified Communications Manager. Follow one of the procedures in this section, depending on your operating system and the manner in which you are adding the user.

Add User Directly to Cisco Unified Communications Manager

If you are not using an LDAP directory, you can add a user directly to Cisco Unified Communications Manager.

Note If LDAP is synchronized, you cannot add a user to Cisco Unified Communications Manager.

Procedure

Step 1 Choose **User Management** > **End User**, then click **Add New**.
The **End User Configuration** window appears.

Step 2 In the User Information pane of this window, enter the following:

- User ID - Enter the end user identification name. Cisco Unified Communications Manager does not permit modification of the user ID after it is created. You may use the following special characters: =, +, <, >, #, ;, \," ", and blank spaces.
- Password and Confirm Password - Enter five or more alphanumeric or special characters for the end user password. You may use the following special characters: =, +, <, >, #, ;, \," ", and blank spaces.
- Last Name - Enter the end user last name. You may use the following special characters: =, +, <, >, #, ;, \," ", and blank spaces.
- Telephone Number - Enter the primary directory number for the end user. End users can have multiple lines on their devices.

Step 3 Click **Save**.

Step 4 Proceed to Identify Device Model, on page 7.

Add User From External LDAP Directory

If you added a user to an LDAP Directory (a non-Cisco Unified Communications Server directory), you can immediately synchronize that directory to the Cisco Unified Communications Manager on which you are adding this same user and device by following these steps:

Procedure

Step 1 Sign in to Cisco Unified Communications Manager Administration.

Step 2 Choose **System** > **LDAP** > **LDAP Directory**.

Step 3 Use the **Find** button to locate your LDAP directory.

Step 4 Click on the LDAP directory name.

Step 5 Click **Perform Full Sync Now**.

Note If you do not need to synchronize the LDAP Directory to the Cisco Unified Communications Manager immediately, the LDAP Directory Synchronization Schedule in the LDAP Directory window determines when the next auto-synchronization is scheduled. However, the synchronization must occur before you can associate a new user to a device.

Step 6 Proceed to Identify Device Model, on page 7.

Identify Device Model

Procedure

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

Step 2 Click **Add New**.

Step 3 Choose the device model from the **Phone Type** drop-down list, and then click **Next**.
The **Phone Configuration** window appears.

Step 4 Proceed to Configure Line Settings, on page 7.

Configure Line Settings

In the **Phone Configuration** window, you can use the default values for most of the fields.

Procedure

Step 1 On the **Phone Configuration** window, click **Line 1** on the left pane of the window. The **Directory Number Configuration** window appears.

Step 2 In the **Directory Number** field, enter the same number that appears in the **Telephone Number** field in the **User Configuration** window.

Step 3 From the **Route Partition** drop-down list, choose the partition to which the directory number belongs. If you do not want to restrict access to the directory number, choose <None> for the partition.

Step 4 From the **Calling Search Space** drop-down list (Directory Number Settings pane of the **Directory Number Configuration** window), choose the appropriate calling search space. A calling search space comprises a collection of partitions that are searched for numbers that are called from this directory number. The value that you choose applies to all devices that use this directory number.

Step 5 In the **Call Forward Settings** pane of the **Directory Number Configuration** window, choose the items (for example, Forward All, Forward Busy Internal) and corresponding destinations to which calls should be sent.

Example:

If you want incoming internal and external calls that receive a busy signal to be forwarded to the voice mail for this line, check the **Voice Mail** box in the Call Forward Settings pane.

Step 6 In the **Line 1** field in the Device pane of the **Directory Number Configuration** window, configure the following:

a) Display (**Internal Caller ID** field): You can enter the first name and last name of the user of this device so that this name will be displayed for all internal calls. You can also leave this field blank to have the system display the phone extension.

b) External Phone Number Mask: Indicate phone number (or mask) that is used to send Caller ID information when a call is placed from this line. You can enter a maximum of 24 number and "X" characters. The Xs represent the directory number and must appear at the end of the pattern.

Example:
If you specify a mask of 555902XXXX, an external call from extension 6640 displays a caller ID number of 5559026640.

c) Click **Save**.

Note This setting applies only to the current device unless you check **Update Shared Device Settings** and click the **Propagate Selected** button. (The check box at right displays only if other devices share this directory number.)

Step 7 Click **Associate End Users** at the bottom of the window to associate a user to the line that you are configuring.

a) Use the **Find** button in conjunction with the **Search** fields to locate the user.

b) Check the box next to the username, then choose **Add Selected**.
The username and user ID appear in the Users Associated With Line pane of the **Directory Number Configuration** window.

c) Click **Save**.
The user is now associated with Line 1 on the device.

Step 8 If the device has a second line, configure Line 2.

Step 9 Proceed to Associate User with Device, on page 8.

Associate User with Device

Procedure

Step 1 From Cisco Unified Communications Manager Administration, choose **User Management** > **End User**.
The **Find and List Users** window appears.

Step 2 Enter the appropriate search criteria and click **Find**.

Step 3 In the list of records that appear, choose the link for the user.

Step 4 Choose **Device Association**.

The **User Device Association** window appears.

Step 5 Enter the appropriate search criteria and click **Find**.

Step 6 Choose the device that you want to associate with the user by checking the box to the left of the device.

Step 7 Choose **Save Selected/Changes** to associate the device with the user.

Step 8 From the **Related Links** drop-down list, choose **Back to User**, and click **Go**.
The **End User Configuration** window appears and the associated devices that you chose display in the Controlled Devices pane.

Step 9 Choose **Save Selected/Changes**.

Survivable Remote Site Telephony

Survivable Remote Site Telephony (SRST) ensures that basic call functions remain accessible when communications with the controlling Cisco Unified Communications Manager are broken. In this scenario, the device can keep an in-progress call active, and the user can access a subset of the features available. When failover occurs, the user receives an alert message on the device. SRST requires Cisco IOS version 12.4(20) or above.

Note SRST does not support IPv6.