Extension Mobility

- Extension Mobility Overview, on page 1
- Extension Mobility Prerequisites, on page 1
- Extension Mobility Configuration Task Flow, on page 2
- Cisco Extension Mobility Interactions, on page 9
- Cisco Extension Mobility Restrictions, on page 11
- Extension Mobility Troubleshooting, on page 12

Extension Mobility Overview

Cisco Extension Mobility allows users to temporarily access their phone settings, such as line appearances, services, and speed dials, from other phones within your system. If you have a single phone that will be used by multiple workers, for example, you can configure extension mobility so that individual users can log in to the phone and access their settings without affecting settings on other user accounts.

After a user logs in using extension mobility and if the extension mobility profile is already associated to the application user, then CTI application sends device-related information.

CTI application can control a device the user is logged into (using that extension mobility profile) without having to have direct control of the device. Therefore, the recording with the device profile association to the application user should work though they have not associated the device directly.

Extension Mobility Prerequisites

- A TFTP server that is reachable.
- Extension mobility functionality extends to most Cisco Unified IP Phones. Check the phone documentation to verify that Cisco Extension Mobility is supported.

Extension Mobility Configuration Task Flow

Before you begin

Procedure

	Command or Action	Purpose
Step 1	Generate a Phone Feature List	Generate a report to identify devices that support the extension mobility feature.
Step 2	Activate Extension Mobility Services, on page 2	
Step 3	Configure the Cisco Extension Mobility Phone Service, on page 3	Configure the extension mobility IP phone service to which users can later subscribe to access extension mobility.
Step 4	Create an Extension Mobility Device Profile for Users, on page 4	Configure an extension mobility device profile. This profile acts as a virtual device that maps onto a physical device when a user logs in to extension mobility. The physical device takes on the characteristics in this profile.
Step 5	Associate a Device Profile to a User, on page 4	Associate a device profile to users so that they can access their settings from a different phone. You associate a user device profile to a user in the same way that you associate a physical device.
Step 6	Subscribe to Extension Mobility, on page 5	Subscribe IP phones and device profiles to the extension mobility service so that users can log in, use, and log out of extension mobility.
Step 7	Configure the Change Credential IP Phone Service, on page 5	To allow users to change their PINs on their phones, you must configure the change credential Cisco Unified IP Phone service and associate the user, the device profile, or the IP phone with the change credential phone service.
Step 8	(Optional) Configure Service Parameters for Extension Mobility, on page 6	If you want to modify the behavior of extension mobility, configure the service parameters.

Activate Extension Mobility Services

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Service Activation**.

Step 2 From the **Server** drop-down list, choose the requried node.

Step 3 Activate the following services:

a) Cisco CallManager
b) Cisco Tftp
c) Cisco Extension Mobility
d) ILS Service

Note You must choose publisher node to activate the ILS services.

Step 4 Click **Save**.

Step 5 Click **OK**.

Configure the Cisco Extension Mobility Phone Service

Configure the extension mobility IP phone service to which users can later subscribe to access extension mobility.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Phone Services**.

Step 2 Click **Add New**.

Step 3 In the **Service Name** field, enter a name for the service.

Step 4 In the **Service URL** field, enter the Service URL.

The format is `http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#`. `IP Address` is the IP address of the Unified Communications Manager where Cisco Extension Mobility is activated and running.

It can either be a IPv4 or a IPv6 address.

Example:

`http://123.45.67.89:8080/emapp/EMAppServlet?device=#DEVICENAME#`

Example:

`http://[2001:0001:0001:0067:0000:0000:0000:0134]:8080/emapp/EMAppServlet?device=#DEVICENAME#`

This format allows a user to sign-in using User ID and PIN. You can configure more sign-in options for IP phone users who have subscribed to the extension mobility service. To configure more sign-in options, append the `loginType` parameter to the Service URL, in the following formats:

- `loginType=DN` enables users to sign in using Primary Extension and PIN.

  The Service URL format is:`http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&loginType=DN`.

- `loginType=SP` enables users to sign in using Self Service User ID and PIN.

  The Service URL format is:`http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&loginType=SP`.

- `loginType=UID` enables users to sign in using User ID and PIN.

  The Service URL format is:`http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&loginType=UID`.

If you do not append `loginType` to the end of the URL, the default sign-in option displayed is User ID and PIN.

Step 5 In the **Service Type** field, choose whether the service is provisioned to the Services, Directories, or Messages button.

Step 6 Click **Save**.

Create an Extension Mobility Device Profile for Users

Configure an extension mobility device profile. This profile acts as a virtual device that maps onto a physical device when a user logs in to extension mobility. The physical device takes on the characteristics in this profile.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Device Profile**.

Step 2 Perform one of the following tasks:

- Click **Find** to modify the settings and choose an existing device profile from the resulting list.
- Click **Add New** to add a new device profile and choose an option from the **Device Profile Type**. Click **Next**.
- Choose a device protocol from the **Device Protocol** drop-down list and click **Next**.

Step 3 Configure the fields. For more information on the fields and their configuration options, see Online Help.

Step 4 Click **Save**.

Step 5 From the **Association Information** section, click **Add a new DN**.

Step 6 In the **Directory Number** field, enter the directory number and click **Save**.

Step 7 Click **Reset** and follow the prompts.

Associate a Device Profile to a User

Associate a device profile to users so that they can access their settings from a different phone. You associate a user device profile to a user in the same way that you associate a physical device.

Tip You can use the Bulk Administration Tool (BAT) to add and delete several user device profiles for Cisco Extension Mobility at one time. See the Bulk Administration Guide for Cisco Unified Communications Manager.

Procedure

Step 1 From Cisco Unified CM Administration, choose **User Management** > **End User**.

Step 2 Perform one of the following tasks:

- Click **Find** to modify the settings for an existing user, enter search criteria, and choosing an existing user from the resulting list.
- Click **Add New** to add a new user.

Step 3 Under **Extension Mobility**, locate the device profile that you created and move it from **Available Profiles** to **Controlled Profiles**.

Step 4 Check the **Home Cluster** check box.

Step 5 Click **Save**.

Subscribe to Extension Mobility

Subscribe IP phones and device profiles to the extension mobility service so that users can log in, use, and log out of extension mobility.

Procedure

Step 1 Perform one of the following tasks from Cisco Unified CM Administration:

- Choose **Device** > **Phone**, specify search criteria, click **Find**, and choose a phone which users will use for extension mobility.
- Choose **Device** > **Device Settings** > **Device Profile**, specify search criteria, click **Find**, and choose the device profile that you created.

Step 2 From the **Related Links** drop-down list, choose **Subscribe/Unsubscribe Services**, and then click **Go**.

Step 3 From the **Select a Service** drop-down list, choose the **Extension Mobility** service.

Step 4 Click **Next**.

Step 5 Click **Subscribe**.

Step 6 Click **Save** and close the popup window.

Configure the Change Credential IP Phone Service

To allow users to change their PINs on their phones, you must configure the change credential Cisco Unified IP Phone service and associate the user, the device profile, or the IP phone with the change credential phone service.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Device** > **Device Settings** > **Phone Services**.

Step 2 Click **Add New**.

Step 3 In the **Service Name** field, enter **`Change Credential`**.

Step 4 In the **Service URL** field, enter the following value, where `server` designates the server where the Change Credential IP phone service runs:

```
http://server:8080/changecredential/ChangeCredentialServlet?device=#DEVICENAME#
```

Step 5 (Optional) In the **Secure-Service URL** field, enter the following value, where `server` is the server where the Change Credential IP phone service runs:

```
https://server:8443/changecredential/ChangeCredentialServlet?device=#DEVICENAME#
```

Step 6 Configure the remaining fields in the **IP Phone Services Configuration** window, and choose **Save**.

Step 7 To subscribe the Cisco Unified IP Phone to the Change Credential IP phone service, choose **Device** > **Phone**.

Step 8 In the **Phone Configuration** window, go to the **Related Links** drop-down list and choose **Subscribe/Unsubscribe Services**.

Step 9 Click **Go**.

Step 10 From the **Select a Service** drop-down list, choose the **Change Credential IP phone service**.

Step 11 Click **Next**.

Step 12 Click **Subscribe**.

Step 13 Click **Save**.

Configure Service Parameters for Extension Mobility

(Optional)

If you want to modify the behavior of extension mobility, configure the service parameters.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Service Parameters**.

Step 2 From the **Server** field, choose the node that is running the Cisco Extension Mobility service.

Step 3 From the **Service** field, choose **Cisco Extension Mobility**.

Step 4 Click **Advanced** to show all service parameters.

See Extension Mobility Service Parameters, on page 7 for more information about these service parameters and their configuration options.

Step 5 Click **Save**.

Extension Mobility Service Parameters

Table 1: Extension Mobility Service Parameters

Service Parameter	Description
Enforce Intra-cluster Maximum Login Time	Select **True** to specify a maximum time for local logins. After this time, the system automatically logs out the device. **False**, which is the default setting, means that no maximum time for logins exists. To set an automatic logout, you must choose **True** for this service parameter and also specify a system maximum login time for the **Intra-cluster Maximum Login Time** service parameter. Cisco Unified Communications Manager then uses the automatic logout service for all logins.
Intra-cluster Maximum Login Time	This parameter sets the maximum time that a user can be locally logged in to a device, such as 8:00 (8 hours) or:30 (30 minutes). The system ignores this parameter and set the maximum login time to 0:00, if the **Enforce Intra-cluster Maximum Login Time** parameter is set to **False**. Valid values are between 0:01 and 168:00 in the format HHH:MM, where HHH represents the number of hours and MM represents the number of minutes.
Maximum Concurrent Requests	Specify the maximum number of login or logout operations that can occur simultaneously. This number prevents the Cisco Extension Mobility service from consuming excessive system resources. The default value of 5 is acceptable in most cases.
Intra-cluster Multiple Login Behavior	Choose one of the following options: • Multiple Logins Allowed—A user can log in to more than one device at a time. • Multiple Logins Not Allowed—The second and subsequent login attempts after a user successfully logs in once will fail. • Auto Logout—After a user logs in to a second device, the Cisco Unified Communications Manager automatically logs the user out of the first device. For EMCC, multiple logins are always allowed.
Alphanumeric User ID	Choose **True** to allow the user ID to contain alphanumeric characters. Choosing **False** allows the user ID to contain only numeric characters. **Note** The Alphanumeric User ID parameter applies systemwide. You can have a mix of alphanumeric and numeric user IDs. The system supports only user IDs that can be entered by using the alphanumeric keypad. The case-sensitive userid field requires the characters to be lowercase.

Service Parameter	Description
Remember the Last User Logged In	When you choose **False**, the system does not remember the last user who logged in to the phone. Use this option when the user access the phone on a temporary basis only. Choose True to remember the last user that logged into the phone. Use this option when a phone has only one user. For example, Cisco Extension Mobility is used to enable the types of calls that are allowed from a phone. Individuals who are not logged in and who are using their office phone can make only internal or emergency calls. But after logging in using Cisco Extension Mobility, the user can make local, long-distance, and international calls. In this scenario, only this user regularly logs in to the phone. It makes sense to set the Cisco Extension Mobility to remember the last user ID that logged in.
Clear Call Logs on Intra-cluster EM	Choose **True** to specify that the call logs are cleared during the Cisco Extension Mobility manual login and logout process. While a user is using the Cisco Extension Mobility service on an IP phone, all calls (placed, received, or missed) appear in a call log and can be retrieved and seen on the IP phone display. To ensure privacy, set the Clear Call Log service parameter to **True**. This ensures that the call logs are cleared when a user logs out and another user logs in. For extension mobility cross cluster (EMCC), the call log is always cleared when the user logs in or out of a phone. **Note** Call logs are cleared only during manual login/logout. If a Cisco Extension Mobility logout occurs automatically or any occurrence other than a manual logout, the call logs are not cleared.
Validate IP Address	This parameter sets whether validation occurs on the IP address of the source that is requesting login or logout. If the parameter is set to **True**, the IP address from which a Cisco Extension Mobility log in or log out request occurs and is validated to ensure that it is trusted. Validation is first performed against the cache for the device that will log in or log out. If the IP address is found in the cache or in the list of trusted IP addresses or is a registered device, the device can log in or log out. If the IP address is not found, the log in or log out attempt is blocked. If the parameter is set to **False**, the Cisco Extension Mobility log in or log out request is not validated. Validation of IP addresses can affect the time that is required to log in or log out a device, but it offers additional security that prevents unauthorized log in or log out attempts. This function is recommended, especially when used with logins from separate trusted proxy servers for remote devices.
Trusted List of IPs	This parameter appears as a text box (the maximum length is 1024 characters). You can enter strings of trusted IP addresses or hostnames which are separated by semicolons, in the text box. IP address ranges and regular expressions are not supported.

Service Parameter	Description
Allow Proxy	If the parameter is **True**, the Cisco Extension Mobility log in and log out operations that use a web proxy are allowed. If the parameter is **False**, the Cisco Extension Mobility log in and log out requests coming from behind a proxy get rejected. The setting that you select takes effect only if the Validate IP Address parameter specifies true.
Extension Mobility Cache Size	In this field, enter the size of the device cache that is maintained by Cisco Extension Mobility. The minimum value for this field is 1000 and the maximum is 20000. The default value is 10000. The value that you enter takes effect only if the Validate IP Address parameter is **True**.

Cisco Extension Mobility Interactions

Table 2: Cisco Extension Mobility Interactions

Feature	Interaction
Assistant	A manager who uses Cisco Extension Mobility can simultaneously use Cisco Unified Communications Manager Assistant. The manager logs in to the Cisco Unified IP Phone by using Cisco Extension Mobility and then chooses the Cisco IP Manager Assistant service. When the Cisco IP Manager Assistant service starts, the manager can access assistants and all Cisco Unified Communications Manager Assistant features (such as call filtering and Do Not Disturb).
BLF Presence	When you configure BLF/speed dial buttons in a user device profile, a phone that supports Cisco Extension Mobility displays BLF presence status on the BLF/SpeedDial buttons after you log in to the device. When the extension mobility user logs out, a phone that supports Cisco Extension Mobility displays BLF presence status on the BLF/SpeedDial buttons for the logout profile that is configured.
Call Display Restrictions	When you enable call display restrictions, Cisco Extension Mobility functions as usual: when a user is logged in to the device, the presentation or restriction of the call information depends on the user device profile that is associated with that user. When the user logs out, the presentation or restriction of the call information depends on the configuration that is defined for that phone type in the Phone Configuration window. To use call display restrictions with Cisco Extension Mobility, check the **Ignore Presentation Indicators (internal calls only)** check obx in both the **Device Profile Configuration** window and the **Phone Configuration** window.

Feature	Interaction
Call Forward All Calling Search Space	An enhancement to call forward all calling search space (CSS) lets you upgrade to later releases of Cisco Unified Communications Manager without loss of functionality. The **CFA CSS Activation Policy** service parameter supports this enhancement. In the **Service Parameter Configuration** window, this parameter displays in the **Clusterwide Parameters (Feature - Forward)** section with two options: • With Configured CSS (default) • With Activating Device/Line CSS
Do Not Disturb	For extension mobility, the device profile settings include do not disturb (DND) incoming call alert and DND status. When a user logs in and enables DND, the DND incoming call alert and DND status settings are saved, and these settings are used when the user logs in again. **Note** When a user who is logged in to extension mobility modifies the DND incoming call alert or DND status settings, this action does not affect the actual device settings.
Intercom	Cisco Extension Mobility supports the intercom feature. To support intercom, Cisco Extension Mobility uses a default device that is configured for an intercom line. An intercom line is presented on only the default device. You can assign an intercom line to a device profile. When a user logs in to a device that is not the default device, the intercome line is not presented. The following additional considerations apply to intercom for Cisco Extension Mobility: • When Unified Communications Manager assigns an intercom line to a device and the default device value is empty, the current device is selected as the default device. • When AXL programatically assigns an intercom DN, you must update the intercom DN separately by using Cisco Unified Communications Manager Administration to set the default device. • When you delete a device that is set as the intercom default device for an intercom line, the intercom default device is no longer set to the deleted device.
Internet Protocol Version 6 (IPv6)	Cisco Extension Mobility Supports IPv6. You can use phones with an IP addressing mode of IPv6 or dual-stack (IPv4 and IPv6).
Prime Line	If you select **On** for the **Always Use Prime Line** parameter in the **Device Profile** or **Default Device Profile Configuration** window, a Cisco Extension Mobility user can use this feature after logging in to the device that supports Cisco Extension Mobility.

Cisco Extension Mobility Restrictions

Table 3: Cisco Extension Mobility Restrictions

Feature	Restriction
Cache	Cisco Extension Mobility maintains a cache of all logged-in user information for 2 minutes. If a request comes to extension mobility regarding a user who is represented in the cache, the user is validated with information from the cache. For example, if a user changes the password, logs out, and then logs back in within 2 minutes, both the old and new passwords are recognized.
Call Back	When a Cisco Extension Mobility user logs out of a device, all call back services that are active for the Cisco Extension Mobility user are automatically cancelled.
Character Display	The characters that display when a user logs in depend on the current locale of the phone. For example, if the phone is currently in the English locale (based on the Logout profile of the phone), the user can only enter English characters in the UserID.
Hold Reversion	Cisco Extension Mobility does not support the hold reversion feature.
IP Phones	Cisco Extension Mobility requires a physical Cisco Unified IP Phone for login. Users of office phones that are configured with Cisco Extension Mobility cannot remotely log in to their phones.
Locale	If the user locale that is associated with the user or profile is not the same as the locale or device, after a successful login, the phone will restart and then reset. This behavior occurs because the phone configuration file is rebuilt. Addon-module mismatches between profile and device can cause the same behavior.
Log Out	If Cisco Extension Mobility is stopped or restarted, the system does not automatically log out users who are already logged in after the logout interval expires. Those phones automatically log out users only once a day. You can manually log out these users from either the phones or from Cisco Unified CM Administration.
Secure Tone	Cisco Extension Mobility and join across line services are disabled on protected phones.
User Group	Although you can add users to the Standard EM authentication proxy rights user group, those users are not authorized to authenticate by proxy.
Remember the Last User Logged In	The service parameter **Remember the Last User Logged In** is applicable only for default Extension Mobility service URL or the Extension Mobility service URL with `loginType` as `UID`.

Extension Mobility Troubleshooting

Troubleshoot Extension Mobility

Procedure

- Configure the Cisco Extension Mobility trace directory and enable debug tracing by performing the following steps:
  a) From Cisco Unified Serviceability, choose **Trace** > **Trace Configuration**.
  b) From the **Servers** drop-down list, select a server.
  c) From the **Configured Services** drop-down-list, select **Cisco Extension Mobility**.
- Make sure that you entered the correct URL for the Cisco Extension Mobility service. Remember that the URL is case sensitive.
- Check that you have thoroughly and correctly performed all the configuration procedures.
- If a problem occurs with authentication of a Cisco Extension Mobility user, go to the user pages and verify the PIN.

Authentication Error

Problem "Error 201 Authentication Error" appears on the phone.

Solution The user should check that the correct user ID and PIN were entered; the user should check with the system administrator that the user ID and PIN are correct.

Blank User ID or PIN

Problem "Error 202 Blank User ID or PIN" appears on the phone.

Solution Enter a valid user ID and PIN.

Busy Please Try Again

Problem "Error 26 Busy Please Try Again" appears on the phone.

Solution Check whether the number of concurrent login and logout requests is greater than the **Maximum Concurrent requests** service parameter. If so, lower the number of concurrent requests.

Note To verify the number of concurrent login and logout requests, use the Cisco Unified Real-Time Monitoring Tool to view the Requests In Progress counter in the Extension Mobility object. For more information, see the Cisco Unified Real-Time Monitoring Tool Administration Guide at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

Database Error

Problem "Error 6 Database Error" appears on the phone.

Solution Check whether a large number of requests exists. If a large number of requests exists, the Requests In Progress counter in the Extension Mobility object counter shows a high value. If the requests are rejected because of a large number of concurrent requests, the Requests Throttled counter also shows a high value. Collect detailed database logs.

Dev Logon Disabled

Problem "Error 22 Dev Logon Disabled" appears on the phone.

Solution Verify that you checked the **Enable Extension Mobility** check box in the **Phone Configuration** window (**Device** > **Phone**).

Device Name Empty

Problem "Error 207 Device Name Empty" appears on the phone.

Solution Check that the URL that is configured for Cisco Extension Mobility is correct. See the Related Topics section for more information.

Related Topics

Configure the Cisco Extension Mobility Phone Service, on page 3

EM Service Connection Error

Problem "Error 207 EM Service Connection Error" appears on the phone.

Solution Verify that the Cisco Extension Mobility service is running by selecting **Tools** > **Control Center—Feature** in Cisco Unified Serviceability.

Host Not Found

Problem The "Host Not Found" error message appears on the phone.

Solution Check that the Cisco Tomcat service is running by selecting **Tools** > **Control Center—Network Services** in CIsco Unified Serviceability.

HTTP Error

Problem HTTP Error (503) appears on the phone.

Solution

- If you get this error when you press the **Services** button, check that the Cisco IP Phone Services service is running by selecting **Tools** > **Control Center—Network Services** in Cisco Unified Serviceability.
- If you get this error when you select Extension Mobility service, check that the Cisco Extension Mobility Application service is running by selecting **Tools** > **Control Center—Network Services** in Cisco Unified Serviceability.

Phone Resets

Problem After users log in or log out, their phones reset instead of restarting.

Possible Cause Locale change is the probable cause of the reset.

Solution No action is required. If the user locale that is associated with the logged-in user or profile is not the same as the locale or device, after a successful login the phone will restart and then reset. This pattern occurs because the phone configuration file is rebuilt.

Phone Services Unavailable After Login

Problem After logging in, the user finds that the phone services are not available.

Possible Cause This problem occurs because the user profile had no services associated with it when it was loaded on the phone.

Solution

- Ensure that the user profile includes the Cisco Extension Mobility service.
- Change the configuration of the phone where the user is logged in to include Cisco Extension Mobility. After the phone is updated, the user can access the phone services.

Phone Services Unavailable After Logout

Problem After a user logs out and the phone reverts to the default device profile, the phone services are no longer available.

Solution

- Verify that the **Synchronization Between Auto Device Profile and Phone Configuration** enterprise parameter is set to **True**.
- Subscribe the phone to the Cisco Extension Mobility service.

User Logged in Elsewhere

Problem "Error 25 User Logged in Elsewhere" appears on the phone.

Solution Check whether the user is logged in to another phone. If multiple logins must be allowed, ensure that the **Multiple Login Behavior** service parameter is set to **Multiple Logins Allowed**.

User Profile Absent

Problem "Error 205 User Profile Absent" appears on the phone.

Solution Associate a device profile to the user.