Extension Mobility Cross Cluster

Extension Mobility Cross Cluster Overview

The extension mobility cross cluster (EMCC) feature provides users with the same functionality as extension mobility, but also allows them to move from one cluster (the home cluster) and log in to a temporary phone on another remote cluster (the visiting cluster). From there, they can access their phone settings from any location as if the they were using an IP phone at the home office.

Extension Mobility Cross Cluster Prerequisites

- Other call-control entities that support and use the extension mobility cross cluster (EMCC) configuration; for example, other Cisco Unified Communications Manager clusters, EMCC intercluster service profiles, and EMCC remote cluster services
- Clusters that are set to nonsecure or mixed mode. See Extension Mobility Cross Cluster and Security Mode for Different Cluster Versions, on page 24 for more information.
- Supported phones in secure or nonsecure mode

Extension Mobility Cross Cluster Configuration Task Flow

Before you begin

- Review Extension Mobility Cross Cluster Prerequisites, on page 1
- Review **Extension Mobility Cross Cluster Interaction and Restriction**

Procedure

	Command or Action	Purpose
Step 1	Generate a Phone Feature List	Generate a report to identify devices that support the extension mobility cross cluster feature.
Step 2	To Configure Extension Mobility, on page 3, perform the following subtasks: • Activate Services for Extension Mobility Cross Cluster, on page 4 • Configure the Extension Mobility Phone Service, on page 4 • Configure a Device Profile for Extension Mobility Cross Cluster, on page 5 • Enable Extension Mobility Cross Cluster for a User, on page 10 • Subscribe Devices to Extension Mobility, on page 11	Configure extension mobility to allow users to temporarily access their phone settings, such as line appearances, services, and speed dials, from other phones in one cluster. Perform this task flow on both home and remote clusters, so that users will be able to access settings from either a home or visiting cluster.
Step 3	To Configure Certificates for Extension Mobility Cross Cluster, on page 11, perform the following subtasks: • Activate the Bulk Provisioning Service, on page 12 • Configure Bulk Certificate Management and Export Certificates, on page 12 • Consolidate the Certificates, on page 13 • Import the Certificates into the Clusters, on page 14	To configure the home and remote clusters properly, you must export certificates on each cluster to the same SFTP server and SFTP directory and consolidate them on one of the participating clusters. This procedure ensures that trust is established between the two clusters.
Step 4	To Configure Extension Mobility Cross Cluster Devices and Templates, on page 14, perform the following subtasks: • Create a Common Device Configuration, on page 15 • Configure an Extension Mobility Cross Cluster Template, on page 15 • Set the Default Template, on page 16 • Add Extension Mobility Cross Cluster Devices, on page 16	
Step 5	Configure a Geolocation Filter for Extension Mobility Cross Cluster, on page 16	Configure a geolocation filter to specify criteria for device location matching, such as country, state, and city values. Geolocations are used to identify the location of a device, and the filter indicates what parts of the geolocation are significant.

	Command or Action	Purpose
Step 6	Configure Feature Parameters for Extension Mobility Cross Cluster, on page 17	Select values for the feature parameters that you configured, such as the geolocation filter.
Step 7	Configure Intercluster SIP Trunk for Extension Mobility Cross Cluster, on page 20	Configure trunks to process inbound or outbound traffic for intercluster PSTN access and RSVP agent services. You can configure one trunk for both PSTN access and RSVP agent services or one trunk for each service. You do not need more than two SIP trunks for extension mobility cross cluster.
Step 8	Configure an Intercluster Service Profile for Extension Mobility Cross Cluster, on page 20	Configure the intercluster service profile to activate extension mobility cross cluster. The profile collects all the configuration that precedes and provides a results report.
Step 9	Configure Remote Cluster Services, on page 21	Configure the remote cluster for extension mobility cross cluster. This step completes the link between the home cluster with remote (visiting) cluster.

Configure Extension Mobility

Configure extension mobility to allow users to temporarily access their phone settings, such as line appearances, services, and speed dials, from other phones in one cluster. Perform this task flow on both home and remote clusters, so that users will be able to access settings from either a home or visiting cluster.

Procedure

	Command or Action	Purpose
Step 1	Activate Services for Extension Mobility Cross Cluster, on page 4	
Step 2	Configure the Extension Mobility Phone Service, on page 4	Create the Extension Mobility phone service to which you can subscribe your users.
Step 3	Configure a Device Profile for Extension Mobility Cross Cluster, on page 5	Create a device profile to map settings onto a real device when a user logs in to Extension Mobility cross cluster.
Step 4	Enable Extension Mobility Cross Cluster for a User, on page 10	
Step 5	Subscribe Devices to Extension Mobility, on page 11	Enable Extension Mobility on devices and subscribe to the service if you have not set up an enterprise subscription for all devices.

Activate Services for Extension Mobility Cross Cluster

Procedure

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

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

Step 3 Activate the following services as needed:

a) Cisco CallManager
b) Cisco Tftp
c) Cisco Extension Mobility

Step 4 Click **Save**.

Step 5 Click **OK**.

Configure the Extension Mobility Phone Service

Create the Extension Mobility phone service to which you can subscribe your users.

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.

For example, enter a name such as Extension Mobility or EM. For Java MIDlet services, the service name must exactly match the name that is defined in the Java Application Descriptor (JAD) file.

Step 4 In the **Service URL** field, enter the service URL in the following format:

```
http://<IP Address>:8080/emapp/EMAppServlet?device=#DEVICENAME#&EMCC=#EMCC#.
```

Step 5 (Optional) If you want to create a secure URL using HTTPS, enter the secure service URL in the following format:

```
https://<IP
Address>:8443/emapp/EMAppServlet?device=#DEVICENAME#&EMCC=#EMCC#
```

Step 6 Use the default values for the **Service Category** and **Service Type** fields.

Step 7 Check the **Enable** check box.

Step 8 (Optional) Check the **Enterprise Subscription** check box to subscribe all phones and device profiles to this phone service.

Note If you check this check box when configuring the service for the first time, you will set up this IP phone service as an enterprise subscription service. All phones and device profiles in the enterprise will automatically subscribe to this IP phone service, removing the need for you to subscribe them individually.

Step 9 Click **Save**.

Configure a Device Profile for Extension Mobility Cross Cluster

Create a device profile to map settings onto a real device when a user logs in to Extension Mobility cross cluster.

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 an existing device profile, enter search criteria. Click a device profile name in the resulting list.
- Click **Add New** to add a new device profile and click **Next** to choose a device profile type. Click **Next** to choose a protocol, then click **Next**.

Step 3 Configure the fields on the **Device Profile Configuration** window. See Device Profile Fields for Extension Mobility Cross Cluster, on page 5 for more information about the fields and their configuration options.

Step 4 Click **Save**.

Step 5 Add a directory number (DN) to the new device profile.

Device Profile Fields for Extension Mobility Cross Cluster

Table 1: Device Profile Settings

Field	Description
Product Type	Displays the product type to which this device profile applies.
Device Protocol	Displays the device protocol to which this device profile applies.
Device Profile Name	Enter a unique name. This name can comprise up to 50 characters in length.
Description	Enter a description of the device profile. For text, use anything that describes this particular user device profile.
User Hold MOH Audio Source	Specifies the audio source that plays when a user initiates a hold action, choose an audio source from the User Hold MOH Audio Source drop-down list. If you do not choose an audio source, Unified Communications Manager uses the audio source that is defined in the device pool or the system default if the device pool does not specify an audio source ID. **Note** You define audio sources in the Music On Hold Audio Source Configuration window. For access, choose **Media Resources** > **Music On Hold Audio Source**.

Field	Description
User Locale	From the drop-down list, choose the locale that is associated with the phone user interface. The user locale identifies a set of detailed information, including language and font, to support users. Unified Communications Manager makes this field available only for phone models that support localization. **Note** If no user locale is specified, Unified Communications Manager uses the user locale that is associated with the device pool. If the users require information to display (on the phone) in any language other than English, verify that the locale installer is installed before configuring user locale. See the Unified Communications Manager Locale Installer documentation.
Phone Button Template	From the Phone Button Template drop-down list, choose a phone button template. **Tip** If you want to configure BLF/SpeedDials for the profile for presence monitoring, choose a phone button template that you configured for BLF/SpeedDials. After you save the configuration, the Add a New BLF SD link displays in the Association Information pane. For more information on BLF/SpeedDials, see the Feature Configuration Guide for Cisco Unified Communications Manager.
Softkey Template	From the Softkey Template drop-down list, choose the softkey template from the list that displays.
Privacy	From the Privacy drop-down list, choose On for each phone on which you want privacy. For more information, see the Feature Configuration Guide for Cisco Unified Communications Manager.
Single Button Barge	From the drop-down list, choose from the following options: • Off—This device does not allow users to use the Single Button Barge/cBarge feature. • Barge—Choosing this option allows users to press the Single Button Barge shared-line button on the phone to barge into a call using Barge. • Default—This device inherits the Single Button Barge/cBarge setting from the service parameter and device pool settings. **Note** If the server parameter and device pool settings are different, the device will inherit the setting from the service parameter setting. For more information, see the Feature Configuration Guide for Cisco Unified Communications Manager.

Field	Description
Join Across Lines	From the drop-down list, choose from the following options: • Off—This device does not allow users to use the Join Across Lines feature. • On—This device allows users to join calls across multiple lines. • Default—This device inherits the Join Across Lines setting from the service parameter and device pool settings. **Note** If the server parameter and device pool settings are different, the device will inherit the setting from the service parameter setting. For more information, see the System Configuration Guide for Cisco Unified Communications Manager.
Always Use Prime Line	From the drop-down list, choose one of the following options: • Off—When the phone is idle and receives a call on any line, the phone user answers the call from the line on which the call is received. • On—When the phone is idle (off hook) and receives a call on any line, the primary line gets chosen for the call. Calls on other lines continue to ring, and the phone user must select those other lines to answer these calls. • Default—Unified Communications Manager uses the configuration from the Always Use Prime Line service parameter, which supports the Cisco CallManager service.
Always Use Prime Line for Voice Message	From the drop-down list, choose one of the following options: • On—If the phone is idle, the primary line on the phone becomes the active line for retrieving voice messages when the phone user presses the Messages button on the phone. • Off—If the phone is idle, pressing the Messages button on the phone automatically dials the voice-messaging system from the line that has a voice message. Unified Communications Manager always selects the first line that has a voice message. If no line has a voice message, the primary line gets used when the phone user presses the Messages button. • Default—Unified Communications Manager uses the configuration from the Always Use Prime Line for Voice Message service parameter, which supports the Cisco CallManager service.

Field	Description
Ignore Presentation Indicators (internal calls only)	To configure call display restrictions and ignore any presentation restriction that is received for internal calls, check the "Ignore Presentation Indicators (internal calls only)" check box. **Tip** Use this configuration in combination with the calling line ID presentation and connected line ID presentation configuration at the translation pattern level. Together, these settings allow you to configure call display restrictions to selectively present or block calling and/or connected line display information for each call. For more information about call display restrictions, see the Feature Configuration Guide for Cisco Unified Communications Manager.
Do Not Disturb	Check this check box to enable Do Not Disturb.
DND Option	When you enable DND on the phone, this parameter allows you to specify how the DND feature handles incoming calls: • Call Reject—This option specifies that no incoming call information gets presented to the user. Depending on how you configure the DND Incoming Call Alert parameter, the phone may play a beep or display a flash notification of the call. • Ringer Off—This option turns off the ringer, but incoming call information gets presented to the device, so that the user can accept the call. • Use Common Phone Profile Setting—This option specifies that the DND Option setting from the Common Phone Profile window will get used for this device. **Note** For 7940/7960 phones that are running SCCP, you can only choose the Ringer Off option. For mobile devices and dual-mode phones, you can only choose the Call Reject option. When you activate DND Call Reject on a mobile device or dual-mode phone, no call information gets presented to the device.
DND Incoming Call Alert	When you enable the DND Ringer Off or Call Reject option, this parameter specifies how a call displays on a phone. From the drop-down list, choose one of the following options: • None—This option specifies that the DND Incoming Call Alert setting from the Common Phone Profile window will get used for this device. • Disable—This option disables both beep and flash notification of a call but for the DND Ringer Off option, incoming call information still gets displayed. For the DND Call Reject option, no call alerts display and no information gets sent to the device. • Beep Only—For an incoming call, this option causes the phone to play a beep tone only. • Flash Only—For an incoming call, this option causes the phone to display a flash alert.

Field	Description
Extension Mobility Cross Cluster CSS	From the drop-down list, choose an existing Calling Search Space (CSS) to use for this device profile for the Extension Mobility Cross Cluster feature. (To configure a new CSS or modify an existing CSS, choose **Call Routing** > **Class of Control** > **Calling Search Space** in Unified Communications Manager.) Default value specifies None. The home administrator specifies this CSS, which gets used as the device CSS that gets assigned to the phone when the user logs in to this remote phone. For more information, see the Feature Configuration Guide for Cisco Unified Communications Manager.
Module 1	You can configure one or two expansion modules for this device profile by choosing phone templates from the expansion module drop-down list in the expansion module fields. **Note** You can view a phone button list at any time by choosing the View button list link next to the phone button template fields. A separate dialog box pops up and displays the phone buttons for that particular expansion module. Choose the appropriate expansion module or None.
Module 2	Choose the appropriate expansion module or None.
MLPP Domain	If this user device profile will be used for MLPP precedence calls, choose the MLLP Domain from the drop-down list. **Note** You define MLPP domains in the MLPP Domain Configuration window. For access, choose **System** > **MLPP Domain**.
MLPP Indication	If this user device profile will be used for MLPP precedence calls, assign an MLPP Indication setting to the device profile. This setting specifies whether a device that can play precedence tones will use the capability when it places an MLPP precedence call. From the drop-down list, choose a setting to assign to this device profile from the following options: 1. Default—This device profile inherits its MLPP indication setting from the device pool of the associated device. 2. Off—This device does not handle nor process indication of an MLPP precedence call. 3. On—This device profile does handle and process indication of an MLPP precedence call. **Note** Do not configure a device profile with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.

Field	Description
MLPP Preemption	If this user device profile will be used for MLPP precedence calls, assign an MLPP Preemption setting to the device profile. This setting specifies whether a device that can preempt calls in progress will use the capability when it places an MLPP precedence call. From the drop-down list, choose a setting to assign to this device profile from the following options: 1. Default—This device profile inherits its MLPP preemption setting from the device pool of the associated device. 2. Disabled—This device does not allow preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. 3. Forceful—This device allows preemption of lower precedence calls to take place when necessary for completion of higher precedence calls. **Note** Do not configure a device profile with the following combination of settings: MLPP Indication is set to Off or Default (when default is Off) while MLPP Preemption is set to Forceful.
Login User Id	From the Login User ID drop-down list, choose a valid login user ID. **Note** If the device profile is used as a logout profile, specify the login user ID that will be associated with the phone. After the user logs out from this user device profile, the phone will automatically log in to this login user ID.

Enable Extension Mobility Cross Cluster for a User

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 and choosing an existing user from the resulting list.
- Click **Add New** to add a new user.

Step 3 In the **Extension Mobility** pane, check the **Enable Extension Mobility Cross Cluster** check box.

Step 4 Choose the device profile from the **Available Profiles** list pane in the **Extension Mobility** pane.

Step 5 Move the device profile to the **Controlled Profiles** list pane.

Step 6 Click **Save**.

Subscribe Devices to Extension Mobility

Enable Extension Mobility on devices and subscribe to the service if you have not set up an enterprise subscription for all devices.

Procedure

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

Step 2 Find the phone on which users can use Extension Mobility Cross Cluster.

Step 3 For this device, check the **Enable Extension Mobility** check box in the **Extension Information** pane.

Step 4 In the **Phone Configuration** window, choose the **Subscribe/Unsubscribe Services** option in the **Related Links** drop-down list.

Step 5 Click **Go**.

Step 6 In the popup window that opens, choose the **Extension Mobility** service in the **Select a Service** drop-down list.

Step 7 Click **Next**.

Step 8 Click **Subscribe**.

Step 9 From the popup window, click **Save**, and then close the window.

Step 10 In the **Phone Configuration** window, click **Save**.

Step 11 Click **OK** if prompted.

Configure Certificates for Extension Mobility Cross Cluster

To configure the home and remote clusters properly, you must export certificates on each cluster to the same SFTP server and SFTP directory and consolidate them on one of the participating clusters. This procedure ensures that trust is established between the two clusters.

Before you begin

Configure Extension Mobility, on page 3

Procedure

	Command or Action	Purpose
Step 1	Activate the Bulk Provisioning Service, on page 12	
Step 2	Configure Bulk Certificate Management and Export Certificates, on page 12	Configure bulk certificate management in Cisco Unified OS Administration to export the certificates from both the home and remote clusters.
Step 3	Consolidate the Certificates, on page 13	Consolidate certificates when all participating clusters have exported their certificates. This option is available only if two or more clusters exported their certificates to the SFTP server.

	Command or Action	Purpose
Step 4	Import the Certificates into the Clusters, on page 14	Import the certificates back into the home and remote (visiting) clusters.

Activate the Bulk Provisioning Service

Before you begin

Configure Extension Mobility, on page 3

Procedure

Step 1 From Cisco Unified Serviceability, choose **Tools** > **Service Activation**.
Step 2 From the **Server** drop-down list, choose the publisher node.
Step 3 Check the **Cisco Bulk Provisioning Service** check box.
Step 4 Click **Save**.
Step 5 Click **OK**.

Configure Bulk Certificate Management and Export Certificates

Configure bulk certificate management in Cisco Unified OS Administration to export the certificates from both the home and remote clusters.

This procedure creates a PKCS12 file that contains certificates for all nodes in the cluster.

Note
- Every participating cluster must export certificates to the same SFTP server and SFTP directory.
- You must export certificates on the cluster whenever the Tomcat, Tomcat-ECDSA, TFTP, or CAPF certificates are regenerated on any of the cluster nodes.

Procedure

Step 1 From Cisco Unified OS Administration, choose **Security** > **Bulk Certificate Management**.
Step 2 Configure the settings for a TFTP server that both the home and remote clusters can reach. See the online help for information about the fields and their configuration options.
Step 3 Click **Save**.
Step 4 Click **Export**.
Step 5 In the **Bulk Certificate Export** window, choose **All** for the **Certificate Type** field.
Step 6 Click **Export**.
Step 7 Click **Close**.

Note When the bulk certificate export is performed, the certificates are then uploaded to the remote cluster as follows:

- CAPF certificate gets uploaded as a CallManager-trust
- Tomcat certificate gets uploaded as a Tomcat-trust
- CallManager certificate gets uploaded as a CallManager-trust
- CallManager certificate gets uploaded as a Phone-SAST-trust
- ITLRecovery certificate gets uploaded as a PhoneSast-trust and CallManager-trust

The above steps are performed when certificates are self-signed and there is no common trust in another cluster. If there is a common trust or the same signer then the export of ALL certificates is not needed.

Consolidate the Certificates

Consolidate certificates when all participating clusters have exported their certificates. This option is available only if two or more clusters exported their certificates to the SFTP server.

This procedure consolidates all PKCS12 files in the SFTP server to form a single file.

Note If you export new certificates after consolidation, you must perform this procedure again to include the newly exported certificates.

Procedure

Step 1 From From Cisco Unified OS Administration, choose **Security** > **Bulk Certificate Management** > **Consolidate** > **Bulk Certificate Consolidate**.

Step 2 In the **Certificate Type** field, choose **All**.

Step 3 Click **Consolidate**.

Note When the bulk certificate consolidate is performed, the certificates are then uploaded to the remote cluster as follows:

- CAPF certificate gets uploaded as a CallManager-trust
- Tomcat certificate gets uploaded as a Tomcat-trust
- CallManager certificate gets uploaded as a CallManager-trust
- CallManager certificate gets uploaded as a Phone-SAST-trust
- ITLRecovery certificate gets uploaded as a PhoneSast-trust and CallManager-trust

Import the Certificates into the Clusters

Import the certificates back into the home and remote (visiting) clusters.

Note After an upgrade, these certificates are preserved. You do not need to reimport or reconsolidate certificates.

Caution After you import the certificates, the phones on the cluster will automatically restart.

Procedure

Step 1 From From Cisco Unified OS Administration, choose **Security** > **Bulk Certificate Management** > **Import** > **Bulk Certificate Import**.

Step 2 From the **Certificate Type** drop-down list, choose **All**.

Step 3 Choose **Import**.

Note When the bulk certificate import is performed, the certificates are then uploaded to the remote cluster as follows:

- CAPF certificate gets uploaded as a CallManager-trust
- Tomcat certificate gets uploaded as a Tomcat-trust
- CallManager certificate gets uploaded as a CallManager-trust
- CallManager certificate gets uploaded as a Phone-SAST-trust
- ITLRecovery certificate gets uploaded as a PhoneSast-trust and CallManager-trust

Note The following types of certificates determines phones that are restarted:

- Callmanager - ALL phones only IF TFTP service is activated on the node the certificate belongs.
- TVS - SOME phones based on Callmanager group membership.
- CAPF - ALL phones only IF CAPF is activated.

Configure Extension Mobility Cross Cluster Devices and Templates

Procedure

	Command or Action	Purpose
Step 1	Create a Common Device Configuration, on page 15	Configure a common device configuration to specify the services or features that will be associated with a particular user.

	Command or Action	Purpose
Step 2	Configure an Extension Mobility Cross Cluster Template, on page 15	Create an extension mobility cross cluster template to link the common device configuration with this feature.
Step 3	Set the Default Template, on page 16	Set the extension mobility cross cluster template that you created as the default template.
Step 4	Add Extension Mobility Cross Cluster Devices, on page 16	Insert extension mobility cross cluster device entries into your system database. Each device is identified with a unique name in the format EMCC1, EMCC2, and so on. The Bulk Administration Tool assigns device numbers by obtaining the last one used.

Create a Common Device Configuration

Configure a common device configuration to specify the services or features that will be associated with a particular user.

Procedure

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

Step 2 Perform one of the following tasks:

- Click **Find** to modify an existing common device configuration and choose a common device configuration from the resulting list.
- Click **Add New** to add a new common device configuration.

Step 3 Configure the fields on the **Common Device Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 4 Click **Save**.

Configure an Extension Mobility Cross Cluster Template

Create an extension mobility cross cluster template to link the common device configuration with this feature.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Bulk Administration** > **EMCC** > **EMCC Template**.

Step 2 Click **Add New**.

Step 3 Configure the fields on the **EMCC Template Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 4 Click **Save**.

Set the Default Template

Set the extension mobility cross cluster template that you created as the default template.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Bulk Administration** > **EMCC** > **Insert/Update EMCC**.

Step 2 Click **Update EMCC Devices**.

Step 3 From the **Default EMCC Template** drop-down list, choose the extension mobility cross cluster device template that you configured.

Step 4 Click **Run Immediately**.

Step 5 Click **Submit**.

Step 6 Verify the success of the job:

a) Choose **Bulk Administration** > **Job Scheduler**.

b) Locate the Job ID of your job.

Add Extension Mobility Cross Cluster Devices

Insert extension mobility cross cluster device entries into your system database. Each device is identified with a unique name in the format EMCC1, EMCC2, and so on. The Bulk Administration Tool assigns device numbers by obtaining the last one used.

Procedure

Step 1 From From Cisco Unified CM Administration, choose **Bulk Administration** > **EMCC** > **Insert/Update EMCC**.

Step 2 Click **Insert EMCC Devices**.

Step 3 Enter the number of devices you are adding in the **Number of EMCC Devices to be added** field.

Step 4 Click **Run Immediately** and click **Submit**.

Step 5 Refresh the window and verify that the **Number of EMCC Devices already in database** value shows the number of devices that you added.

Configure a Geolocation Filter for Extension Mobility Cross Cluster

Configure a geolocation filter to specify criteria for device location matching, such as country, state, and city values. Geolocations are used to identify the location of a device, and the filter indicates what parts of the geolocation are significant.

Procedure

Step 1 From Cisco Unified CM Administration, choose **System** > **Geolocation Filter**.

Step 2 Click **Add New**.

Step 3 Configure the fields on the **Geolocation Filter Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 4 Click **Save**.

Configure Feature Parameters for Extension Mobility Cross Cluster

Select values for the feature parameters that you configured, such as the geolocation filter.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advanced Features** > **EMCC** > **EMCC Feature Configuration**.

Step 2 Configure the fields on the **EMCC Feature Configuration** window. See Feature Parameter Fields for Extension Mobility Cross Cluster, on page 17 for more information about the fields and their configuration options.

Step 3 Click **Save**.

Feature Parameter Fields for Extension Mobility Cross Cluster

Table 2: Feature Parameter Fields for Extension Mobility Cross Cluster

EMCC Parameter	Description
Default TFTP Server for EMCC Login Device	Choose the computer name or IP address of the default TFTP server that devices logging into extension mobility cross cluster (EMCC) from a remote cluster should use.
Backup TFTP Server for EMCC Login Device	Choose the computer name or IP address of the backup TFTP server that devices logging into EMCC from a remote cluster should use.
Default Interval for Expired EMCC Device Maintenance	Specify the number of minutes that elapse between system checks for expired EMCC devices. An expired EMCC device is a device that logged in to EMCC from a remote cluster, but that, because of a WAN failure or a connectivity issue, the phone logged out of the visiting cluster. When connectivity was restored, the device logged back into the visiting cluster. During this maintenance job, the Cisco Extension Mobility service checks the Unified Communications Manager database for any expired EMCC devices and automatically logs them out. The default value is 1440 minutes. Valid values range from 10 minutes to 1440 minutes.

EMCC Parameter	Description
Enable All Remote Cluster Services When Adding A New Remote Cluster	Choose whether you want all services on a new remote cluster to be automatically enabled when you add a new cluster. Valid values are True (enable all services on the remote cluster automatically) or False (manually enable the services on the remote cluster via the Remote Cluster Configuration window in Unified Communications Manager). You can enable the services manually so that you have time to configure the EMCC feature completely before enabling the remote services. The default value is False.
CSS for PSTN Access SIP Trunk	Choose the calling search space (CSS) that the PSTN Access SIP trunk for processing EMCC calls uses. The PSTN Access SIP trunk is the SIP trunk that you configured for PSTN access in the **Intercluster Service Profile** window. Calls over this trunk are intended for and are routed to only the local PSTN that is co-located with the EMCC logged-in phone that initiates the call. Valid values are the following: • Use Trunk CSS (PSTN calls use the local route group, which can prove useful for properly routing emergency service calls) • Use phone's original device CSS (PSTN calls are routed using the configured calling search space on the remote phone, that is, the CSS that is used when the phone is not logged into EMCC). The default value is Use trunk CSS.
EMCC Geolocation Filter	Choose the geolocation filter that you have configured for use EMCC. Based on the information in the geolocation that associates with a phone that is logged in through Extension Mobility from another cluster, as well as the selected EMCC geolocation filter, Cisco Unified Communications Manager places the phone into a roaming device pool. Cisco Unified Communications Manager determines which roaming device pool to use by evaluating which device pool best matches the phone geolocation information after the EMCC geolocation filter is applied.
EMCC Region Max Audio Bit Rate	This parameter specifies the maximum audio bit rate for all EMCC calls, regardless of the region associated with the other party. The default value is 8 kbps (G.729). **Note** All participating EMCC clusters must specify the same value for the EMCC region max audio bit rate.

EMCC Parameter	Description
EMCC Region Max Video Call Bit Rate (Includes Audio)	This parameter specifies the maximum video call bit rate for all EMCC video calls, regardless of the maximum video call bit rate of the region associated with the other party. The default value is 384. Valid values range from 0 to 8128. **Note** All participating EMCC clusters must specify the same value for the EMCC region max video call bit rate.
EMCC Region Link Loss Type	This parameter specifies the link loss type between any EMCC phone and devices in any remote cluster. **Note** To allow two-way audio on EMCC calls, all participating EMCC clusters must use the same EMCC region link loss type. Based on the option that you choose, Cisco Unified Communications Manager attempts to use the optimal audio codec for the EMCC call while observing the configured EMCC region max audio bit rate. Valid values are the following: • **Lossy**—A link where some packet loss can or may occur, for example, DSL. • **Low Loss**—A link where low packet loss occurs, for example, T1. When you set this parameter to **Lossy**, Cisco Unified Communications Manager chooses the optimal codec within the limit that is set by the EMCC Region Max Audio Bit Rate, based on audio quality. Some packet loss will occur. When this parameter is set to **Low Loss**, Cisco Unified Communications Manager chooses the optimal codec within the limit that is set by the EMCC Region Max Audio Bit Rate, based on audio quality. Little or no packet loss will occur. The only difference in the audio codec preference ordering between the low loss and lossy options is that G.722 is preferred over Internet Speech Audio Codec (iSAC) when the link loss type is set as low loss, whereas iSAC is preferred over G.722 when the link loss type is set as lossy. The default value is **Low Loss**.
RSVP SIP Trunk KeepAlive Timer	Specify the number of seconds that Unified Communications Manager waits between sending or receiving KeepAlive messages or acknowledgments between two clusters over EMCC RSVP SIP trunks. An EMCC RSVP SIP trunk is a SIP trunk that has Cisco Extension Mobility Cross Cluster configured as the Trunk Service Type and that has been selected as the SIP Trunk for RSVP Agent in the Intercluster Service Profile window. When two of these intervals elapse without receipt of a KeepAlive message or an acknowledgment, Unified Communications Manager releases the RSVP resources with the remote cluster. The default value is 15 seconds. Valid values range from 1second to 600 seconds.

EMCC Parameter	Description
Default Server For Remote Cluster Update	Choose the default server name or IP address of the primary node in this local cluster that has the Cisco Extension Mobility service activated. The remote cluster accesses this node to get information about this local cluster.
Backup Server for Remote Cluster Update	Choose the default server name or IP address of the secondary node in this local cluster that has the Cisco Extension Mobility service activated. The remote cluster accesses this node when the primary node is down to retrieve information about this local cluster.
Remote Cluster Update Interval	Specify an interval, in minutes, during which the Cisco Extension Mobility service on the local node collects information about the remote EMCC cluster. Collected information includes such details as the remote cluster Unified Communications Manager version and service information. The default value is 30. Valid values range from 15 minutes to 10,080 minutes.

Configure Intercluster SIP Trunk for Extension Mobility Cross Cluster

Configure trunks to process inbound or outbound traffic for intercluster PSTN access and RSVP agent services. You can configure one trunk for both PSTN access and RSVP agent services or one trunk for each service. You do not need more than two SIP trunks for extension mobility cross cluster.

Procedure

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

Step 2 Click **Add New**.

Step 3 From the **Trunk Type** drop-down list, choose **SIP Trunk**.

Step 4 From the **Trunk Service Type** drop-down list, choose **Extension Mobility Cross Clusters**.

Step 5 Click **Next**.

Step 6 Configure the fields in the **Trunk Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 7 Click **Save**.

Configure an Intercluster Service Profile for Extension Mobility Cross Cluster

Configure the intercluster service profile to activate extension mobility cross cluster. The profile collects all the configuration that precedes and provides a results report.

Procedure

Step 1 From Cisco Unified CM Administration, choose **Advance Features** > **EMCC** > **EMCC Intercluster Service Profile**.

Step 2 Configure the fields on the **EMCC Intercluster Service Profile Configuration** window. For more information on the fields and their configuration options, see Online Help.

Step 3 If no failure messages appear in the popup window, click **Save**.

Configure Remote Cluster Services

Configure the remote cluster for extension mobility cross cluster. This step completes the link between the home cluster with remote (visiting) cluster.

Procedure

Step 1 From From Cisco Unified CM Administration, choose **Advanced Features** > **Cluster View**.

Step 2 Click **Find** to show a list of known remote clusters.

Step 3 Perform one of the following steps:

- Click the remote cluster name and verify the fields if the remote cluster that you want to configure appears.
- Click **Add New** if the remote cluster that you want to configure does not appear and configure the following fields:

  a. For the **Cluster Id** field, ensure that the ID matches the enterprise parameter value of the cluster ID of the other clusters.

  b. n the **Fully Qualified Name** field, enter the IP address of the remote cluster or a domain name that can resolve to any node on the remote cluster.

  c. Click **Save**.

Note For extension mobility cross cluster, the **TFTP** check box should always be disabled.

Extension Mobility Cross Cluster Interactions and Restrictions

- Extension Mobility Cross Cluster Restrictions, on page 22

Extension Mobility Cross Cluster Interactions

Table 3: Extension Mobility Cross Cluster Interactions

Feature	Interaction
Audio	The default maximum audio bit-rate for EMCC login device is set to 8 kbps (G.729).

Feature	Interaction
Call Admission Control (CAC)	• The home cluster is unaware of visiting cluster locations and regions. • The system cannot apply Cisco Unified Communications Manager locations and regions across the cluster boundaries. • RSVP agent-based CAC uses RSVP agents in the visiting cluster.
Call Forwarding	EMCC supports call forwarding.
Cisco Extension Mobility login and logout	User authentication takes place across clusters.
Media resources for the visiting phone	Examples include RSVP agent, TRP, music on mold (MOH), MTP, transcoder, and conference bridge. Media resources are local to the visiting phone (other than RSVP agents).
PSTN access for the visiting phone	• E911 calls are routed to the local gateways of the PSTN. • Local calls are routed to the local gateways of the PSTN. • Calls terminating to local route groups route to local gateways in the visiting cluster.
Other call features and services	Example restriction: Intercom configuration specifies configuration to a static device, so EMCC does not support the intercom feature.
Security	• Cross-cluster security is provided by default. • Cisco Unified IP Phones with secure and nonsecure phone security profiles are supported.

Extension Mobility Cross Cluster Restrictions

Table 4: Extension Mobility Cross Cluster Restrictions

Restriction	Description
Unsupported Features	• EMCC does not support the intercom feature, because intercom configuration requires a static device. • Location CAC is not supported, but RSVP-based CAC is supported.
EMCC Device Cannot Be Provisioned in More Than One Cluster	For EMCC to function properly, you cannot configure the same phone (device name) in two clusters. Otherwise, login will fail due to the duplicate device error (37). For this reason, for cluster deployed with EMCC you should disable Autoregistration on all Unified Communication Manager nodes to prevent a new device being created in the home cluster after EMCC logout.

Restriction	Description
Number of EMCC Devices	Cisco Unified Communications Manager can support a MaxPhones value of 60,000. Include EMCC in the total number of devices that are supported in the cluster by using the following calculation: Phones + (2 x EMCC devices) = MaxPhones **Note** EMCC login does not affect the number of licenses that are used in the home cluster.
Visiting Device Logout Limitations	• If the home cluster administrator disables EMCC for a user while the user is logged in with EMCC, the system does not automatically log this user out. Instead, the system does not allow future EMCC attempts by this user. The current EMCC session continues until the user logs out. • In the visiting cluster, the **Phone Configuration** window has a Log Out button for extension mobility. This button is also used by the visiting cluster administrator to log out an EMCC phone. Because the EMCC phone is not currently registered with the visiting Cisco Unified Communications Manager, this operation is like a database cleanup in the visiting cluster. The EMCC phone remains registered with the home Cisco Unified Communications Manager until the phone returns to the visiting cluster because of a reset or a logout from the home cluster.
Visiting Device Login Limitations	The extension mobility service in participating clusters performs a periodic remote cluster update. The **Remote Cluster Update Interval** feature parameter controls the update interval. The default interval is 30 minutes. If the extension mobility service on clusterA does not receive a reply from a remote cluster (such as clusterB) for this update, the Remote Cluster window for clusterA shows that the Remote Activated service is set to False for clusterB. In this case, the visiting cluster does not receive any response from the home cluster and sets the Remote Activated values for the home cluster to False. During this interval, a visiting phone may not be able to log in by using EMCC. The visiting phone receives the “Login is unavailable” error message. At this point, a login attempt to EMCC from a visiting phone can fail; the phone displays the “Login is unavailable” error message. This error occurs because the visiting cluster has not yet detected the change of the home cluster from out-of-service to in-service. Remote cluster status change is based on the value of the Remote Cluster Update Interval EMCC feature parameter and on when the visiting extension mobility service performed the last query or update. You can select **Update Remote Cluster Now** in the **Remote Cluster Service Configuration** window (**Advanced Features** > **EMCC** > **EMCC Remote Cluster**) to change Remote Activate values to True, which also allows EMCC logins. Otherwise, after the next periodic update cycle, EMCC logins by visiting phones will return to normal.

Extension Mobility Cross Cluster and Security Mode for Different Cluster Versions

Note Phone configuration files can be encrypted only if both the home cluster and visiting cluster versions are 9.x or later, and when the TFTP encryption configuration flag is enabled.

During EMCC login, if both the visiting cluster and home cluster versions are in 9.x or later, the phone will behave in various modes as shown in the following table.

Table 5: Supported Security Modes When Both Visiting Cluster and Home Cluster Are In 9.x or later Versions

Home Cluster Version	Home Cluster Mode	Visiting Cluster Version	Visiting Cluster Mode	Visiting Phone Mode	EMCC Status
9.x or later	Mixed	9.x or later	Mixed	Secure	Secure EMCC
9.x or later	Mixed	9.x or later	Mixed	Non-secure	Non-secure EMCC
9.x or later	Mixed	9.x or later	Non-secure	Non-secure	Non-secure EMCC
9.x or later	Non-secure	9.x or later	Mixed	Secure	Login fails
9.x or later	Non-secure	9.x or later	Non-secure	Non-secure	Non-secure EMCC

During EMCC login, if the visiting cluster version is 8.x and the home cluster version is 9.x or later, the phone will behave in various modes as shown in the following table.

Table 6: Supported Security Modes When Visiting Cluster Is In 8.x and Home Cluster Is In 9.x or later Version

Home Cluster Version	Home Cluster Mode	Visiting Cluster Version	Visiting Cluster Mode	Visiting Phone Mode	EMCC Status
9.x or later	Mixed	8.x	Mixed	Secure	Not supported
9.x or later	Mixed	8.x	Mixed	Non-secure	Non-secure EMCC
9.x or later	Mixed	8.x	Non-secure	Non-secure	Non-secure EMCC
9.x or later	Non-secure	8.x	Mixed	Secure	Not supported
9.x or later	Non-secure	8.x	Non-secure	Non-secure	Non-secure EMCC

During EMCC login, if the visiting cluster version is 9.x or later and the home cluster version is 8.x, the phone will behave in various modes as shown in the following table.

Table 7: Supported Security Modes When Visiting Cluster Is In 9.x or later and Home Cluster Is In 8.x Version

Home Cluster Version	Home Cluster Mode	Visiting Cluster Version	Visiting Cluster Mode	Visiting Phone Mode	EMCC Status
8.x	Mixed	9.x or later	Mixed	Secure	Login fails
8.x	Mixed	9.x or later	Mixed	Non-secure	Non-secure EMCC
8.x	Mixed	9.x or later	Non-secure	Non-secure	Non-secure EMCC
8.x	Non-secure	9.x or later	Mixed	Secure	Login fails
8.x	Non-secure	9.x or later	Non-secure	Secure	Non-secure EMCC

Extension Mobility Cross Cluster Troubleshooting

Extension Mobility Application Error Codes

Table 8: Extension Mobility Application Error Codes

Error Code	Phone Display	Quick Description	Reason
201	Please try to login again (201)	Authentication Error	If the user is an EMCC user, this error can occur if "EMCC" is not activated on the **Intercluster Service Profile** window.
202	Please try to login again (202)	Blank userid or pin	The user enters a blank user ID or PIN.
204	Login is unavailable (204)	Directory server error	The EMApp sends this error to the phone when IMS could not authenticate the user with the given PIN.
205	Login is unavailable (205) Logout is unavailable (205)	User Profile Absent	Occurs when the user profile information cannot be retrieved from the cache or the database.

Error Code	Phone Display	Quick Description	Reason
207	Login is unavailable(207) Logout is unavailable(207)	Device Name Empty	Occurs when the device or name tag is missing in the request URI. This cannot happen with real devices and can occur only if the request is sent from third-party applications.
208	Login is unavailable(208) Logout is unavailable(208)	EMService Connection Error	The visiting EMApp cannot connect to any Visiting EMService. (The service is down or not activated.) The visiting EMService cannot connect to the Home EMService (the WAN is down or certificates are not trusted.)
210	Login is unavailable(210) Logout is unavailable(210)	Init Fail-Contact Admin	An error (such as a database connection failure) occurred while initializing EMApp. The error can occur because of a failure to connect to the database during startup.
211	Login is unavailable(211) Logout is unavailable(211)	EMCC Not Activated	Occurs when the PSTN is not activated in the **Intercluster Service Profile** window of the visiting cluster.
212	Login is unavailable(212)	Cluster ID is invalid	Occurs when a remote cluster update fails by sending an incorrect cluster ID to the remote cluster.
213	Login is unavailable(213) Logout is unavailable(213)	Device does not support EMCC	Occurs when a device does not support EMCC.

Extension Mobility Service Error Codes

Table 9: Extension Mobility Service Error Codes

Error Code	Phone Display	Quick Description	Reason
0	Login is unavailable(0) Logout is unavailable(0)	Unknown Error	The EMService failed for an unknown reason.
1	Login is unavailable(1) Logout is unavailable(1)	Error on parsing	When the EMService cannot parse the XML request from the EMApp or EMService. This error occurs when third-party applications send an incorrect query to login XML (EM API). The error can also occur because of a version mismatch between home and visiting clusters.
2	Login is unavailable(2)	EMCC Authentication Error	The EMCC user credentials cannot be authenticated because the user entered an incorrect PIN.
3	Login is unavailable(3) Logout is unavailable(3)	Invalid App User	Invalid application user. This error commonly occurs because of the EM API.
4	Login is unavailable(4) Logout is unavailable(4)	Policy Validation error	The EM Service sends this error when it cannot validate the login or logout request because of an unknown reason, an error while querying the database or an error while retrieving information from the cache.
5	Login is unavailable(5) Logout is unavailable(5)	Dev. logon disabled	A user logs into a device that has **Enable Extension Mobility** unchecked in the **Phone Configuration** window.

Error Code	Phone Display	Quick Description	Reason
6	Login is unavailable(6) Logout is unavailable(6)	Database Error	Whenever the database returns an exception while executing the query or stored procedure that the EM Service requests (login/logout or device/user query), the EM Service sends this error code to EMApp.
8	Login is unavailable(8) Logout is unavailable(8)	Query type undetermined	No valid query was sent to the EMService (DeviceUserQuery and UserDeviceQuery are valid ones). This error occurs because of the EM API or incorrect XML input.
9	Login is unavailable(9) Logout is unavailable(9)	Dir. User Info Error	This error appears in two cases: **1.** IMS returns an exception when it attempts to authenticate a user. **2.** When information about a user cannot be retrieved either from the cache or database.
10	Login is unavailable(10) Logout is unavailable(10)	User lacks app proxy rights	The user tries to log in on behalf of another user. By default, a CCMSysUser has administrative rights.
11	Login is unavailable(11) Logout is unavailable(11)	Device Does not exist	The phone record entry is absent in the device table.
12	Phone record entry is absent in the device table	Dev. Profile not found	No device profile is associated with the remote user.
18	Login is unavailable(18)	Another user logged in	Another user is already logged in on the phone.

Error Code	Phone Display	Quick Description	Reason
19	Logout is unavailable(19)	No user logged in	The system attempted to log out a user who has not logged in. This error occurs when sending logout requests from third-party applications (EM API).
20	Login is unavailable(20) Logout is unavailable(20)	Hoteling flag error	**Enable Extension Mobility** is unchecked in the **Phone Configuration** window.
21	Login is unavailable(21) Logout is unavailable(21)	Hoteling Status error	The current user status was not retrieved from either the local cache or database.
22	Login is unavailable(22)	Dev. logon disabled	Occurs when EM is not enabled on device and the request is sent via EM API or when the services button is pressed on phone.
23	Login is Unavailable (23) Logout is Unavailable (23)	User does not exist	Occurs when the given user ID is not found (in any of the remote clusters).
25	Login is unavailable(25)	User logged in elsewhere	The user is currently logged in to some other phone.
26	Login is unavailable(26) Logout is unavailable(26)	Busy, please try again	Occurs when the EMService has currently reached the threshold level of Maximum Concurrent Requests service parameter.

Error Code	Phone Display	Quick Description	Reason
28	Login is unavailable(28) Logout is unavailable(28)	Untrusted IP Error	Occurs when the Validate IP Address service parameter is set to **True** and the user tries to log in or log out from a machine whose IP address is not trusted. For example, a third-party application or EM API from a machine is not listed in the Trusted List of Ips service parameter.
29	Login is unavailable(29) Logout is unavailable(29)	ris down-contact admin	The Real-Time Information Server Data Collector (RISDC) cache is not created or initialized, and the EMService is unable to connect to RISDC.
30	Login is unavailable(30) Logout is unavailable(30)	Proxy not allowed	When login and logout occur through proxy ("Via" is set in HTTP header) and the Allow Proxy service parameter is set to **False**.
31	Login is unavailable(31) Logout is unavailable(31)	EMCC Not Activated for the user	Occurs when the **Enable Extension Mobility Cross Cluster** check box is not checked in the **End User Configuration** window of the home cluster.
32	Login is unavailable(32) Logout is unavailable(32)	Device does not support EMCC	Occurs when a device model does not have EMCC capability.
33	Login is unavailable(33) Logout is unavailable(33)	No free EMCC dummy device	Occurs when all the EMCC dummy devices are in use by other EMCC logins.
35	Login is unavailable(35) Logout is unavailable(35)	Visiting Cluster Information is not present in Home Cluster	Occurs when the home cluster does not have an entry for this visiting cluster.

Error Code	Phone Display	Quick Description	Reason
36	Login is unavailable(36) Logout is unavailable(36)	No Remote Cluster	Occurs when the administrator has not added a remote cluster.
37	Login is Unavailable (37) Logout is Unavailable (37)	Duplicate Device Name	Occurs when the same device name exists in both the home cluster and visiting cluster.
38	Login is unavailable(38) Logout is unavailable(38)	EMCC Not Allowed	Occurs when the home cluster does not want to allow EMCC login (The **Enable Extension Mobility Cross Cluster** check box is not checked in the home cluster).
39	Please try to login again (201)	Configuration Issue	Occurs when the **Default TFTP Server** and **Backup TFTP Server** for EMCC login device are not set properly in EMCC Feature Configuration Page. **Note** This is internal error code.
40	Please try to login again (23)	No Response from Remote Host	Occurs when response not getting from Remote Host. **Note** This is internal error code.
41	PIN change is required	PIN change is required	Occurs when admin enables **User Must Change at Next Login** for PIN. In that case user is redirected to Change credentials page. **Note** This is internal error code.
42	Login is unavailable(42) Logout is unavailable(42)	Invalid ClusterID	Occurs when the remote cluster ID is not valid. This error can occur during a remote cluster update.

Error Code	Phone Display	Quick Description	Reason
43	Login is unavailable(43)	Device Security mode error	The Device Security Profile that is associated to the EMCC device should be set to Nonsecure for its Device Security Mode.
44	Please try to login again (201)	Configuration Issue	Occurs when the cluster ID is not valid. **Note** This is internal error code.
45	Login is unsuccessful(45)	Remote Cluster version not supported	Occurs during EMCC login when the visiting cluster version is 9.x and is in mixed mode, the phone is in secure mode, and the home cluster version is 8.x.
46	Login is unsuccessful(46)	Remote Cluster security mode not supported	Occurs during EMCC login when the visiting cluster security mode is in mixed mode, the phone is in secure mode, and the home cluster is in nonsecure mode.