Cisco Intercompany Media Engine configuration

Cisco Intercompany Media Engine (Cisco IME) allows customers to establish direct IP connectivity between enterprises. After you install the software on the Cisco IME server and perform the post-installation tasks, you must configure the Cisco Unified Communications Manager server to enable the Cisco Intercompany Media Engine feature.

This chapter contains information on using the Cisco Unified Communications Manager Administration user interface and provides detailed steps on configuring the Cisco Unified Communications Manager server for the Cisco Intercompany Media Engine feature.

- Cisco Unified Communications Manager Administration basics, page 1
- Set up Cisco IME, page 5
- Set up Cisco IME security and server connection, page 6
- Set up IME Enrolled and Exclusion numbers, page 15
- Set up IME Trust Groups and Elements, page 19
- Intercompany media service configuration settings, page 21
- CUCM external address list configuration settings, page 24
- Set up IME Transformation Patterns and Profiles, page 25
- Set up PSTN access trunks, page 32
- Set up IME feature configurations, page 33
- Server communication, page 37
- Set up fallback information, page 39
- Set up off-path settings, page 46

Cisco Unified Communications Manager Administration basics

You use Cisco Unified Communications Manager Administration, a web-based application, to perform configuration tasks for Cisco Unified Communications Manager servers. This section describes basic elements of the graphical user interface, including the navigation menus and the documentation search feature that allows you to search Cisco Unified Communications Manager documentation on Cisco.com.
Graphical user interface options

The Cisco Unified Communications Manager Administration interface contains the following options.

Note
For information on logging into Cisco Unified Communications Manager Administration, refer to the Cisco Unified Communications Manager Administration Guide.

• Navigation - After you log on, the main Cisco Unified Communications Manager Administration window redisplays. The window includes the drop-down list box in the upper, right corner called Navigation. To access the applications in the drop-down list box, choose the program that you want and click Go. The choices in the drop-down list box include the following Cisco Unified Communications Manager applications:

  ◦ Cisco Unified Communications Manager Administration - Shows as default when you access Cisco Unified Communications Manager. Use Cisco Unified Communications Manager Administration to configure system parameters, route plans, devices, and much more.

  ◦ Cisco Unified Serviceability - Takes you to the main Cisco Unified Serviceability window. Use Cisco Unified Serviceability to configure trace files and alarms and to activate and deactivate services.

  ◦ Cisco Unified OS Administration - Takes you to the main Cisco Unified Operating System Administration window, so you can configure and administer the Cisco Unified Communications Manager platform. You must log off from any other application before you can log in to this application.

  ◦ Disaster Recovery System - Takes you to the Cisco Disaster Recovery System, a program that provides full data backup and restore capabilities for all servers in a Cisco Unified Communications Manager cluster. You must log off from any other application before you can log in to this application.

• Search Documentation - Click this link to search Cisco Unified Communications Manager documentation on Cisco.com for the current release. The Cisco Unified CM Documentation Search window displays. Type the word or words for which you want to search and click the Search button. The search results display. You can narrow the search results by choosing a documentation type modifier button that displays above your search result; for example, Unified CM Install/Upgrade or Unified CM Business Edition Release Notes.

• About - Displays the Cisco Unified Communications Manager Administration main window and allows you to view the system software version.

• Logout - Allows you to log out of Cisco Unified Communications Manager Administration application. The window redisplays with the login fields.

• Menu Bar - The horizontal bar located across the top of the interface contains the names of the menus. Click the menu options to display the Cisco Unified Communications Manager Administration windows. Menu items in this document appear in boldface font. A > (greater than) symbol separates menu item selections. In the browser, this indicates a menu item selection; for example: Choose Advanced Features > Intercompany Media Services > Service.
Related Topics

Cisco Unified Communications Manager Administration basics, on page 1

Administration help options

To access Help, click the Help menu in the Cisco Unified Communications Manager Administration navigation bar, and choose one of the following options:

- **Contents** - Opens a new browser window and displays the home page for the Cisco Unified Communications Manager Administration Help system. The links in the left pane of the Help window allow you to access all topics in the Help system.

- **This Page** - Opens a new browser window for the Cisco Unified Communications Manager Administration Help system. The right pane of the window contains definitions for each field in the current window in Cisco Unified Communications Manager Administration. In most cases, cross-references point to additional topics that relate to the current window.

- **About** - Displays the Cisco Unified Communications Manager Administration main window and allows you to view the system software version.

The left pane of the Help system provides a table of contents for all of the product guides that the Help system includes. The table of contents expands to show the location within the hierarchy of the Help topic that displays on the right.

To learn more about the Cisco Unified Communications Manager Administration system, including instructions on how to search Help, click the **Using Help** link at the top of any Help window.

Related Topics

Cisco Unified Communications Manager Administration basics, on page 1

Find and delete records

You can search for all records or enter search criteria to narrow your search. The search parameters vary, depending on the records for which you are searching. For example, when searching for a phone, you can search for phones with certain digits in the directory number or certain characters in the device name. When searching for an end user, you can search for first or last names that contain certain letters.

Once you have found records, you can delete them from the **Find and List** window that contains your records. You can delete individual records or delete all records that display in the window.

Use the following procedure to find and delete records from Cisco Unified Communications Manager Administration.

**Procedure**

**Step 1** Navigate to the **Find and List** window in Cisco Unified Communications Manager Administration for the component that you want to find. For example, if you want to find a phone, choose **Device > Phone** to display the **Find and List Phones** window.

**Step 2** To find all records in the database, ensure the dialog box is empty; go to Step 3.

**Step 3** To filter or search records
Add and copy records

Complete the following steps to add and copy records:

Procedure

Step 1 Navigate to the Find and List window in Cisco Unified Communications Manager Administration for the component that you want to add (or copy). For example, if you want to add a trust element, select Advanced Services > Intercompany Media Services > Trust Element to display the Find and List Trust Elements window.

Step 2 To add a new record, click the Add New button.
The window refreshes with a new record. Make the necessary changes, and click Save.

Step 3 To copy an existing record, do one of the following:
  • In the Find and List window, click the Copy button.
  • Locate the record that you want to copy, as described in Find and delete records, on page 3. Choose the record, and click the Copy button in the configuration window. For example, find the trust element record that you want to copy, and click the Copy button in the Trust Element Configuration window.
Step 4  To copy an existing record and populate a new record with all of the associated information from the existing record:
   a) In the Find and List window, click the **Super Copy** button.
   b) Locate the record that you want to copy, as described in Find and delete records, on page 3. Choose the record, and click the **Super Copy** button in the configuration window. For example, find the phone record that you want to copy, and click the **Super Copy** button in the Phone Configuration window.

The window refreshes with a new Device Name field. Make the necessary changes, and click **Save**.

---

**Related Topics**

Cisco Unified Communications Manager Administration basics, on page 1

---

**Set up Cisco IME**

**Before You Begin**

Before you begin, make sure that you have installed the Cisco Intercompany Media Engine software on the server and performed the post-installation tasks, including uploading the license file and enrolling the certificates. See the Cisco IME server installation and configuration.

**Procedure**

1. **Step 1** Set up the Cisco IME security and server connection to the Cisco Unified Communications Manager Administration.
   For more information, see Set up Cisco IME security and server connection, on page 6.
2. **Step 2** Set up IME Enrolled and Exclusion numbers.
   For more information, see Set up IME Enrolled and Exclusion numbers, on page 15.
3. **Step 3** Set up IME Trust Groups and Elements.
   For more information, see Set up IME Trust Groups and Elements, on page 19.
4. **Step 4** Set up the Cisco IME service.
   For more information, see Intercompany media service configuration settings, on page 21.
5. **Step 5** Define external IP addresses and ports for each Cisco Unified Communications Manager in the cluster.
   For more information, see CUCM external address list configuration settings, on page 24.
6. **Step 6** Set up IME Transformation Patterns and Profiles.
   For more information, see Set up IME Transformation Patterns and Profiles, on page 25.
7. **Step 7** Configure trunks to enable them to send VCRs to the Cisco IME server.
   For more information, see Set up PSTN access trunks, on page 32.
8. **Step 8** Set up IME feature configurations.
   For more information, see Set up IME feature configurations, on page 33.
9. **Step 9** Verify the VAP connectivity between the Cisco IME server and the Cisco Unified Communications Manager server.
Set up Cisco IME security and server connection

Complete the following tasks to set up the Cisco IME system security and connection to the Cisco Unified Communications Manager Administration:

**Procedure**

**Step 1** Check that the appropriate adaptive security appliance (ASA) license is installed. For information, refer to the Cisco Unified Communications Manager Software Compatibility Matrix at [http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html](http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html).

**Step 2** Set the Retry Count for SIP Invite service parameter to a small value. For more information, see **Set SIP Invite service retry count**, on page 7.

**Step 3** Create an application user in the Cisco Unified Communications Manager Administration. For more information, see **Create Cisco Unified Communications Manager Administration user**, on page 7.

**Step 4** Check that the SIP security profile specifies the correct SIP listening port and the security mode. For more information, see **Check SIP listening port and security mode**, on page 8.

**Step 5** Set up a SIP trunk to use with Cisco Intercompany Media Engine. For more information, see **Set up SIP trunk**, on page 8.

**Step 6** Set the Cisco CallManager service parameter. For more information, see **Set the Cisco CallManager service parameter**, on page 9.

**Step 7** Specify information about the Cisco IME server to which Cisco Unified Communications Manager connects, including the IP address and the port that VAP communications use. For more information, see **Cisco IME server connection configuration**, on page 9.

**Step 8** If you choose the Encrypted and Authenticated security mode for the IME server, you must set up a TLS connection using third-party certificates or self-signed certificates. For more information, see **Cisco Unified Communications Manager and Cisco Intercompany Media Engine servers TLS connections**, on page 11.

**What to Do Next**

Set up IME Enrolled and Exclusion numbers. For more information, see **Set up IME Enrolled and Exclusion numbers**, on page 15.
Set SIP Invite service retry count

Cisco Systems recommends setting the parameter to a value of 2.

To determine whether you have UDP trunks, check the transport type of the SIP security profile (System > Security > SIP Trunk Security Profile.)

If you keep the default value of 6 and an ASA outage occurs, Cisco Unified Communications Manager takes up to a minute to revert a Cisco IME call to the PSTN.

Note

The Retry Count for SIP Invite service parameter applies to all SIP trunks that you configure on the Cisco Unified Communications Manager server.

Procedure

Step 1
Choose System > Service Parameters.

Step 2
Select the appropriate server from the Server drop-down list box.

Step 3
Select the Cisco CallManager service from the Service drop-down list box.

Step 4
Enter a Retry Count for SIP Invite service parameter value.

Step 5
Click Save.

Create Cisco Unified Communications Manager Administration user

Cisco Unified Communications Manager obtains the IP address and port of the Cisco IME server and checks the application user name and password configuration for that server. Cisco Unified Communications Manager also checks the security setting and the application user information for the Cisco IME service.

Cisco Unified Communications Manager initiates a connection to the Cisco IME server over TCP. If the security mode specifies encrypted, a TLS connection gets established. That TLS connection uses the self-signed certificate that is created for Cisco Unified Communications Manager upon installation.

The certificate for the Cisco IME server must exist in the trust store on the Cisco Unified Communications Manager server.

The Cisco Unified Communications Manager node accepts any certificate from the Cisco IME server that exists in the trust store. Once the connection gets established, Cisco Unified Communications Manager sends a Register message that contains the user ID and password that associate with the application user for the Cisco IME service. The Cisco IME server checks the credentials against its configured username and password.

Procedure

Step 1
From Cisco Unified Communications Manager Administration, click User Management > Application User > Add New.

Step 2
In the User ID and Password fields, enter the VAP username and password values that you set up on the Cisco IME server.
User ID and passwords are set up using the `add vapusercredentials` CLI command.

Leave the other fields in the Application User Configuration window set to the default values.

If the username and password values that you enter in the Application User Configuration window do not match those of the VAP username and password on the Cisco IME server, the Cisco Unified Communications Manager server cannot register with the Cisco IME server.

**Step 3** Click Save.

---

### Check SIP listening port and security mode

Complete the following steps to check the SIP listing port and security mode:

**Procedure**

**Step 1** Click System > Security > SIP Trunk Security Profile.

**Step 2** Ensure that the value that is selected from Device Security Mode drop-down list box enables you to connect to the ASA.

The value must match what you have configured on the ASA.

**Step 3** Ensure that the Incoming Port field contains the correct value of the port that Cisco Unified Communications Manager uses to communicate with the ASA.

By default, Cisco Unified Communications Manager uses port 5060. If you are using a non-default port, you need to enter that port here.

**Step 4** Select the Accept Out-of-Dialo REFER check box.

**Step 5** In the SIP Trunk Security Profile Configuration window select choose the corresponding check boxes to allow the Cisco IME trunk to accept unsolicited notification, replaces header, presence subscription, and to transmit security status.

---

### Set up SIP trunk

IME SIP trunks do not support IPv6, so ensure that the IME trunk specifies IPv4 only. If you do not have IPv6 enabled on your system, this issue does not apply.

For more information on configuring trunks, refer to the Cisco Unified Communications Manager Administration Guide.
**Procedure**

**Step 1** Click Device > Trunk > Add New.

**Step 2** From the Trunk Type drop down list box, select SIP Trunk.

**Step 3** From the Trunk Service Type drop-down list box, select Cisco Intercompany Media Engine.

**Step 4** Configure the trunk by following these considerations:

- For Cisco IME calls, the incoming calling and called numbers always specify an +E.164 number format; that is, globalized numbers preceded by “+”. Based on the Cisco Unified Communications Manager dial plan and the routing architecture, you may also need to define calling and called party number transformations or translation patterns to allow the called number to route within Cisco Unified Communications Manager. Otherwise, incoming Cisco IME calls will fail with a digit analysis error. For example, you may need to remove a leading “+” from the calling party number at the gateway level to allow the call to get routed in Cisco Unified Communications Manager.

- To configure the necessary transformations, configure the fields in the Inbound Calls group box.

**Step 5** Restart the trunk.

---

**Set the Cisco CallManager service parameter**

**Procedure**

**Step 1** Click System > Service Parameters.

**Step 2** From the Server drop-down list box, select a server.

**Step 3** From the Service drop-down list box, select the Cisco CallManager service.

**Step 4** Set the Duplex Streaming Enabled parameter to True.

---

**Cisco IME server connection configuration**

Use the Intercompany Media Engine Server Connection Configuration window to specify information about the Cisco Intercompany Media Engine (Cisco IME) server to which Cisco Unified Communications Manager connects. The information that you provide enables Cisco Unified Communications Manager to connect to the Cisco IME server to initiate VAP messaging. The interface between servers allows Cisco Unified Communications Manager to publish its configured direct inward dialing (DID) patterns and to learn new routes.

After Cisco Unified Communications Manager establishes a connection, Cisco Unified Communications Manager sends a VAP Register message to the Cisco IME server. This message contains the username that associates with the application user that the Application User field specifies. The Cisco IME server checks the credentials against the configured VAP username and password that you configured in the Perform
post-installation configurations. If the values do not match, validation does not occur and the Cisco IME server cannot communicate with the Cisco Unified Communications Manager server.

---

**Note**

Cisco recommends that you install the Cisco IME server and ensure that the server is functional before configuring the Cisco IME server in Cisco Unified Communications Manager Administration.

If you configure the Cisco IME server in Cisco Unified Communications Manager Administration, make sure to deactivate the Cisco Intercompany Media Engine service in the **Intercompany Media Service Configuration** window (Advanced Features > Intercompany Media Services > Service) until the Cisco Intercompany Media Engine servers become available.

If the Cisco IME servers are not available when you configure Cisco Unified Communications Manager Administration, Cisco Unified Communications Manager continues to attempt to connect to the Cisco Intercompany Media Engine server based on the reconnect interval that you configure for the Cisco Intercompany Media Engine service.

To access the **Intercompany Media Engine Server Connection Configuration** window, click Advanced Features > Intercompany Media Services > Server Connections.

**Using the GUI**

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the Cisco Unified Communications Manager Administration basics, on page 1 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

**Configuration Settings Table**

The following table describes the Cisco IME server configuration settings.

**Table 1: Cisco IME server configuration settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server information</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Name of the Cisco IME server, up to 50 characters. Specify a name that is unique in the cluster. Valid values include alphanumeric (a-z, A-Z, 0-9), period (.), dash (-), underscore (_), space ().</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a descriptive name of the Cisco IME server. The description can comprise up to 128 characters. (Optional)</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the Cisco IME server to which Cisco Unified Communications Manager connects. You must enter an IPv4 address.</td>
</tr>
<tr>
<td>Port</td>
<td>Specify the port that the Cisco Unified Communications Manager server uses for Validation Access Protocol (VAP) communications to the Cisco IME server. The default specifies 5620. Valid values range from 0 to 65535. The port number that you enter must match the port number that you configured on the Cisco IME server.</td>
</tr>
</tbody>
</table>
### Authentication information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application User</td>
<td>Choose the application user that you configured when you created an application user in the Cisco Unified Communications Manager Administration. The application user ID must match the vapusername that you configured in the post-installation tasks.</td>
</tr>
</tbody>
</table>
| Server Security Mode         | Choose the appropriate security mode for communications between the Cisco Unified Communications Manager server and the Cisco IME server, either Authenticated or Encrypted and Authenticated. The security mode that you choose must match the security mode that you configured on the Cisco Intercompany Media Engine server, as described in the post-installation tasks.  

The Authenticated mode uses a digest-based authentication between the servers but does not encrypt the data. The Encrypted and Authenticated mode uses digest authentication that must run over a TLS connection between the Cisco Unified Communications Manager server and the Cisco IME server. If you choose Encrypted and Authenticated, you must upload the Cisco Intercompany Media Engine certificate into the Cisco Unified Communications Manager trust store by using the Cisco Unified Communications Operating System (Security > Certificate Management). The default specifies Authenticated. Cisco strongly recommends that you choose the Encrypted and Authenticated mode.

**Note** If you change the server security mode, the Cisco Unified Communications Manager closes the connections to the Cisco IME server.

| Server Reconnect/VAP Retry Interval | Indicate the frequency (in seconds) with which you want the Cisco Unified Communications Manager server to try to connect to the Cisco IME server after losing connectivity. The Cisco Unified Communications Manager server tries to connect to the Cisco IME server indefinitely at this interval. Valid values include 60 through 600 seconds. The default specifies 120 seconds. |

### Related Topics

- Set up Cisco IME, on page 5

### Cisco Unified Communications Manager and Cisco Intercompany Media Engine servers TLS connections

You can set up TLS connections between the Cisco Unified Communications Manager and Cisco Intercompany Media Engine (Cisco IME) servers using self-signed certificates or third-party certificates.
Generate self-signed certificate

Use this procedure to generate the self-signed certificates.

Procedure

Step 1 Open the generated self-signed certificate file on your PC using a text editor, and copy the contents of the file from BEGIN CERTIFICATE to END CERTIFICATE.

Step 2 Log into the Cisco IME CLI and enter the set cert import trust IME command.

Step 3 Paste the previously copied certificate.

Step 4 Enter the following CLI command to check that the authentication mode on the Cisco IME is encrypted:

Example:
ime vapserver vapservername
The vapservername value must be name of the VAP server instance that you created on the Cisco IME server.

Step 5 Check that the Server Security Mode value for the corresponding Cisco IME Server is set to Encrypted and Authenticated.
To access these values, navigate to the Server Connections option on the Intercompany Media Engine Server Connection Configuration window.

Step 6 Click Security > Certificate > Find to find the certificate on the Cisco Unified Communications Manager server.

Step 7 Choose the CallManager.pem certificate.

Step 8 In the Cisco IME CLI, locate the Cisco IME trust name by entering the show cert list trust command, and then enter the show cert trust name command.

Step 9 Compare the certificate content from the Cisco Unified Communications Manager server and the Cisco IME server and make sure that they match.

Note You must repeat this procedure for each Cisco Unified Communications Manager server that connects to the Cisco IME server.

Related Topics
Set up Cisco IME, on page 5
Upload self-signed certificate to IME server, on page 12

Upload self-signed certificate to IME server

Use this procedure to upload the self-signed certificates.
**Procedure**

**Step 1**  
On the Cisco IME server, log into the Cisco IME command line interface (CLI) and enter the `show cert own` IME command.

**Step 2**  
Copy the contents of the certificate from **BEGIN CERTIFICATE** to **END CERTIFICATE**, and paste it to a file named `IME_Cert.pem` that you store on your PC.

**Step 3**  
On the Cisco Unified Communications Manager server, login to Cisco Unified Communications Operating System, and click **Security > Certificate Management**.

**Step 4**  
Click **Upload Certificate**.

**Step 5**  
Choose **CallManager-trust** from the **Certificate Name** drop down list.

**Step 6**  
Choose the file to upload by doing one of the following steps:

- In the **Upload File** text box, enter the path to the file.
- Click the **Browse** button and navigate to the file; then, click **Open**.

**Step 7**  
Click **Upload File** to upload the file to the Cisco Unified Communications Manager server.

**Step 8**  
Click **Security > Certificate > Find** to find the certificate on the Cisco Unified Communications Manager server.

**Step 9**  
Choose the **CallManager.pem** certificate.

The description of this certificate indicates that it is a self-signed certificate generated by the system.

**Step 10**  
Click **Download** to save the file to your PC.

---

**What to Do Next**

Generate self-signed certificate, on page 12

---

**Generate third party certificate**

Use this procedure to generate the Certificate Signing Requests (CSRs) for the third party certificates.

**Procedure**

**Step 1**  
In the Cisco IME command line interface (CLI), enter the `set csr gen` IME command and then the `show csr own` IME command to generate the CSR.

**Step 2**  
Copy the CSR to the third party certificate agent (CA).

**Step 3**  
Obtain and download the signed application certificate for Cisco IME and the root certificate from the CA.

**Step 4**  
In the Cisco IME CLI, enter the `set cert import trust` IME command to import the root certification. Make note of the newly generated Cisco IME trust.

**Step 5**  
Enter the `set cert import own` IME CA Cert command to import the signed application certification to the Cisco IME.

**Step 6**  
Enter the `show ime vapserver vapservername` command to check that the authentication mode value on the Cisco IME is set to encrypted.
The vapservername is the name of the VAP server instance that you created on the Cisco IME server. If you need to change the authentication mode, enter the `set ime vapserver authenticationmode vapservername` encrypted command.

**Step 7**  
On the Cisco Unified Communications Manager server, login to Cisco Unified Communications Operating System, and click **Security > Certificate Management.**

**Step 8**  
Generate and download a CallManager CSR, as described in the *Cisco Unified Communications Operating System Administration Guide.*  
Make sure to choose CallManager from the Certificate Name drop-down list box.

---

**What to Do Next**

Upload third party certificate to IME server,  on page 14

**Related Topics**

Set up Cisco IME,  on page 5

---

### Upload third party certificate to IME server

Use this procedure to upload the certificates to the Cisco Unified Communications Manager and Cisco IME servers.

**Procedure**

**Step 1**  
Obtain and download the third party signed application certificate and the root certificate from the certificate agent (CA) using the generated CSR.

**Step 2**  
On the Cisco Unified Communications Manager server, login to Cisco Unified Communications Operating System, and click **Security > Certificate Management.**

**Step 3**  
Upload the CallManager-Trustroot and the CallManager signed certificates.

**Step 4**  
Check that the **Server Security Mode** value for the corresponding Cisco IME Server is set to **Encrypted** and **Authenticated.**  
To access these values, navigate to the Server Connections option on the **Intercompany Media Engine Server Connection Configuration** window.

**Step 5**  
In the Cisco Unified Communications Operating System, click **Security > Certificate Management.**

**Step 6**  
Find and display the CallManager root certificate that you uploaded.

**Step 7**  
Log into the Cisco IME server CLI, and use the `show cert trust list` command to obtain the name of the root certificate.

**Step 8**  
Compare the certificate content from the Cisco Unified Communications Manager server and the Cisco IME server and make sure that they match.  
**Note**  
You must repeat this procedure for each Cisco Unified Communications Manager server that connects to the Cisco IME server.

---

**Related Topics**

Set up Cisco IME,  on page 5
Set up IME Enrolled and Exclusion numbers

Complete the following tasks to set up Cisco IME Enrolled and Exclusion numbers:

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Create the enrolled groups to which you can assign enrolled patterns. For more information, see Enrolled group configuration settings, on page 15.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Specify the set of +E.164 numbers that you will allow to make and receive Cisco IME calls by creating enrolled patterns. For more information, see Enrolled pattern configuration settings, on page 16.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Create an exclusion group to associate to numbers are prevented from using Cisco IME. For more information, see Exclusion group configuration settings, on page 18.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Specify numbers that are prevented from using Cisco IME, including numbers of analog devices and fax machines. For more information, see Exclusion number configuration settings, on page 18.</td>
</tr>
</tbody>
</table>

What to Do Next

Set up IME Trust Groups and Elements. For more information, see Set up IME Trust Groups and Elements, on page 19.

Enrolled group configuration settings

Cisco IME publishes these numbers to the IME distributed cache. By doing so, Cisco IME makes these numbers available for other enterprises to learn through Cisco IME. Numbers within your enterprise must also match a pattern in an enrolled group in order to make Cisco IME calls. You can create an enrolled group for each of your campuses or sites to facilitate incremental deployment of Cisco IME, starting with certain sites or campuses and extending the deployment as usage grows.

After you create the enrolled group, you create the enrolled patterns, assign the patterns to a group, and associate the group with a Cisco IME service. If you want to disable Cisco IME for certain phones in the enterprise, you can unassign the enrolled group for those phones from the Cisco IME service.

To access the IME Enrolled Group Configuration window, click Advanced Features > Intercompany Media Services > IME Enrolled Group.

GUI use

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the Cisco Unified Communications Manager Administration basics, on page 1 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.
**Configuration settings table**

The following table describes the Cisco IME enrolled group configuration settings.

**Table 2: Cisco Intercompany Media Engine enrolled group configuration settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Enter a unique name for the enrolled group. The name must be at least one character and can include up to 32 characters.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the enrolled group. The description can include up to 128 characters. (Optional)</td>
</tr>
<tr>
<td>Fallback Profile</td>
<td>Choose the fallback profile that you want to associate to this enrolled group.</td>
</tr>
<tr>
<td></td>
<td>The fallback profile defines how Cisco Unified Communications Manager handles fallback to the PSTN for numbers that are associated with this enrolled group.</td>
</tr>
<tr>
<td></td>
<td>If you choose None, calls to direct inward dialing numbers (DIDs) in this pattern group do not fallback to the PSTN.</td>
</tr>
<tr>
<td></td>
<td>Configure fallback profiles in the Fallback Profile Configuration window. For more information, see the Fallback profile configuration settings, on page 40.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If you are setting up Cisco IME for the first time, Cisco Systems recommends that you complete the rest of the Cisco Unified Communications Manager Administration configuration before you choose a fallback profile from this field.</td>
</tr>
<tr>
<td>All Patterns in Group Are Aliases</td>
<td>Check this check box if all of the patterns within the group need to be aliases to each other. For example, check this check box if you have 18xx numbers for which you enrolled the +E.164 numbers, but the service provider performs mapping from the 18xx number and provides the DID as the called party number for the 18xx instead.</td>
</tr>
<tr>
<td></td>
<td>Check this check box only if the patterns specify exact aliases to other patterns in the same group. Only exact patterns can be aliases; no wild cards are allowed.</td>
</tr>
</tbody>
</table>

**Related Topics**

Set up Cisco IME, on page 5

**Enrolled pattern configuration settings**

To eliminate the need for day-to-day provisioning of specific numbers as individual phones are added to and removed from the system, you can add a pattern that represents a large group of numbers for a given site. The enrolled pattern can include numbers that you have not assigned to a phone. Numbers that are not associated to a phone cannot be validated.
After you create enrolled patterns, you associate them to an enrolled group and assign the enrolled group to a Cisco Intercompany Media Engine service. You can disable or enable Cisco IME from calling certain phones in the enterprise by disassociating or associating the enrolled group to the Cisco IME service.

Note

You can exclude specific numbers that fall within the range of an enrolled pattern from participating in Cisco IME by configuring exclusion groups and exclusion numbers. For more information, see the Exclusion group configuration settings, on page 18 and Exclusion number configuration settings, on page 18.

To access the IME Enrolled Pattern Server Configuration window, click Advanced Features > Intercompany Media Services > Enrolled Pattern.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the Cisco Unified Communications Manager Administration basics, on page 1 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration settings table

The following table describes the Cisco IME enrolled pattern configuration settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern</td>
<td>Create a unique pattern that contains the following characteristics:</td>
</tr>
<tr>
<td></td>
<td>• Begins with a plus sign (+).</td>
</tr>
<tr>
<td></td>
<td>• Contains up to 15 digits, including numbers between 0 and 9 and up to 3</td>
</tr>
<tr>
<td></td>
<td>wildcard (X) characters at the end of the pattern.</td>
</tr>
<tr>
<td></td>
<td>• Wildcard characters represent numbers between 0 and 9.</td>
</tr>
<tr>
<td></td>
<td>The following patterns represent valid enrolled patterns:</td>
</tr>
<tr>
<td></td>
<td>• +14089021xxx</td>
</tr>
<tr>
<td></td>
<td>• +191937611xx</td>
</tr>
<tr>
<td></td>
<td>• +14089523513</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a descriptive name for the enrolled pattern. The description can</td>
</tr>
<tr>
<td></td>
<td>contain up to 128 characters.</td>
</tr>
<tr>
<td>Enrolled Group</td>
<td>Choose the Cisco IME enrolled group to associate with this enrolled pattern.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> To configure more enrolled groups, see the Enrolled group</td>
</tr>
<tr>
<td></td>
<td>configuration settings, on page 15</td>
</tr>
</tbody>
</table>
**Related Topics**

Set up Cisco IME, on page 5

---

**Exclusion group configuration settings**

This section describes how to create an exclusion group.

To access the **Intercompany Media Services Exclusion Group Configuration** window, click **Advanced Features > Intercompany Media Services > Exclusion Group**.

**GUI use**

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the *Cisco Unified Communications Manager Administration basics*, on page 1 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

**Configuration settings table**

The following table describes the Cisco IME exclusion group configuration settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name for the exclusion group. The name can comprise up to 32 characters in length.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a descriptive name of the exclusion group. The description can comprise up to 128 characters. (Optional)</td>
</tr>
</tbody>
</table>

**Related Topics**

Set up Cisco IME, on page 5

---

**Exclusion number configuration settings**

To access the **Intercompany Media Services Exclusion Number Configuration** window, click **Advanced Features > Intercompany Media Services > Exclusion Number**.

**GUI use**

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the *Cisco Unified Communications Manager Administration basics*, on page 1 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.
Configuration settings table

The following table describes the Cisco IME exclusion number settings.

Table 5: Cisco Intercompany Media Engine exclusion number configuration settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern</td>
<td>Specify the +E.164 number that you want to exclude from Cisco IME. You must precede the number by a plus sign (+). The number may contain up to 15 digits. You must enter the exact +E.164 number with no wildcards.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a descriptive name of the exclusion number. The description can comprise up to 128 characters. (Optional)</td>
</tr>
<tr>
<td>Exclusion Group</td>
<td>From the drop-down list box, choose the Cisco IME group to associate with this exclusion number. To configure additional exclusion groups, see the Exclusion group configuration settings, on page 18.</td>
</tr>
</tbody>
</table>

Related Topics

Set up Cisco IME, on page 5

Set up IME Trust Groups and Elements

Complete the following tasks to set up the IME Trust Groups and Elements:

Procedure

Step 1
Create trust groups to which you can assign domains and prefixes, or trust elements, that the Cisco IME trusts. For more information, see Trust group configuration settings, on page 19.

Step 2
Specify the prefixes or domains that you want to trust or not trust and associate these trust elements with a trust group. For more information, see Trust element configuration settings, on page 20.

What to Do Next

Set up the Cisco IME service. For more information, see Intercompany media service configuration settings, on page 21.

Trust group configuration settings

Configuration of trust groups is optional. If you do not create trust groups, Cisco IME trusts all calls by default.
This section describes how to configure a trust group. For information on creating domains and prefixes to include in the trust group, see the Trust element configuration settings, on page 20.

To access the Intercompany Media Services Trusted Group Configuration window, click Advanced Features > Intercompany Media Services > Trust Group.

GUI use

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the Cisco Unified Communications Manager Administration basics, on page 1 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration settings table

The following table describes the Intercompany Media Services trust group configuration settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name for the trust group. The name can comprise up to 32 characters in length.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a descriptive name of the trust group. The description can comprise up to 128 characters. (Optional)</td>
</tr>
<tr>
<td>Trusted</td>
<td>Choose a trust value from the drop-down list box, either Yes (trusted) or No (untrusted). You cannot change this value if any trust elements use this trust group. This limitation prevents you from accidentally changing an untrusted group (or blacklist) to a trusted group (or whitelist) by changing one value. No default value exists. You must select a value.</td>
</tr>
</tbody>
</table>

Related Topics

Set up Cisco IME, on page 5

Trust element configuration settings

This section describes how to create trust elements and how to associate the trust elements with a trust group. After you create the trust elements, you associate trust groups with an Cisco IME service to trust or not trust the prefixes or domains that the trust group specifies.

To access the Intercompany Media Services Trust Element Configuration window, choose Advanced Features > Intercompany Media Services > Trust Element.
GUI use

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the Cisco Unified Communications Manager Administration basics, on page 1 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration settings table

The following table describes the Intercompany Media Services trust element configuration settings.

Table 7: Intercompany Media Services trust element configuration settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a domain name or a prefix. Domain names can contain up to 128 characters. You must specify a valid domain name. Prefixes must begin with a + sign followed by up to 15 characters or up to 14 characters and a wildcard !.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a descriptive name for the engine trust element. The description can comprise up to 128 characters.</td>
</tr>
<tr>
<td>Element Type</td>
<td>Choose the appropriate element type, either Domain or Prefix.</td>
</tr>
<tr>
<td>Trust Group</td>
<td>Choose the appropriate trust group. To include this element in a whitelist (trusted group), choose a trusted group from the drop-down list box. To include this element in a blacklist (untrusted group), choose an untrusted group from the drop-down list box. For information on configuring trust groups, see the Trust group configuration settings, on page 19</td>
</tr>
</tbody>
</table>

Related Topics

Set up Cisco IME, on page 5

Intercompany media service configuration settings

To begin load balancing so that the system work spreads across multiple Cisco Intercompany Media Engine servers, create more than one Cisco Intercompany Media Engine service with different Cisco Intercompany Media Engine servers and move some of the enrolled groups from the old Cisco Intercompany Media Engine service to the new service.

To access the Intercompany Media Service Configuration window, click Advanced Features > Intercompany Media Services > Service.

For information about the CUCM External Address List pop-up window, see the CUCM external address list configuration settings, on page 24.
**GUI use**

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the Cisco Unified Communications Manager Administration basics, on page 1 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

**Configuration settings table**

The following table describes the Intercompany Media Service configuration settings.

*Table 8: Intercompany Media Service configuration settings*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intercompany Media Service information</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter a unique name for the Cisco IME service. The name can comprise up to 50 characters in length.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a descriptive name for the Cisco IME service. The description can comprise up to 128 characters in length.</td>
</tr>
<tr>
<td>Domain</td>
<td>Enter the domain name to use with Cisco IME. Typically, you specify the domain name of your enterprise, such as <code>cisco.com</code>. The domain name must match the domain name that is contained in the SSL certificate from GoDaddy.com for the ASA.</td>
</tr>
<tr>
<td>SIP Trunk</td>
<td>Choose the SIP trunk that you want to use with this service. The drop-down list box populates with trunks that specify the Cisco Intercompany Media Engine trunk service type. The trunk that you select runs on a specific set of nodes in the cluster, as defined by the Cisco Unified Communications Manager group that associates with the trunk. The Cisco IME service also runs on that same set of nodes. <strong>Tip</strong> You configured Cisco Intercompany Media Engine trunks in the Set up Cisco IME, on page 5.</td>
</tr>
<tr>
<td>Trust Group</td>
<td>If desired, choose a trust group. Trust groups contain a list of domains and prefixes that are trusted (or untrusted) by the Cisco IME service with which the group associates. Cisco Unified Communications Manager can only place Cisco IME calls to domains or prefixes that are trusted. The drop-down list box populates with servers that you configured in the Intercompany Media Services Trust Group Configuration window (Advanced Features &gt; Intercompany Media Services &gt; IME Trusted Group). If you do not choose a trust group, Cisco IME trusts all prefixes and domains.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Exclusion Group</td>
<td>If desired, choose an exclusion group. Exclusion groups contain numbers that you want to prevent from using Cisco Intercompany Media Engine. The drop-down list box populates with servers that you configured in the Intercompany Media Services Exclusion Group Configuration window (Advanced Features &gt; Intercompany Media Services &gt; IME Exclusion Group).</td>
</tr>
<tr>
<td>Firewall</td>
<td>If you are using an off-path ASA deployment model, choose the firewall to associate with this service.</td>
</tr>
<tr>
<td>Available Enrolled Groups</td>
<td>This list box displays the enrolled groups that are available for association with this Cisco IME service. Enrolled groups specify the set of +E.164 numbers that make and receive Cisco IME calls. To associate an enrolled group with this Cisco IME service, select the enrolled group and click the down arrow below this list box.</td>
</tr>
<tr>
<td>Selected Enrolled Groups</td>
<td>This list box displays the enrolled groups that associate with this Cisco IME service. To remove an enrolled group, select the enrolled group name and click the Up arrow above this list box. To add an enrolled group, select an enrolled group in the Available Enrolled Groups list box and click the Down arrow between the list group boxes. You can reorder the enrolled groups by clicking the Up and Down arrows to the right of the list box.</td>
</tr>
<tr>
<td>Activated</td>
<td>Check the Activated check box to activate the Cisco IME service. If you do not activate the service, you cannot make and receive Cisco IME calls.</td>
</tr>
</tbody>
</table>

**Server information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary IME Server</td>
<td>Choose a primary Cisco IME server. The drop-down list box populates with servers that you configure in the Intercompany Media Server Connection Configuration window (Advanced Features &gt; Intercompany Media Services &gt; Server Connections). You can use the selected server in more than one service. If you define multiple Cisco IME services but you have only one Cisco IME server, you can associated multiple Cisco IME services with a single server.</td>
</tr>
</tbody>
</table>
(Optional) Choose a secondary Cisco IME server. The drop-down list box populates with servers that you configure in the Intercompany Media Server Connection Configuration window (Advanced Features > Intercompany Media Services > Server Connections).

You must choose different servers for the primary and secondary Cisco IME servers. You can use the selected server in more than one service.

**CUCM external address list configuration settings**

For inbound calls, the Cisco Intercompany Media Engine-enabled ASA utilizes network address translation (NAT). A specific IP/port on one of the ASA interfaces has a static mapping to each Cisco Unified Communications Manager node on the inside. Cisco Unified Communications Manager, through its existing configuration, advertises the IP/port on the ASA instead. As a result, inbound calls arrive at the Cisco Intercompany Media Engine-enabled ASA.

You need to provide external IP addresses or hostnames if your Cisco Unified Communications Manager servers reside behind a firewall or NAT.

To access the CUCM External Address List pop-up window, find the Cisco IME service to which you want to associate the IP Address and port by choosing Advanced Features > Intercompany Media Services > Service. From the Related Links drop-down list box in the Intercompany Media Service Configuration window, click Add/Update CUCM External Address List > Go.

The following table describes the address list configuration settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CUCM External Address List</strong></td>
<td></td>
</tr>
<tr>
<td>Cisco Unified CM</td>
<td>Displays the Cisco Unified Communications Manager servers in your system.</td>
</tr>
<tr>
<td>IP Address/Host</td>
<td>Enter the IP address or hostname that you want other enterprises to use to route calls to your enterprise. You must provide an IP address or hostname that all enterprises that use Cisco IME can resolve.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port to use for external Cisco IME traffic.</td>
</tr>
</tbody>
</table>
Set up IME Transformation Patterns and Profiles

Complete the following tasks to set up the IME Transformation Patterns and Profiles:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Set up the calling party and called party transformation patterns.</td>
<td>For more information, see Set up transformation patterns for Cisco IME, on page 25.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Set up two transformation profiles: one for incoming calling party numbers and one for incoming called party numbers.</td>
<td>For more information, see Transformation profile configuration settings, on page 25.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Set up Cisco IME+E.164 transformations.</td>
<td>For more information, see E.164 transformation configuration settings, on page 31.</td>
</tr>
</tbody>
</table>

**What to Do Next**

Set up IME feature configurations. For more information, see Set up IME feature configurations, on page 33.

**Set up transformation patterns for Cisco IME**

- To access the Calling Party Transformation Pattern Configuration window, click **Call Routing > Transformation > Transformation Pattern > Calling Party Transformation Pattern**.
- To access the Called Party Transformation Pattern Configuration window, click **Call Routing > Transformation > Transformation Pattern > Called Party Transformation Pattern**.

For calling and called party transformation pattern configuration settings, refer to the *Cisco Unified Communications Manager Administration Guide* or click **Help** in the respective window in the Cisco Unified Communications Manager Administration.

**Related Topics**

Set up Cisco IME, on page 5

**Transformation profile configuration settings**

You must create one profile for the incoming called number and one for the incoming calling number. You associate the transformation profiles with the Cisco IME transformation as described in E.164 transformation configuration settings, on page 31.
Cisco IME does not upload VCRs that do not contain numbers in +E.164 format.

To access the Transformation Profile Configuration window, click **Call Routing > Transformation > Transformation Profile**.

**Using the GUI**

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the *Cisco Unified Communications Manager Administration basics*, on page 1 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

**Configuration settings table**

The following table describes the transformation profile configuration settings.

*Table 10: Cisco Intercompany Media Engine transformation profile configuration settings*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Transformation profile information</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter a unique name for the transformation profile. The name can comprise up to 50 characters in length.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a descriptive name for the transformation profile. The description can comprise up to 128 characters in length.</td>
</tr>
<tr>
<td><strong>Incoming party setting</strong></td>
<td></td>
</tr>
<tr>
<td>Clear Prefix Settings</td>
<td>To delete prefixes for all calling party number types, click the <strong>Clear Prefix Settings</strong> button.</td>
</tr>
<tr>
<td>Default Prefix Settings</td>
<td>To reset prefixes for all calling party number types to the default values, click the <strong>Default Prefix Settings</strong> button.</td>
</tr>
</tbody>
</table>
Configure the following settings to globalize calling party numbers that use National for the Number Type. The National number type gets used for calls within your country.

- **Prefix** - Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use National for the Calling Party Number Type. You can enter up to eight characters, which include digits, the international escape character (+), asterisk (*), or the octothorpe (#). You can enter the word, Default, instead of entering a prefix.

  **Tip**  
  If the word, Default, displays in the Prefix field in the Gateway Configuration or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway Configuration or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that applies to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip-digit capabilities.

  **Tip**  
  To configure the Strip Digits field in the Device Pool Configuration, Gateway Configuration, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field.

- **Strip Digits** - Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of National number type before Cisco Unified Communications Manager applies the prefixes.

- **Calling Search Space** - This setting allows you to globalize the calling party number of National calling party number type on the device. Make sure that the calling search space that you choose contains the calling party transformation pattern that you want to assign to this device.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| National Number | Configure the following settings to globalize calling party numbers that use National for the Number Type. The National number type gets used for calls within your country.  
  - **Prefix** - Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use National for the Calling Party Number Type. You can enter up to eight characters, which include digits, the international escape character (+), asterisk (*), or the octothorpe (#). You can enter the word, Default, instead of entering a prefix.  
    **Tip**  
    If the word, Default, displays in the Prefix field in the Gateway Configuration or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway Configuration or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that applies to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip-digit capabilities.  
    **Tip**  
    To configure the Strip Digits field in the Device Pool Configuration, Gateway Configuration, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field.  
    - **Strip Digits** - Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of National number type before Cisco Unified Communications Manager applies the prefixes.  
    - **Calling Search Space** - This setting allows you to globalize the calling party number of National calling party number type on the device. Make sure that the calling search space that you choose contains the calling party transformation pattern that you want to assign to this device. |
### Configure the following settings to globalize calling party numbers that use International for the Number Type.

The International number type gets used for calls outside the dialing plan for your country.

- **Prefix** - Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use International for the Calling Party Numbering Type. You can enter up to eight characters, which include digits, the international escape character (+), asterisk (*), or the octothorpe (#). You can enter the word, Default, instead of entering a prefix.

**Tip**  
If the word, Default, displays in the Prefix field in the Gateway Configuration or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway Configuration or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that applies to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip-digit capabilities.

**Tip**  
To configure the Strip Digits field in the Device Pool Configuration, Gateway Configuration, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field.

- **Strip Digits** - Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of International type before Cisco Unified Communications Manager applies the prefixes.

- **Calling Search Space** - This setting allows you to globalize the calling party number of International calling party number type on the device. Make sure that the calling party transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.

**Tip**  
Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as None, the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>International Number</td>
<td>Configure the following settings to globalize calling party numbers that use International for the Number Type. The International number type gets used for calls outside the dialing plan for your country.</td>
</tr>
</tbody>
</table>

- **Prefix** - Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use International for the Calling Party Numbering Type. You can enter up to eight characters, which include digits, the international escape character (+), asterisk (*), or the octothorpe (#). You can enter the word, Default, instead of entering a prefix.

**Tip**  
If the word, Default, displays in the Prefix field in the Gateway Configuration or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway Configuration or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that applies to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip-digit capabilities.

**Tip**  
To configure the Strip Digits field in the Device Pool Configuration, Gateway Configuration, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field.

- **Strip Digits** - Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of International type before Cisco Unified Communications Manager applies the prefixes.

- **Calling Search Space** - This setting allows you to globalize the calling party number of International calling party number type on the device. Make sure that the calling party transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.

**Tip**  
Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as None, the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing.
Configure the following settings to globalize calling party numbers that use Unknown for the Number Type. The Unknown number type gets used when the dialing plan is unknown.

- **Prefix** - Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use Unknown for the Calling Party Numbering Type. You can enter up to eight characters, which include digits, the international escape character (+), asterisk (*), or the octothorpe (#). You can enter the word, Default, instead of entering a prefix.  

  **Tip**  
  If the word, Default, displays in the Prefix field in the Gateway Configuration or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway Configuration or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that applies to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip-digit capabilities.  

  **Tip**  
  To configure the Strip Digits field in the Device Pool Configuration, Gateway Configuration, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field.  

- **Strip Digits** - Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of Unknown type before Cisco Unified Communications Manager applies the prefixes.  

- **Calling Search Space** - This setting allows you to globalize the calling party number of Unknown calling party number type on the device. Make sure that the calling party transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.  

  **Tip**  
  Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as None, the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unknown Number</td>
<td>Configure the following settings to globalize calling party numbers that use Unknown for the Number Type. The Unknown number type gets used when the dialing plan is unknown.</td>
</tr>
</tbody>
</table>

- **Prefix** - Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use Unknown for the Calling Party Numbering Type. You can enter up to eight characters, which include digits, the international escape character (+), asterisk (*), or the octothorpe (#). You can enter the word, Default, instead of entering a prefix.  

  **Tip**  
  If the word, Default, displays in the Prefix field in the Gateway Configuration or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway Configuration or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that applies to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip-digit capabilities.  

  **Tip**  
  To configure the Strip Digits field in the Device Pool Configuration, Gateway Configuration, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field.  

- **Strip Digits** - Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of Unknown type before Cisco Unified Communications Manager applies the prefixes.  

- **Calling Search Space** - This setting allows you to globalize the calling party number of Unknown calling party number type on the device. Make sure that the calling party transformation CSS that you choose contains the calling party transformation pattern that you want to assign to this device.  

  **Tip**  
  Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as None, the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing.
Configure the following settings to globalize calling party numbers that use Subscriber for the Number Type. The Subscriber number type gets used when you are dialing a subscriber by using a shortened subscriber number.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Subscriber Number | Configure the following settings to globalize calling party numbers that use Subscriber for the Number Type. The Subscriber number type gets used when you are dialing a subscriber by using a shortened subscriber number.  
  
  - **Prefix** - Cisco Unified Communications Manager applies the prefix that you enter in this field to calling party numbers that use Subscriber for the Calling Party Numbering Type. You can enter up to eight characters, which include digits, the international escape character (+), asterisk (*), or the octothorpe (#). You can enter the word, Default, instead of entering a prefix.  
  
  **Tip**  
  If the word, Default, displays in the Prefix field in the Gateway Configuration or Trunk Configuration window, you cannot configure the Strip Digits field in the Gateway Configuration or Trunk Configuration window. In this case, Cisco Unified Communications Manager takes the configuration for the Prefix and Strip Digits fields from the device pool that applies to the device. If the word, Default, displays in the Prefix field in the Device Pool Configuration window, Cisco Unified Communications Manager applies the service parameter configuration for the incoming calling party prefix, which supports both the prefix and strip-digit capabilities.  
  
  **Tip**  
  To configure the Strip Digits field in the Device Pool Configuration, Gateway Configuration, or Trunk Configuration window, you must leave the Prefix field blank or enter a valid configuration in the Prefix field. To configure the Strip Digits fields in these windows, do not enter the word, Default, in the Prefix field.  
  
  - **Strip Digits** - Enter the number of digits that you want Cisco Unified Communications Manager to strip from the calling party number of Subscriber type before Cisco Unified Communications Manager applies the prefixes.  
  
  - **Calling Search Space** - This setting allows you to globalize the calling party number of Subscriber calling party number type on the device. Make sure that the CSS that you choose contains the calling party transformation pattern that you want to assign to this device.  
  
  **Tip**  
  Before the call occurs, the device must apply the transformation by using digit analysis. If you configure the CSS as None, the transformation does not match and does not get applied. Ensure that you configure the calling party transformation pattern in a non-null partition that is not used for routing. |

**Related Topics**

Set up Cisco IME, on page 5
**E.164 transformation configuration settings**

Cisco Intercompany Media Engine (Cisco IME) E.164 transformations convert calling numbers and called numbers on both the originating and terminating (incoming and outgoing) sides to +E.164 format after a PSTN call terminates. Cisco IME E.164 transformations do not impact call routing or digit analysis in Cisco Unified Communications Manager. The transformations allow the following actions to occur:

- Send UploadVCRs to the Cisco Intercompany Media Engine server for unlearned direct inward dialing numbers (DIDs).
- Reroute calls to the Cisco IME trunk if the DID exists in the learned table.

You associate Cisco IME E.164 transformations with a PSTN access trunk. If the transformation does not yield valid calling and called numbers on the incoming and outgoing sides of the call, no VCR upload takes place, and Cisco IME processing stops for that call.

To access the Intercompany Media Services E.164 Transformation Configuration window, click Advanced Features > Intercompany Media Services > E.164 Transformation.

**GUI use**

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the Cisco Unified Communications Manager Administration basics, on page 1 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

**Configuration settings table**

The following table describes the transformation configuration settings.

| Table 11: Cisco Intercompany Media Engine E.164 transformation configuration settings |
|-----------------------------------------|-----------------------------------------------|
| Field                                  | Description                                   |
| **E.164 transformation**               |                                               |
| Name                                   | Enter a unique name for the transformation profile. This name can comprise up to 50 characters in length. |
| Description                            | Enter a descriptive name for the transformation profile. The description can comprise up to 128 characters in length. |
| **Outgoing Calling Party settings**    |                                               |
| Outgoing Party E.164 Transformation CSS| From the drop-down list box, choose the appropriate calling search space for the calling party on outgoing calls. Choose a calling search space that contains the partitions used by the calling party transformation pattern that you configured on the Calling Party Transformation window (Call Routing > Transformation > Transformation Pattern > Calling Party Transformation Pattern). |
### Field Description

**Apply On**
Choose whether you want to apply the calling search space to the original number or to the routing transformed number.

**Outgoing Called Party settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Outgoing Party E.164 Transformation CSS</strong></td>
<td>From the drop-down list box, choose the appropriate calling search space for the called party on outgoing calls. Choose a calling search space that contains the partitions used by the called party transformation pattern that you configured on the Called Party Transformation window (Call Routing &gt; Transformation &gt; Transformation Pattern &gt; Called Party Transformation Pattern).</td>
</tr>
</tbody>
</table>

**Apply On**
Choose whether you want to apply the calling search space to the original number or to the routing transformed number.

**Incoming transformation profile settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Incoming Calling Party Transformation Profile</strong></td>
<td>Choose the appropriate incoming calling party transformation profile that you configured in the Transformation Profile Configuration window (Call Routing &gt; Transformation &gt; Transformation Profile), as described in the Transformation profile configuration settings, on page 25.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Incoming Called Party Transformation Profile</strong></td>
<td>Choose the appropriate incoming called party transformation profile that you configured in the Transformation Profile Configuration window (Call Routing &gt; Transformation &gt; Transformation Profile), as described in the Transformation profile configuration settings, on page 25.</td>
</tr>
</tbody>
</table>

### Related Topics

Set up Cisco IME, on page 5

### Set up PSTN access trunks

If a SIP trunk in your network connects to a SIP gateway that connects to the PSTN, you can configure this SIP trunk as a PSTN access trunk. If another SIP trunk that is an intercluster trunk connects to another cluster in your network, you do not have to configure this SIP trunk as a PSTN access trunk, because calls from this trunk will never go to the PSTN.
Procedure

Step 1  Click Device > Trunk and find the PSTN trunk that you want to configure.

Step 2  Select the PSTN Access check box.

Step 3  Click Advanced Features > Intercompany Media Services > E.164 Transformation and choose the E.164 transformation profile that you configured in the E.164 Transformation Configuration window. The profile transforms the called party and calling party numbers to +E.164 format. Numbers must use +E.164 format for call validation. If you do not choose a profile from this drop-down list box, Cisco Unified Communications Manager does not upload VCRs to the Cisco Intercompany Media Engine server.

Related Topics

Set up Cisco IME, on page 5

Set up IME feature configurations

Complete the following tasks to set up the IME feature and device configurations:

Procedure

Step 1  Set up the IME feature configurations. For more information, see Feature configuration settings, on page 33.

Step 2  Set up a common device. For more information, see Set up common device, on page 36.

What to Do Next

Verify the VAP connectivity between the Cisco IME server and the Cisco Unified Communications Manager server. For more information, see Server communication, on page 37.

Feature configuration settings

Use the Intercompany Media Services Feature Configuration window to configure feature parameters that apply to Cisco Intercompany Media Engine (Cisco IME).

To access the Intercompany Media Services Feature Configuration window, choose Advanced Features > Intercompany Media Services > Feature Configuration.

Configuration settings table

The following table describes the Intercompany Media Services feature configuration settings.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intercompany Media Services parameters</strong></td>
<td></td>
</tr>
<tr>
<td>Allow IME Calls through MGCP FXS/FXOs</td>
<td>Indicate whether Cisco IME allows MGCP FXS/FXO analog gateway devices, such as those used to connect to fax machines, to make Cisco IME calls. Choose True to allow MGCP FXO/FXS gateways to make Cisco IME calls. Choose False to prevent MGCP FXO/FXS gateways from making Cisco IME calls. The default value specifies False.</td>
</tr>
<tr>
<td>Enable Intradomain IME</td>
<td>Indicate whether you want to enable Cisco IME for calls to another cluster within your enterprise. Generally, intercluster trunks manage calls between clusters; however, if you are using the PSTN between clusters within the same domain, you can use Cisco IME to learn the patterns between those clusters by enabling this field. Select <strong>True</strong> to enable Cisco IME between clusters in the same enterprise domain. Select <strong>False</strong> to disable Cisco IME between clusters in the same enterprise domain. The default value specifies False.</td>
</tr>
<tr>
<td>Allow MWI via IME Learned Routes</td>
<td>Indicate whether Cisco Unified Communications Manager can use Cisco IME learned routes for message waiting indicator (MWI) notifications. Choose True to allow Cisco Unified Communications Manager to use Cisco IME learned routes for MWI messages. Choose False to prevent Cisco Unified Communications Manager from using Cisco IME learned routes for MWI messages. The default value specifies True.</td>
</tr>
<tr>
<td>SIP Trunk IME Connection Timer for Destination Enterprise</td>
<td>Specify the amount of time in seconds that a Cisco IME SIP trunk attempts to establish a connection to a SIP uniform resource identifier (URI) that exists for a learned route to a destination enterprise. When this timer expires, the SIP trunk attempts to establish a connection to the next URI, if available, for that learned route to the destination enterprise. The default value specifies 2 seconds. Valid values range from 1 to 5.</td>
</tr>
<tr>
<td>Firewall Connection Request Timer for IME Calls</td>
<td>Specify the amount of time, in seconds, that the Cisco Unified Communications Manager waits to establish a TCP connection with the Cisco IME firewall. If the firewall does not send a connection response to the Cisco Unified Communications Manager connection request before the timer expires, Cisco Unified Communications Manager continues the call without going through the Cisco IME firewall. In other words, Cisco Unified Communications Manager makes a PSTN call. The default value specifies 2 seconds. Valid values range from 1 to 5.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Firewall Mapping Response Timer for IME Calls</td>
<td>Specify the amount of time, in seconds, that the Cisco Unified Communications Manager waits to complete a mapping transaction (request and response) with the Cisco IME firewall. If the firewall does not send a mapped address response to the Cisco Unified Communications Manager mapped address request before the timer expires, Cisco Unified Communications Manager continues the call without going through the Cisco IME firewall. In other words, Cisco Unified Communications Manager makes a PSTN call. The default value specifies 2 seconds. Valid values range from 1 to 5.</td>
</tr>
<tr>
<td>Firewall Mapping Connection Idle Timer for IME calls</td>
<td>Specify the amount of time, in minutes, that the connection between the Cisco Unified Communications Manager and the Cisco IME firewall can remain idle before Cisco IME firewall tears down the connection with the Cisco Unified Communications Manager. This timer begins when Cisco Unified Communications Manager stops sending new call requests to the Cisco IME firewall. You can choose a higher value in this field to decrease delay in establishing new calls through the Cisco IME firewall, or you can choose a lower value to close the connection sooner. A lower value enhances security but may cause a minor delay in establishment of new calls. The default value specifies 10. Valid values range from 5 to 60.</td>
</tr>
<tr>
<td>ICM Failed Call Attempt Threshold</td>
<td>Specify the percentage of failed Cisco IME call attempts to exceed before Cisco Unified Communications Manager generates the IMEQualityAlertEntry alarm. When the percentage of failed Cisco IME call setup attempts falls below the threshold defined in this field and the system does not exceed the fallback threshold that the IME Call Fallback Attempt Threshold field specifies, Cisco Unified Communications Manager triggers the IMEQualityAlertExit alarm, which clears the IMEQualityAlertEntry alarm. Entering a higher threshold value makes the system more tolerant of failed Cisco IME call attempts, so that more calls fail before Cisco Unified Communications Manager triggers an alarm. A higher value may be useful during minor network outages. Entering a lower threshold value makes the system less tolerant of Cisco IME call setup failures, so fewer calls fail before Cisco Unified Communications Manager triggers an IMEQualityAlertEntry alarm. The default value specifies 50 percent. Valid values range from 10 to 100.</td>
</tr>
</tbody>
</table>
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICM Call Fallback Attempt Threshold</td>
<td>Specify the percentage of active Cisco IME calls that fallback to the PSTN to exceed before Cisco Unified Communications Manager generates the IMEQualityAlertEntry alarm. When the percentage of Cisco IME calls that experience mid-call fallback to the PSTN falls below the threshold defined in this field and the percentage of failed Cisco IME call setup attempts falls below the value specified in the IME Failed Call Attempt Threshold field, Cisco Unified Communications Manager generates the IMEQualityAlertExit alarm, which clears the IMEQualityAlertEntry alarm. Entering a higher threshold value makes the system more tolerant of Cisco IME calls that experience mid-call fallback to the PSTN, so that more calls fallback to the PSTN before Cisco Unified Communications Manager triggers an alarm. A higher value may be useful during minor network outages. Entering a lower threshold value makes the system less tolerant of Cisco IME calls that experience mid-call fallback to the PSTN, so fewer calls fallback before Cisco Unified Communications Manager triggers an IMEQualityAlertEntry alarm. The default value specifies 50. Valid values range from 10 to 100.</td>
</tr>
<tr>
<td>ICM Quality Alert Evaluation Interval</td>
<td>Specify the time interval in seconds that Cisco Unified Communications Manager uses to check the status of the ICM Failed Call Attempt Threshold and ICM Call Fallback Attempt Threshold parameters to determine whether to continue generating the IMEQualityAlertEntry alarm. The default value specifies 120. Valid values range from 30 to 1800.</td>
</tr>
<tr>
<td>Use IME for Outbound Calls</td>
<td>Specify whether to allow devices to make calls using the Cisco Intercompany Media Engine feature. Choose True to allow devices to make Cisco IME calls. Choose False to prevent devices from making Cisco IME calls. The default value specifies True.</td>
</tr>
</tbody>
</table>

#### Related Topics

- Set up Cisco IME, on page 5

---

### Set up common device

You can also disable Cisco Intercompany Media Engine from the Intercompany Media Services Feature Configuration window (Advanced Features > Intercompany Media Services > Feature Configuration) and create a common device configuration to enable Cisco IME for associated devices.
Procedure

Step 1  Click Device > Device Settings > Common Device Configuration.

Step 2  Create a common device configuration.
To disable Cisco IME for devices that associate with this common device configuration, select Off from the Use Intercompany Media (IME) for Outbound Calls drop-down list box. To enable Cisco IME, select On from the drop-down list box.

The default value equals the value that you set for the Use IME for Outbound Calls field in the Intercompany Media Services Feature Configuration window (Advanced Features > Intercompany Media Services > Feature Configuration).

Step 3  Associate the appropriate devices with this common device configuration.
For more information on associating devices with a common device configuration, refer to the Cisco Unified Communications Manager Administration Guide.

Server communication

The Cisco Unified Communications Manager server and the Cisco Intercompany Media Engine (Cisco IME) server communicate using the Validation Access Protocol (VAP). Without the communication between the servers, Cisco Unified Communications Manager cannot learn Cisco IME routes, and users cannot make Cisco IME calls. To determine if the VAP connection exists, you must verify that the Cisco Unified Communications Manager server registers with the Cisco IME server and that the Cisco Unified Communications Manager server has published Vservices with the Cisco IME server.

Related Topics

- Monitor server communication, on page 37
- Verify Vservice publication, on page 38
- Verify DID publication, on page 39
- Set up Cisco IME, on page 5

Monitor server communication

After you verify the registration status, you can continue to verify connectivity between the Cisco Unified Communications Manager server and the Cisco IME server by verifying that the Cisco Unified Communications Manager server has published the Cisco IME service (or Vservice) to the Cisco IME server.

From the CLI

- From the Cisco Intercompany Media Engine CLI, enter the following command: show ime vapstatus summary.
  
  This command displays the registration status for the client specified by port number. Make sure that the Registration Status equals Registered, and the Client IP ADDR equals the IP address of the Cisco Unified Communications Manager server.
Verify Vservice publication

The following example shows the output of the `show ime vapstatus summary` command in which the Cisco Unified Communications Manager registered with the Cisco IME server:

```
admin:show ime vapstatus summaryVAP Client Connection Details
Registration Status ...... Registered
Client IP ADDR............ 10.94.150.96
Client Handle ............ 1
Packets Sent ............. 106
Packets Rcvd ............. 106
VAPServer Name .......... vapuser
Missed Keep Alive Count .. 0
Connection Up Time ....... 3 hours 7 min 0 sec
```

**From RTMT**

- Access the Cisco Unified Communications Manager server using RTMT, and choose the following menu and counter: System > Performance > Open Performance Monitoring > IME Client Instance > VAPStatus

If a connection between the Cisco IME server and Cisco Unified Communications Manager server exists, the counter should equal 1 (healthy). The valid values equal: 0=unknown; 1=healthy; 2=unhealthy.

**Note**

This counter monitors connections to primary and secondary Cisco IME servers.

**Related Topics**

Set up Cisco IME, on page 5

**Verify Vservice publication**

Click the Advanced Features > Intercompany Media Services > Service and select the Activated check box. The Cisco Unified Communications Manager publishes the Vservice when you select the Activated check box on the Intercompany Media Service Configuration window.

Published Vservices indicate that an active service exists on the Cisco Unified Communications Manager and that it has connectivity into the Cisco IME server.

**Procedure**

To verify Vservice publication, enter the following command on the Cisco IME command line: `show ime vservice details`.

**Example:**

The following example shows the output of the command in which Cisco Unified Communications Manager has published a Vservice. The VServiceProfiles field matches the Cisco IME service name that you entered on the Intercompany Media Service Configuration window.

```
admin: show ime vservice detailsVServiceProfiles: Vservice12-ccm18
VServiceId = 3834353762636435
overlay = intercompanymediannetwork
domain = cisco.com
DiDCount (max) = 100
SIPURI = sip:d954c46b-51b4-ea2d-cda4-8a20134279f6@cisco.com:5082;
maddr=10.94.150.96,transport=tcp
```
What to Do Next

After you verify the Vservice publication, you can continue to verify connectivity between the Cisco Unified Communications Manager server and the Cisco IME server by verifying that the Cisco Unified Communications Manager server has published DID to the IME distributed cache as described in the Verify DID publication, on page 39.

Related Topics

Set up Cisco IME, on page 5

Verify DID publication

Use the following methods to verify DID publication:

- From the Cisco Intercompany Media Engine CLI, enter the following command: `utils ime fetch did E.164 number`
  The command output shows whether the Cisco IME server published DID to the IME distributed cache and which node owns the number.

- Access the Cisco Unified Communications Manager server using RTMT, and choose the following menu and counter: System > Performance > Open Performance Monitoring > IME Client Instance > PublishedRoutes.
  This counter indicates the total number of DID published successfully into the IME distributed cache across all Cisco IME client instances.

Set up fallback information

Complete the following tasks to set up the fallback information:

Procedure

**Step 1**
Increase the Media Exchange Stop Streaming Timer.
For more information, see increase Media Exchange Stop Streaming Timer, on page 40.

**Step 2**
Set up a fallback profile.
For more information, see Fallback profile configuration settings, on page 40.

**Step 3**
Associate the fallback profile with an enrolled group.
For more information, see Associate fallback profile to enrolled group, on page 44.

**Step 4**
Associate the enrolled group that you associated with a fallback profile to a device pool.
For more information, see Associate enrolled group to device pool, on page 44.

**Step 5**
Review the fallback feature parameters that Cisco Unified Communications Manager uses for mid-call fallback of Cisco IME calls to the PSTN.
For more information, see Fallback feature configuration settings, on page 45.
What to Do Next

Set up off-path settings. For more information, see Set up off-path settings, on page 46.

Increase Media Exchange Stop Streaming Timer

This parameter specifies the maximum seconds that the Cisco Unified Communications Manager waits to receive a response to a stop streaming request. If the Cisco Unified Communications Manager does not receive a within the specified time, the Cisco Unified Communications Manager terminates the call.

Complete the following steps to increase the Media Exchange Stop Streaming Timer:

Procedure

Step 1  Click `System > Service Parameters`.
Step 2  From the `Server` drop-down list box, select a server.
Step 3  From the `Service` drop-down list box, select the Cisco CallManager service.
Step 4  Set the `Media Exchange Stop Streaming Timer` parameter to 12 seconds.

Fallback profile configuration settings

When a user makes a call to a number that is linked to a fallback profile, the Cisco Unified Communications Manager of the calling party receives a fallback directory number that is configured on the Cisco Unified Communications Manager of the called party. The Cisco Unified Communications Manager uses the fallback number for the PSTN call when the ASA triggers a fallback to the PSTN.

After you configure the fallback profile and set the fallback feature parameters, you associate the fallback profile with an IME enrolled group (`Advanced Features > Intercompany Media Services > Enrolled Group`).

![Note](image)

If you want calls to fallback to the PSTN, make sure that you Enable Fallback for IME Calls parameter in the Fallback Feature Configuration window (`Advanced Features > Fallback > Fallback Feature Configuration`).

To access the Fallback Profile Configuration window, click `Advanced Features > Fallback > Fallback Profile`.

GUI use

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the Cisco Unified Communications Manager Administration basics, on page 1 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.
### Configuration settings table

The following table describes the fallback profile configuration settings.

**Table 13: Fallback profile configuration settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fallback profile information</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Enter a unique name for the fallback profile. This name can comprise up to 32 characters in length.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a descriptive name for the fallback profile. The description can comprise up to 128 characters in length. (Optional)</td>
</tr>
<tr>
<td><strong>Call setup fallback settings</strong></td>
<td></td>
</tr>
<tr>
<td>Advertised Fallback Directory E.164 Number</td>
<td>Specify the +E.164 DID number that Cisco Unified Communications Manager uses to fallback Cisco IME calls to the PSTN. The number that you enter must begin with a + and may contain up to 15 digits. The Cisco Unified Communications Manager from the terminating side of the call passes this number to the Cisco Unified Communications Manager on the originating side of the call so that the originating Cisco Unified Communications Manager can initiate fallback to the PSTN when the quality of service falls below the level that this fallback profile specifies. For example, if the originating enterprise receives +14089023232 as a fallback DID, the originating enterprise must have a route pattern or translation pattern that routes that number over the PSTN to the terminating enterprise that sent that fallback DID. You must provide a dedicated +E.164 number that has not been allocated to any device.</td>
</tr>
<tr>
<td><strong>Call fallback trigger settings</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fallback QOS Sensitivity Level</td>
<td>Indicate the RTP audio stream sensitivity level that you want the IME-enabled ASA to use to determine when to fallback a call to the PSTN. The Cisco Unified Communications Manager sends this value to the ASA firewall. Choose one of the following options:&lt;br&gt;  - Disable Fallback - This option disables the mid-call fallback feature. When you choose this option, no PSTN fallback of Cisco IME VoIP calls occurs.&lt;br&gt;  - Utility - This option maintains the lowest quality Cisco IME calls. This option does not provide consistent quality VoIP, but it does allow the greatest number of calls to be maintained on the VoIP network rather than being rerouted over the more costly PSTN. Cisco Systems does not recommend using this option for extended-duration calls. Cisco Systems recommends this option if you want to maintain as many calls as possible via the IP network, regardless of call quality.&lt;br&gt;  - Accommodative - Choose this option to accept a basic or low-level quality of audio on Cisco IME VoIP calls. With this level, the IME-enabled ASA attempts to retain calls over the IP network rather than falling back to the PSTN, even if the calls have less than desirable audio quality.&lt;br&gt;  - Nominal - Choose this option to maintain Cisco IME VoIP calls that have good or better quality than PSTN calls. Most enterprise deployments qualify based on reasonably high quality and high-speed Internet connectivity. (Default)&lt;br&gt;  - Moderate - This option maintains only Cisco IME VoIP calls that have very good QoS. Calls with lesser QoS statistics fallback to the PSTN. For this option, the enterprises at both ends of the call must have Tier 1 or Tier 2 networks. If both enterprises do not meet the network requirement, the system routes the calls over the PSTN.&lt;br&gt;  - Aggressive - This option maintains only Cisco IME VoIP calls that have superior QoS quality; that is, calls that are virtually identical to QoS-provisioned VoIP. All calls that do not meet the QoS statistics for calls at this level fallback to the PSTN. For this option, the enterprises at both ends of the call must have Tier 1 or Tier 2 networks. If both enterprises do not meet the network requirement, the system routes the calls over the PSTN.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
**Fallback Call CSS** | Choose which calling search space to use to route a fallback call to the PSTN on the originating Cisco Unified Communications Manager cluster. The default specifies Calling device AAR Calling Search Space. If you have not defined an AAR calling search space, the re-route CSS can be used, depending on your system configuration.

**Fallback Call Answer Timer** | Do not change this value unless a Cisco TAC engineer instructs you to do so. This field indicates the amount of time in seconds (from 1 to 10) that the originating Cisco Unified Communications Manager waits for a mid-call fallback PSTN call to be answered. The default value equals the value of the Fallback Call Answer Timer in the Fallback Feature Configuration window (Advanced Features > Fallback > Fallback Feature Configuration).

**Note** | If the value of the Fallback Call Answer Time field on the Fallback Feature Configuration window is greater than the value that you configure here, the fallback call uses the value from the Fallback Feature Configuration window when a mid-call fallback takes place.

### Fallback call handling settings

| Field | Description |
--- | ---
**Fallback Directory Number Partition** | Choose the partition that Cisco Unified Communications Manager uses in routing fallback calls. This partition should be included in the calling search space used by the gateway devices that receive calls for the fallback number. The default specifies the default partition. For more information on configuring partitions and calling search spaces, refer to the Cisco Unified Communications Manager Administration Guide.

**Fallback Directory Number** | (Optional) Use this field to specify a non-E.164 version of the fallback directory number. For example, if the advertised +E.164 fallback number specifies +14089023092 and you normalize incoming numbers to seven digits before routing, the fallback directory number should specify 9023092. If you do not specify a value in this field, the +E.164 number gets injected into digit analysis. **Tip** | If you are using a dial plan that supports an +E.164 backplane, you can leave this field blank.
### Related Topics

- **Set up Cisco IME**, on page 5

### Associate fallback profile to enrolled group

Complete the following steps to associate a fallback profile to an enrolled group:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Click <em>Advanced Features &gt; Intercompany Media Services &gt; IME Enrolled Group.</em> Find the enrolled group to associate with the fallback profile that you created.</td>
</tr>
<tr>
<td>Step 2</td>
<td>From the <strong>Fallback Profile</strong> drop-down list box, choose the profile to associate with the selected enrolled group.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

### Associate enrolled group to device pool

Devices associated with this device pool use caller ID for PSTN fallback using the patterns from the enrolled group in the device pool.

Complete the following steps to associate an enrolled group to a device pool:

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Click <em>System &gt; Device Pool.</em></td>
</tr>
<tr>
<td>Step 2</td>
<td>Select the device pool to which you want to associate the fallback profile.</td>
</tr>
<tr>
<td>Step 3</td>
<td>From the <strong>Intercompany Media Services Enrolled Group</strong> drop-down list box, select the enrolled group.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>Save</strong>.</td>
</tr>
</tbody>
</table>
Fallback feature configuration settings

Use the Fallback Feature Configuration window to configure feature parameters that apply to mid-call fallback of Cisco Intercompany Media Engine (Cisco IME) calls to the PSTN.

To access the Fallback Profile Configuration window, click Advanced Features > Fallback > Fallback Feature Configuration.

Configuration settings table

The following table describes the fallback configuration settings.

Table 14: Fallback feature configuration settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Fallback for IME Calls</td>
<td>Specify whether Cisco Unified Communications Manager uses PSTN fallback. This value overrides any other setting for fallback.</td>
</tr>
<tr>
<td></td>
<td>This parameter must be enabled on the originating and terminating side of a call in order for PSTN fallback to occur.</td>
</tr>
<tr>
<td></td>
<td>The default specifies True.</td>
</tr>
<tr>
<td>Fallback QOS Sensitivity Level</td>
<td>Specify the sensitivity level for the ASA firewall to use to determine when to fallback a call to the PSTN. The Cisco Unified Communications Manager sends this value to the ASA firewall.</td>
</tr>
<tr>
<td></td>
<td>This parameter populates the default value of the Fallback QOS Sensitivity Level in the Fallback Profile Configuration window (Advanced Features &gt; Fallback &gt; Fallback Profile). This parameter also provides a default sensitivity level if you do not define a fallback profile.</td>
</tr>
<tr>
<td></td>
<td>This parameter applies to the terminating side during PSTN fallback. The default value specifies Nominal sensitivity.</td>
</tr>
<tr>
<td>Fallback Number of DTMF Correlation Digits</td>
<td>Specify the number of DTMF digits that the Cisco Unified Communications Manager uses for a mid-call fallback PSTN call.</td>
</tr>
<tr>
<td></td>
<td>This parameter applies to the terminating side during PSTN fallback. The default value specifies 4. Valid values range from 4 to 20.</td>
</tr>
<tr>
<td>Fallback DTMF Collection Timer</td>
<td>Specify the amount of time (in seconds) that Cisco Unified Communications Manager waits for DTMF digits collection during a mid-call fallback PSTN call.</td>
</tr>
<tr>
<td></td>
<td>This parameter applies to the terminating side during PSTN fallback. The default value specifies 3. Valid values range from 1 to 10.</td>
</tr>
</tbody>
</table>
Set up off-path settings

Complete the following steps to set up off-path settings:

**Procedure**

**Step 1** Configure the IP address and port of the ASA mapping service.
For more information, see Firewall configuration settings, on page 47.

**Step 2** Configure the feature parameters that apply to the firewall settings.
For more information, see Feature configuration settings, on page 33.

**Step 3** View the routes that the Cisco Intercompany Media Engine learned.
For more information, see Learned route configuration settings, on page 47.

---

**Field** | **Description**
--- | ---
Fallback Call Answer Timer | Specify the amount of time (in seconds) that Cisco Unified Communications Manager waits, after receiving alerting indication, for a mid-call fallback PSTN call to be answered before giving up. This parameter applies to the originating side during PSTN fallback. This parameter populates the default values in the fallback profile, as well as provides the default value if a profile is not defined. The default value specifies 3. Valid values range from 1 to 10.

**Note** If the value that you enter in the Fallback Call Answer Timer field on this window is greater than the value that you configure in the Fallback Call Answer Timer field on the Fallback Profile Configuration window (Advanced Features > Fallback > Fallback Profile). The fallback call uses the value from the Fallback Feature Configuration window when a mid-call fallback takes place.

Fallback Call CSS | Specify the calling search space to use to route the fallback calls. This parameter applies to the originating side during PSTN fallback. The default value specifies AAR CSS.

---

**Related Topics**

Set up Cisco IME, on page 5
**Firewall configuration settings**

During an outbound call attempt, the SIP invite message must be routed to the offpath Cisco IME enabled ASA. Cisco Unified Communications Manager sends a request to the ASA for a mapping of the global IP/port of the remote enterprise (found in the Cisco IME learned route) to an internal IP/port on the Cisco IME enabled ASA. Cisco Unified Communications Manager then initiates a SIP Invite that routes to this internal IP/port. The Cisco IME enabled ASA performs NAT, mapping to the global IP/port of the remote enterprise from the IME learned route. The offpath Cisco IME enabled ASA proxies this signaling session and initiates a TLS session to this global IP/port (the Cisco IME enabled ASA of the remote enterprise).

To access the Intercompany Media Services Firewall Configuration window, click Advanced Features > Intercompany Media Services > Firewall.

**GUI use**

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the Cisco Unified Communications Manager Administration basics, on page 1 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

**Configuration settings table**

The following table describes the Intercompany Media Services firewall configuration settings.

For related procedures, see the Set up Cisco IME, on page 5.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify a unique name for the ASA mapping service.</td>
</tr>
<tr>
<td>Description</td>
<td>Specify a description for the ASA mapping service.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the ASA mapping service.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port of the ASA mapping service.</td>
</tr>
</tbody>
</table>

**Learned route configuration settings**

To access the IME Learne Id Routes window, click Advanced Features > Intercompany Media Services > Learned Route.

**GUI use**

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the Cisco Unified Communications Manager Administration basics, on page 1 and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.
## Configuration settings table

The following table describes the Intercompany Media Services learned route configuration settings.

**Table 16: Cisco Intercompany Media Engine learned route configuration settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E.164</td>
<td>The field specifies +E.164 number that the Cisco Unified Communications Manager has learned.</td>
</tr>
<tr>
<td>Domain</td>
<td>This field specifies the domain for the +E.164 number.</td>
</tr>
<tr>
<td>Signaling</td>
<td>This field specifies the destination remote IP address and port of the dynamic SIP trunk that the system uses to reach the destination DID.</td>
</tr>
<tr>
<td>Learned-On</td>
<td>This field specifies the date that Cisco Unified Communications Manager learned this route.</td>
</tr>
<tr>
<td>Expires-On</td>
<td>This field specifies the date that this route expires. Routes expire a year after the learned-on date.</td>
</tr>
<tr>
<td>Admin Enabled</td>
<td>This field indicates whether a learned route is in use. To disable a route without deleting it from the database, clear the <strong>Admin Enabled</strong> check box. To enable a route so that Cisco Intercompany Media Engine can use the route, select this check box.</td>
</tr>
</tbody>
</table>

## Related Topics

- [Set up Cisco IME, on page 5](#)