Configuring Cisco Unified Communications Manager (CUCM)

Cisco Unified Communications Manager (CUCM) Configuration Summary

To enable teleconferencing on Cisco WebEx Meetings Server you must configure one CUCM system to manage call control but you can optionally configure a second CUCM system for audio high availability.

Before you configure CUCM, you must obtain your Load Balancer Point and Application Point information from your Cisco WebEx Meetings Server **Audio** page. Sign into your Administration site and select **Settings > Audio** to see this information. Load balancer points manage call load balancing and application points manage calls, conference flow, and feature control. Systems of different sizes have different numbers of load balancer points and application points and the numbers are not customized.

- Size (50/250/800/2000)

- High availability
- Transport type

On the **Audio** page there is a SIP Configuration Table that displays load balancer point and application point information including IP addresses and ports. This table is also displayed on the **Configuring Your Audio Settings for the First Time** page that appears the first time you configure your audio settings.

To make CUCM work with Cisco WebEx Meetings Server, CUCM requires the following base and specific configurations:

- Base configuration

  Note These configurations can be shared with multiple Cisco WebEx Meetings Server systems.

  - SIP trunk security profile
  - SIP profile

- Specific configuration

  Note These configurations must be made for individual Cisco WebEx Meetings Server systems and cannot be shared by multiple systems.

  - Certificate management
  - SIP trunk
  - Route group
  - Route list
  - Route pattern
  - SIP route pattern

Configuration Checklist

The configuration checklist displays the number of each CUCM configuration type that you must configure for your system.

System Size	Security Profiles (Base Configuration)	SIP Profiles (Base Configuration)	SIP Trunks (Specific Configuration)	Route Groups (Specific Configuration)	Route Lists (Specific Configuration)	Route Patterns (Specific Configuration)	SIP Route Patterns (Specific Configuration)
50 users	2	1	2	1	1	N[1]	1
50 users with high availability	2	1	4	1	1	N	2

System Size	Security Profiles (Base Configuration)	SIP Profiles (Base Configuration)	SIP Trunks (Specific Configuration)	Route Groups (Specific Configuration)	Route Lists (Specific Configuration)	Route Patterns (Specific Configuration)	SIP Route Patterns (Specific Configuration)
250 users	2	1	2	1	1	N	1
250 users with high availability	2	1	4	1	1	N	2
800 users	2	1	2	1	1	N	1
800 users with high availability	2	1	4	1	1	N	2
2000 users	2	1	5	1	1	N	3
2000 users with high availability	2	1	6	1	1	N	4

[1] N is the number of Call-In Access Numbers that you configure in Cisco WebEx Meetings Server.

Configuring CUCM for High-Availability and Non-High-Availability Systems

The following sections provide a description of the tasks required to configure high-availability and non-high-availability systems of various sizes.

Configuring CUCM on 50-, 250-, and 800-User Systems with No High Availability

This section describes the information required and detailed instructions on how to configure CUCM for 50-, 250-, and 800-user systems without high availability.

Information Required

- One load balance point IP address
- One application point IP address
- The number of call-in access numbers you will configure on your system

Configuration Procedure

Perform the following steps:

Task	Description	Detailed Information
1	Review the existing SIP trunk security profile and determine whether or not it satisfies your Cisco WebEx Meetings Server setup requirement. If it does not, configure two SIP trunk security profiles.	Add a SIP trunk security profile for your load balance point and add a SIP trunk security profile for your application point. See Configuring a SIP Trunk Security Profile for a Load Balance Point, on page 7 and Configuring a SIP Trunk Security Profile for an Application Point, on page 8.
2	Review the existing SIP profile and determine whether or not it satisfies your Cisco WebEx Meetings Server setup requirement. If it does not, configure one SIP profile.	Configure a SIP profile as described in Configuring a TLS SIP Profile or Configuring an IPv6 SIP Profile, on page 10.
3	Configure one SIP trunk for your load balance point.	See Configuring a SIP Trunk on a Load Balance Point.
4	Configure one SIP trunk for your application point.	See Configuring a SIP Trunk for an Application Point.
5	Configure one route group by using the SIP trunk that you configured for your load balance point in Task 3, above.	See Configuring a Route Group.
6	Configure one route list using the route group that you configured in Task 5, above.	See Configuring a Route List.
7	Configure *N* route patterns by using the above route list. *N* is the number of call-in access numbers that you configured in your audio settings on the Administration site.	See Configuring a Route Pattern.
8	Configure one SIP route pattern for your application point.	See Configuring a SIP Route Pattern.

Configuring CUCM on 50-, 250-, and 800-User Systems with High Availability

This section describes the information required and detailed instructions on how to configure CUCM for 50-, 250-, and 800-user systems with high availability.

Information Required

- Two load balance point IP addresses
- Two application point IP addresses
- The number of call-in access numbers you will configure on your system

Configuration Procedure

Perform the following steps:

Task	Description	Detailed Information
1	Review the existing SIP trunk security profile and determine whether or not it satisfies your Cisco WebEx Meetings Server setup requirement. If it does not, configure two SIP trunk security profiles.	Add a SIP trunk security profile for your load balance point and add a SIP trunk security profile for your application point. See Configuring a SIP Trunk Security Profile for a Load Balance Point, on page 7 and Configuring a SIP Trunk Security Profile for an Application Point, on page 8.
2	Review the existing SIP profile and determine whether or not it satisfies your Cisco WebEx Meetings Server setup requirement. If it does not, configure one SIP profile.	Configure a SIP profile as described in Configuring a TLS SIP Profile or Configuring an IPv6 SIP Profile, on page 10.
3	Configure two SIP trunks for your load balance points.	See Configuring a SIP Trunk on a Load Balance Point.
4	Configure two SIP trunks for your application points.	See Configuring a SIP Trunk for an Application Point.
5	Configure one route group by using the SIP trunk that you configured for your load balance point in Task 3, above.	See Configuring a Route Group.
6	Configure one route list by using the route group that you configured in Task 5, above.	See Configuring a Route List.
7	Configure *N* route patterns by using the above route list. *N* is the number of call-in access numbers that you configured in your audio settings on the Administration site.	See Configuring a Route Pattern.
8	Configure two SIP route patterns for your application points.	See Configuring a SIP Route Pattern.

Configuring CUCM on 2000-User Systems with No High Availability

This section describes the information required and detailed instructions on how to configure CUCM for 2000-user systems without high availability.

Information Required

- Two load balance points' IP addresses
- Three application points' IP addresses
- The number of call-in access numbers you will configure on your system

Configuration Procedure

Perform the following steps in the order presented:

Task	Description	Detailed Information
1	Review the existing SIP trunk security profile and determine whether or not it satisfies your Cisco WebEx Meetings Server setup requirement. If it does not, configure two SIP trunk security profiles.	Add a SIP trunk security profile for your load balance point and add a SIP trunk security profile for your application point. See Configuring a SIP Trunk Security Profile for a Load Balance Point, on page 7 and Configuring a SIP Trunk Security Profile for an Application Point, on page 8.
2	Review the existing SIP profile and determine whether or not it satisfies your Cisco WebEx Meetings Server setup requirement. If it does not, configure one SIP profile.	Configure a SIP profile as described in Configuring a TLS SIP Profile or Configuring an IPv6 SIP Profile, on page 10.
3	Configure two SIP trunks for your load balance points.	See Configuring a SIP Trunk Security Profile for a Load Balance Point, on page 7.
4	Configure three SIP trunks for your application points.	See Configuring a SIP Trunk Security Profile for an Application Point, on page 8.
5	Configure one route group using the SIP trunk that you configured for your load balance point in Task 3, above.	See Configuring a Route Group, on page 16.
6	Configure one route list using the route group that you configured in Task 5, above.	See Configuring a Route List, on page 17.
7	Configure *N* route patterns using the above route list. *N* is the number of call-in access numbers that you configured in your audio settings on the Administration site.	See Configuring a Route Pattern, on page 17.
8	Configure three SIP route patterns for your application points.	See Configuring a SIP Route Pattern, on page 18.

Configuring CUCM on 2000-User Systems with High Availability

This section describes the information required and detailed instructions on how to configure CUCM for 2000-user systems with high availability.

Information Required

- Two load balance points' IP addresses
- Four application points' IP addresses
- The number of call-in access numbers you will configure on your system

Configuration Procedure

Perform the following steps in the order presented:

Task	Description	Detailed Information
1	Review the existing SIP trunk security profile and determine whether or not it satisfies your Cisco WebEx Meetings Server setup requirement. If it does not, configure two SIP trunk security profiles.	Add a SIP trunk security profile for your load balance point and add a SIP trunk security profile for your application point. See Configuring a SIP Trunk Security Profile for a Load Balance Point, on page 7 and Configuring a SIP Trunk Security Profile for an Application Point, on page 8.
2	Review the existing SIP profile and determine whether or not it satisfies your Cisco WebEx Meetings Server setup requirement. If it does not, configure one SIP profile.	Configure a SIP profile as described in Configuring a TLS SIP Profile or Configuring an IPv6 SIP Profile, on page 10.
3	Configure two SIP trunks for your load balance points.	See Configuring a SIP Trunk Security Profile for a Load Balance Point, on page 7.
4	Configure four SIP trunks for your application points.	See Configuring a SIP Trunk Security Profile for an Application Point, on page 8.
5	Configure one route group using the SIP trunk that you configured for your load balance point in Task 3, above.	See Configuring a Route Group, on page 16.
6	Configure one route list using the route group that you configured in Task 5, above.	See Configuring a Route List, on page 17.
7	Configure *N* route patterns using the above route list. *N* is the number of call-in access numbers that you configured in your audio settings on the Administration site.	See Configuring a Route Pattern, on page 17.
8	Configure four SIP route patterns for your application points.	See Configuring a SIP Route Pattern, on page 18.

Configuring a SIP Trunk Security Profile

Configuring a SIP Trunk Security Profile for a Load Balance Point

Before You Begin

If your Cisco WebEx Meetings Server system is configured for TLS, you must import a secure teleconferencing certificate. For more information refer to the "Importing Secure Teleconferencing Certificates" section in the Administration Guide.

Procedure

Step 1 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Select **Cisco Unified CM Administration**.

Step 3 Select **System** > **Security** > **SIP Trunk Security Profile**.

Step 4 Select **Add New**.

Step 5 Configure the following fields.

- Name—Enter a name to identify your SIP trunk security profile.
- Device Security Mode— Select **No Secure** if you want CUCM to communicate with Cisco WebEx Meetings Server using UDP/TCP. Select **Encrypted** if you want CUCM to communicate with Cisco WebEx Meetings Server using TLS.
- X.509 Subject Name— Enter your certificate name if you want CUCM to communicate with Cisco WebEx Meetings Server using TLS.

  Note If you want CUCM to communicate with Cisco WebEx Meetings Server using TLS, a different Cisco WebEx Meetings Server system cannot share the same SIP Trunk Security Profile because each system must have a different certificate. Obtain the Cisco WebEx Meetings Server certificate name from the Administration site. For more information refer to "Managing Certificates" in the *Administration Guide*.
- Incoming Port— Enter 5060 if you want CUCM to communicate with Cisco WebEx Meetings Server using UDP/TCP. Enter 5061 if you want CUCM communicates Cisco WebEx Meetings Server using TLS.

Note Do not configure any of the other fields on the page. Leave them with their default settings.

Step 6 Select **Save**.

Configuring a SIP Trunk Security Profile for an Application Point

Before You Begin

If your Cisco WebEx Meetings Server system is configured for TLS, you must import a secure teleconferencing certificate. For more information refer to the "Importing Secure Teleconferencing Certificates" section in the *Administration Guide*.

Procedure

Step 1 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Select **Cisco Unified CM Administration**.

Step 3 Select **System** > **Security** > **SIP Trunk Security Profile**.

Step 4 Select **Add New**.

Step 5 Configure the following fields.

- Name—Enter a name to identify your SIP trunk security profile.
- Device Security Mode— Select **No Secure** if you want CUCM to communicate with Cisco WebEx Meetings Server using UDP/TCP. Select **Encrypted** if you want CUCM to communicate with Cisco WebEx Meetings Server using TLS.
- X.509 Subject Name— Enter your certificate name if you want CUCM to communicate with Cisco WebEx Meetings Server using TLS.

  Note If you want CUCM to communicate with Cisco WebEx Meetings Server using TLS, a different Cisco WebEx Meetings Server system cannot share the same SIP Trunk Security Profile because each system must have a different certificate. Obtain the Cisco WebEx Meetings Server certificate name from the Administration site. For more information refer to "Managing Certificates" in the *Administration Guide*.
- Incoming Port— Enter 5062 if you want CUCM to communicate with Cisco WebEx Meetings Server using UDP/TCP. Enter 5063 if you want CUCM to communicate with Cisco WebEx Meetings Server using TLS.

Note Do not configure any of the other fields on the page. Leave them with their default settings.

Step 6 Select **Save**.

Configuring a SIP Profile

Configuring a Standard SIP Profile

The standard SIP profile uses the default settings and requires no additional configuration steps.

Configuring a TLS SIP Profile

Procedure

Step 1 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Select **Cisco Unified CM Administration**.

Step 3 Select **Device** > **Device Settings** > **SIP Profile**.

Step 4 Select **Add New**.

Step 5 Configure the following fields:

- Name—Enter a name for your SIP profile.
- Redirect by Application—Select the check box.

Note Do not configure any of the other fields on the page. Leave them with their default settings.

Step 6 Select **Save**.

Configuring an IPv6 SIP Profile

Procedure

Step 1 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Select **Cisco Unified CM Administration**.

Step 3 Select **Device** > **Device Settings** > **SIP Profile**.

Step 4 Select **Add New**.

Step 5 Configure the following fields:

- Name—Enter a name for your SIP profile.
- Enable ENAT—Select the check box.

Note Do not configure any of the other fields on the page. Leave them with their default settings.

Step 6 Select **Save**.

Certificate Management

If you want CUCM to communicate with Cisco WebEx Meetings Server using TLS, you must perform the following actions:

- Obtain a Cisco WebEx Meetings Server certificate from the Administration site and then upload it to CUCM.

  Note If Cisco WebEx Meetings Server uses third-party certificates, then all certificates in the certificate chain need to be uploaded to CUCM.

- Download your CUCM certificate and then upload it to Cisco WebEx Meeting Server Administration site.

  Note If CUCM uses third-party certificates, then only the last certificate in the certificate chain (Root Certificate Authority (CA) certificate) needs to be uploaded to Cisco WebEx Meetings Server.

Refer to "Managing Certificates" in the *Administration Guide* for more information. See http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html for more details.

Uploading Cisco WebEx Meetings Server Certificates

Procedure

Step 1 Download and export your Cisco WebEx Meetings Server certificate.

a) Sign in to the Cisco WebEx Meetings Server Administration site.
b) Select **Settings** > **Security** > **Certificates**.
c) Copy the certificate name from the SSL Certificate section.
d) Select **More Options** > **Export SSL certificate**.
e) Save your certificate to your local hard drive.

Step 2 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 3 Select **Cisco Unified OS Administration**.

Step 4 Select **Security** > **Certificate Management**.

Step 5 Select **Upload Certificate/Certificate Chain**.

Step 6 Select **CallManager-trust** in the Certificate name drop-down menu.

Step 7 Select **Browse** button and select the certificate that you saved to your local hard drive.

Step 8 Select **Upload File**.

Wait for your system to indicate "Success: Certificate Uploaded."

Step 9 Select **Close**.

Installing a Third-Party CUCM Certificate

This procedure explains how to upload a third-party certificate to your Cisco WebEx Meetings Server.

Before You Begin

- Generate a Certificate Signing Request (CSR) and send it to a third part certificate authority to apply for certificates. See Generating a Certificate Signing Request (CSR) for instructions.
- The certificate authority will send you a certificate chain which can have the following:
  - Certificate 1 (end user) - issued to an end-user entity by an intermediate certificate authority.
  - Certificate 2 (intermediate) - issued to an intermediate certificate authority by a root certificate authority.
  - Certificate 3 (Root CA) - issued by the root certificate authority.
- When you receive multiple certificates in a certificate chain, you should concatenate the three certificates into one file, with the end user certificate first.

Procedure

Step 1 Import your third-party certificate file into you Cisco WebEx Meetings Server. See Importing a SSL Certificate for instructions.

Step 2 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 3 Select **Cisco Unified OS Administration**.

Step 4 Select **Security** > **Certificate Management**.

Step 5 Select **Upload Certificate/Certificate Chain**.

Step 6 Select **CallManager-trust** in the Certificate name drop-down menu.

Step 7 Select **Browse** button and select the Root Certificate Authority (CA) certificate that you saved to your local hard drive.
This is the last, self-signed certificate from the verification chain, which is used to verify the CallManager.pem certificate.

Note You can obtain the Root CA certificate from a certificate authority directly, at the same time the CallManager.pem certificate is created.

Step 8 Select **Upload File**.
Wait for your system to indicate "Success: Certificate Uploaded."

Step 9 Select **Close**.

What to Do Next

For more information about certificates, refer to the "Managing Certificates" section in the *Administration Guide* at http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.

Downloading CUCM Certificates

Refer to your CUCM documentation for more information on generating CUCM certificates.

Procedure

Step 1 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Select **Cisco Unified OS Administration**.

Step 3 Select **Security** > **Certificate Management**.

Step 4 Search for the certificate in "Certificate Name" field for the certificate with name "CallManager". Select the ".PEM File" field.

Step 5 Select **Download** to save the CUCM certificate (CallManager.pem) on your local hard drive.

What to Do Next

For more information on uploading CUCM certificates to Cisco WebEx Meetings Server, refer to "Managing Certificates" in the *Administration Guide*. See http://www.cisco.com/en/US/products/ps12732/products_installation_and_configuration_guides_list.html for more details.

Configuring a SIP Trunk

Configuring a SIP Trunk on a Load Balance Point

Procedure

Step 1 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Select **Cisco Unified CM Administration**.

Step 3 Select **Device** > **Trunk**.

Step 4 Select **Add New**.

Step 5 On the **Trunk Type** drop-down menu select **SIP Trunk**.

Note Do not change any other fields on this page. Leave them at their default settings.

Note Leave the **Media Termination Point Required** check box deselected on the **Trunk Configuration** page when CUCM is communicating with Cisco WebEx Meeting Server. If you are not using Cisco WebEx Meetings Server with CUCM SIP audio, you can select the **Media Termination Point Required** check box when providing telephony services using a third-party PBX infrastructure.

Step 6 Select **Next**.

Step 7 Configure the following fields:

- Device Name—Enter a name for the SIP trunk.
- Device Pool—Select an appropriate device pool from the drop-down menu.

  To determine which Cisco Unified Communications Manager Group has been configured on that device pool, select **System** > **Device Pool menu**. To verify which Cisco Unified Communications Managers are part of this group, select **System** > **Cisco Unified CM Group**.

  Note Record the IP addresses of the primary and secondary server. You will enter these IP addresses when you configure your audio settings in Cisco WebEx Meetings Server. See "Configuring Your Audio Settings for the First Time" in the *Administration Guide* for more details. See Cisco WebEx Meetings Server Install and Upgrade Guides.

- Destination Address—Enter your load balance point IPv4 address. Refer to the SIP Configuration table on your Administration Site Audio page the IP address.
- Destination Address IPv6—Enter your load balance point IPv6 address if you want to enable IPv6 between CUCM and Cisco WebEx Meetings Server.
- Destination Port—Enter 5060 if you want CUCM to communicate with Cisco WebEx Meetings Server using UDP/TCP. Enter 5061 if you want CUCM to communicate with Cisco WebEx Meetings Server using TLS.
- SIP Trunk Security Profile—Select your load balance point's security profile from the drop-down menu.
- SIP Profile—Select **Standard SIP Profile** if you want CUCM to communicate with Cisco WebEx Meetings Server using UDP/TCP. Select **TLS SIP Profile** if you want CUCM to communicate with Cisco WebEx Meetings Server using TLS. Select **IPv6 SIP Profile** if you want to enable IPv6 between CUCM and Cisco WebEx Meetings Server.
- Calling Search Space—Select a Calling Search Space that can call the phone numbers and route patterns configured in CUCM that you want Cisco WebEx Meetings Server to call out to. Select **Call Routing** > **Class of Control** > **Calling Search Space**. A calling search space consists of an ordered list of route partitions that are typically assigned to devices or route patterns. Calling search spaces determine the partitions that calling devices search when they are attempting to complete a call. For more information, refer to "Calling Search Space Configuration" in the *Cisco Unified Communications Manager Administration Guide* or "Partitions and Calling Search Spaces" in the *Cisco Unified Communications Manager System Guide*.
- Rerouting Calling Search Space—Select a Calling Search Space that contains the route partition that is configured for the SIP route pattern from the section below, "Configuring a SIP Route Pattern." If this is set to **< None >**, then this will only be able to route calls to route patterns with a route partition set to **< None >**, so the SIP route pattern will need to have the route partition set to **< None >**. This configuration is necessary to enter meetings in Cisco WebEx Meetings Server. For more information, refer to "Calling Search Space Configuration" in the *Cisco Unified Communications Manager Administration Guide* or "Partitions and Calling Search Spaces" in the *Cisco Unified Communications Manager System Guide* for more information.

Note Do not change any other fields on this page. Leave them at their default settings.

Step 8 Select **Save**.

Step 9 Select **Reset** and then select **Reset and Restart** in the pop-up window.
You must reset the SIP trunk to complete your configuration.

Configuring a SIP Trunk for an Application Point

Procedure

Step 1 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Select **Cisco Unified CM Administration**.

Step 3 Select **Device** > **Trunk**.

Step 4 Select **Add New**.

Step 5 On the **Trunk Type** drop-down menu select **SIP Trunk**.

Note Do not change any other fields on this page; leave the values at their default settings.

Step 6 Select **Next**.

Step 7 Configure the following fields:

- Device Name—Enter a name for your SIP trunk.
- Device Pool—Select **Default** from the drop-down menu.
- Destination Address—Enter the application server IPv4 address.
- Destination Address IPv6—Enter your application server IPv6 address if you want to enable IPv6 between CUCM and Cisco WebEx Meetings Server.
- Destination Port—Enter 5062 if you want CUCM to communicate with Cisco WebEx Meetings Server by using UDP/TCP. Enter 5063 if you want CUCM to communicate with Cisco WebEx Meetings Server by using TLS.
- SIP Trunk Security Profile—Select your application server security profile from the drop-down menu.
- SIP Profile—Select **Standard SIP Profile** if you want CUCM to communicate with Cisco WebEx Meetings Server by using UDP/TCP. Select **TLS SIP Profile** if you want CUCM to communicate with Cisco WebEx Meetings Server by using TLS. Select **IPv6 SIP Profile** if you want to enable IPv6 between CUCM and Cisco WebEx Meetings Server.
- Calling Search Space—Select a Calling Search Space that can call the phone numbers and route patterns configured in CUCM that you want to enable Cisco WebEx Meetings Server to call. Select **Call Routing** > **Class of Control** > **Calling Search Space**. A calling search space consists of an ordered list of route partitions that are typically assigned to devices or route patterns. Calling search spaces determine the partitions that calling devices search when they are attempting to complete a call. If this is set to **< None >**, this will only be able to call devices or route patterns with a partition set to **< None >**. For more information, refer to *Calling Search Space Configuration* in the *Cisco Unified Communications Manager*

Administration Guide or *Partitions and Calling Search Spaces* in the *Cisco Unified Communications Manager System Guide*.

Note Do not change any other fields on this page; leave the values at their default settings.

Note Leave the **Media Termination Point Required** check box deselected on the **Trunk Configuration** page when CUCM is communicating with Cisco WebEx Meeting Server. If you are not using Cisco WebEx Meetings Server with CUCM SIP audio, you can select the **Media Termination Point Required** check box when providing telephony services using a third-party PBX infrastructure.

Step 8 Select **Save**.

Step 9 Select **Reset** and then select **Reset and Restart** in the pop-up window.
You must reset the SIP trunk to complete the configuration.

Configuring a Route Group

Procedure

Step 1 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Select **Cisco Unified CM Administration**.

Step 3 Select **Call Routing** > **Route/Hunt** > **Route Group**.

Step 4 Select **Add New**.

Step 5 Configure the following fields

- Route Group Name—Enter a name for your route group.
- Distribution Algorithm. Select **Circular** in drop-down menu.
  Note By selecting **Circular**, you enable CUCM to distribute a call to idle or available users starting from the (N+1)th member of a route group, where the Nth member is the member to which CUCM most recently extended a call. If the Nth member is the last member of a route group, CUCM distributes a call starting from the top of the route group.
- Find Devices to Add to Route Group—Select **SIP trunk of Load Balance Point** in the Available Devices list. Then select **Add to Route Group**.

Note Do not change any other fields on this page. Leave them at their default settings.

Step 6 Select **Save**.

What to Do Next

Create a route list for your route group. Proceed to Configuring a Route List, on page 17.

Configuring a Route List

Procedure

Step 1 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Select **Cisco Unified CM Administration**.

Step 3 Select **Call Routing** > **Route/Hunt** > **Route List**.

Step 4 Select **Add New**.

Step 5 Configure the following fields

- Name—Enter a name for your route list.
- Cisco Unified Communications Manager Group—Select **Default** in drop-down menu.

Note Do not change any other fields on this page. Leave them at their default settings.

Step 6 Select **Save**.

Step 7 Select **Add Route Group**.
The **Route List Detail Configuration** page appears.

Step 8 Select the previously configured route group from **Route Group** drop-down menu and select **Save**.
The **Route List Configuration** page appears.

Step 9 Select **Save**.

What to Do Next

Configure a route pattern for your route list. Proceed to Configuring a Route Pattern, on page 17.

Configuring a Route Pattern

Procedure

Step 1 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Select **Cisco Unified CM Administration**.

Step 3 Select **Call Routing** > **Route/Hunt** > **Route Pattern**.

Step 4 Select **Add New**.

Step 5 Configure the following fields

- Route Pattern—Enter a name for your route pattern.
- Route Partition—Select a route partition that is accessible by phones or devices that can call Cisco WebEx Meetings Server. If this set to **< None >** any device configured in CUCM would be able to call

Cisco WebEx Meetings Server. For more information, refer to "Calling Search Space Configuration" in the *Cisco Unified Communications Manager Administration Guide* or "Partitions and Calling Search Spaces" in the *Cisco Unified Communications Manager System Guide*.

- Gateway/Route List—Select the previously configured route list from the drop-down menu.

Note Do not change any other fields on this page. Leave them at their default settings.

Step 6 Select **Save**.

Configuring a SIP Route Pattern

Procedure

Step 1 Sign in to http://ccm-server/, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Select **Cisco Unified CM Administration**.

Step 3 Select **Call Routing** > **SIP Route Pattern**.

Step 4 Select **Add New**.

Step 5 Configure the following fields

- Route Partition—Select a route partition that is included in the calling search space that is configured as the Rerouting Calling Search Space from the section "Configuring a SIP Trunk for an Application Point" above. If this set to **< None >** then the Rerouting Calling Search Space configured for the SIP trunk for an application point must be set to **< None >**. For more information refer to "Calling Search Space Configuration" in the *Cisco Unified Communications Manager Administration Guide* or "Partitions and Calling Search Spaces" in the *Cisco Unified Communications Manager System Guide*.
- Pattern Usage—Select **IP Address Routing**.
- IPv4 Pattern—Enter the application point IP address. Refer to the SIP Configuration table on your Administration Site Audio page the IP address.
- SIP Trunk—Select the previously configured SIP trunk for the application point from the drop-down menu.

Note Do not change any other fields on this page. Leave them at their default settings.

Step 6 Select **Save**.

CUCM Feature Compatibility and Support

The following tables provide feature compatibility information for the supported versions of CUCM.

CUCM Feature Compatibility

Cisco WebEx Meetings Server supports CUCM 7.1, 8.6, 9.0, and 9.1.

The following table provides feature compatibility for the supported versions of CUCM. Cisco WebEx Meetings Server system capacity is not affected by any of your configuration choices.

Note Cisco WebEx Meetings Server does not support any unlisted CUCM versions or other third-party SIP proxy management applications.

Feature	CUCM 7.1	CUCM 8.6	CUCM 9.0-9.1	Pre-Conditions/Remarks
Call out (IPv6)	Yes	Yes	Yes	Configure your Cisco WebEx Meetings Server system with IPv6 addresses during installation process.
Call in (IPv6)	Yes	Yes	Yes	Configure your Cisco WebEx Meetings Server system with IPv6 addresses during installation process.
TLS/SRTP	Yes	Yes	Yes	Configure your Cisco WebEx Meetings Server system with security certificates.
RFC2833	Yes	Yes	Yes	Select this option during CUCM SIP trunk configuration.
KPML	Yes	Yes	Yes	Select this option during CUCM SIP trunk configuration.
Keepalive—Cisco WebEx Meetings Server sending	Yes	Yes	Yes	Performed using the SIP OPTIONS message.
Keepalive—Cisco WebEx Meetings Server receiving	No	Yes	Yes	Performed using the SIP OPTIONS message.
Quality of Service	Yes	Yes	Yes	For control packets.

Feature	CUCM 7.1	CUCM 8.6	CUCM 9.0-9.1	Pre-Conditions/Remarks
TCP	Yes	Yes	Yes	Make sure your default ports are configured as follows: 5060 for conferencing load balance points; 5062 for conferencing application points.
TLS	Yes	Yes	Yes	Make sure your default ports are configured as follows: 5061 for conferencing load balance points; 5063 for conferencing application points.
UDP	Yes	Yes	Yes	Make sure your default ports are configured as follows: 5060 for conferencing load balance points; 5062 for conferencing application points.
Self-signed certificates	Yes	Yes	Yes	n/a
Third-party certificates	Yes	Yes	Yes	n/a

Telephony Call Features

Cisco WebEx Meetings Server supports the following CUCM call features.

Note The CUCM 9.0 software that is part of the BE6K (Business Edition 6000) product is also supported by Cisco WebEx Meetings Server.

Feature	CUCM 7.1	CUCM 8.6	CUCM 9.0-9.1
Call hold	Yes	Yes	Yes
Call un-hold	Yes	Yes	Yes
Caller ID display on EP	Yes	Yes	Yes
Calling name display on EP	Yes	Yes	Yes

Feature	CUCM 7.1	CUCM 8.6	CUCM 9.0-9.1
Call transfer (IPv4 to IPv4)	Yes	Yes	Yes
Call transfer (IPv6 to IPv4)	Yes	Yes	Yes
Call transfer (IPv4 to IPv6)	No	No	Yes
Call transfer (IPv6 to IPv6)	No	No	Yes

Telephony Media Features

Cisco WebEx Meetings Server supports participants with G.711/G.722/G.729 codecs at the same time. Changing your codec configuration does not affect system performance.

Feature	G.711	G.722	G.729
Noise Compression	Yes	Yes	Yes
Comfort noise	Yes	No	No
Echo cancellation	No	No	No
Packet loss concealment	Yes	Yes	No
Automatic gain control	Yes	Yes	Yes
Quality of Service	Yes	Yes	Yes