Configuring Cisco Unified Communications Manager (CUCM)

Configuring Cisco Unified Communications Manager (CUCM)

Configure call control settings with CUCM. You must configure one CUCM system to manage call control but you can optionally configure a second CUCM system for audio high availability.

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

Configuring a single CUCM system (no audio high availability) requires the following:

- To call in to your Cisco WebEx Meetings Server system from CUCM, you must configure a call-in route pattern on your conferencing load balancer servers and several SIP route patterns on your conferencing application servers. A call-in route pattern enables CUCM to route calls based on a dial-in

phone number that you configure. SIP route patterns are telephony call route patterns that enable CUCM to route calls based on the SIP URL in the SIP messages of calls that are placed.

Note The call-in route pattern number is also the number you use as your call-in access number when you configure your audio features in the Administration site. Make sure to configure your port numbers as described in the following sections.

  - Configure several SIP trunks pointing to your Cisco WebEx Meetings Server conferencing load balancers and configure a route group, a route list, and a route pattern.
  - Configure several SIP trunks pointing to your Cisco WebEx Meetings Server conferencing application servers and configure several SIP route patterns.

- To call out to CUCM from Cisco WebEx Meetings Server:
  - Sign in to the Administration site and configure your CUCM settings. Refer to "Configuring Your Audio Settings for the First Time" in the Administration Guide for more information.

Note CUCM requires that the conference application server is configured on CUCM as a SIP trunk. Otherwise it will reject messages from the application server.

CUCM Feature Compatibility and Support

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

CUCM Feature Compatibility

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	Pre-Conditions/Remarks
Call out (IPv6)	Yes	Yes	Yes	Configure your Cisco WebEx Meetings Server system with IPv6 addresses during installation process.

Feature	CUCM 7.1	CUCM 8.6	CUCM 9.0	Pre-Conditions/Remarks
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.
TCP	Yes	Yes	Yes	Make sure your default ports are configured as follows: 5060 for conferencing load balancer servers; 5062 for conferencing application servers.
TLS	Yes	Yes	Yes	Make sure your default ports are configured as follows: 5061 for conferencing load balancer servers; 5063 for conferencing application servers.

Feature	CUCM 7.1	CUCM 8.6	CUCM 9.0	Pre-Conditions/Remarks
UDP	Yes	Yes	Yes	Make sure your default ports are configured as follows: 5060 for conferencing load balancer servers; 5062 for conferencing application servers.
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
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
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

CUCM Base Configuration

You must create some base CUCM configurations to manage calls for your Cisco WebEx Meetings Server system. Multiple systems can share the same base configuration. Your base configuration consists of the following:

- SIP trunk security profile
- SIP profile

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
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

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)
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 a SIP Trunk Security Profile

Configuring a SIP Trunk Security Profile for a Load Balancer Server

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 communicate 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 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 Server

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 communicate 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 Cisco WebEx Meetings Server using UDP/TCP. Enter 5063 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 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**.

CUCM Specific Configuration

The following CUCM configurations must be made for individual Cisco WebEx Meetings Server systems. These configurations cannot be shared by multiple systems.

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

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

Refer to "Managing Certificates" in the online help and *Administration Guide* for more information.

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**.

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 online help and *Administration Guide*.

Configuring a SIP Trunk

Configuring a SIP Trunk on a Load Balancer Server

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.

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 your load balancer server IPv4 address.
- Destination Address IPv6—Enter your load balancer server 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 balancer server's security profile from the drop-down menu.
- SIP Profile—Select **Standard SIP Profile** if you want CUCM communicates 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.

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 Server

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.

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 your load balancer server IPv4 address.
- Destination Address IPv6—Enter your load balancer 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 using UDP/TCP. Enter 5063 if you want CUCM to communicate with Cisco WebEx Meetings Server using TLS.
- SIP Trunk Security Profile—Select your load balancer server's security profile from the drop-down menu.
- SIP Profile—Select **Standard SIP Profile** if you want CUCM communicates 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.

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 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 Balancer Server** 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 13.

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 14.

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.
- 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

- Pattern Usage—Select **IP Address Routing**.
- IPv4 Pattern—Enter the application server IP address.
- SIP Trunk—Select the previously configured SIP trunk for the application server 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 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 balancer server's IP address
- One application server's IP address
- 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 balancer server and add a SIP trunk security profile for your application server. See Configuring a SIP Trunk Security Profile for a Load Balancer Server, on page 6 and Configuring a SIP Trunk Security Profile for an Application Server, on page 7.
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 8.
3	Configure one SIP trunk for your load balancer server.	See Configuring a SIP Trunk Security Profile for a Load Balancer Server, on page 6.
4	Configure one SIP trunk for your application server.	See Configuring a SIP Trunk Security Profile for an Application Server, on page 7.
5	Configure one route group using the SIP trunk that you configured for your load balancer server in Task 3, above.	See Configuring a Route Group, on page 13.
6	Configure one route list using the route group that you configured in Task 5, above.	See Configuring a Route List, on page 13.
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 14.
8	Configure one SIP route pattern for your application server.	See Configuring a SIP Route Pattern, on page 15.

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 balancer servers' IP addresses
- Two application servers' 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 balancer server and add a SIP trunk security profile for your application server. See Configuring a SIP Trunk Security Profile for a Load Balancer Server, on page 6 and Configuring a SIP Trunk Security Profile for an Application Server, on page 7.
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 8.
3	Configure two SIP trunks for your load balancer servers.	See Configuring a SIP Trunk Security Profile for a Load Balancer Server, on page 6.
4	Configure two SIP trunks for your application servers.	See Configuring a SIP Trunk Security Profile for an Application Server, on page 7.
5	Configure one route group using the SIP trunk that you configured for your load balancer server in Task 3, above.	See Configuring a Route Group, on page 13.
6	Configure one route list using the route group that you configured in Task 5, above.	See Configuring a Route List, on page 13.
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 14.
8	Configure two SIP route patterns for your application servers.	See Configuring a SIP Route Pattern, on page 15.

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 balancer servers' IP addresses
- Three application servers' 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 balancer server and add a SIP trunk security profile for your application server. See Configuring a SIP Trunk Security Profile for a Load Balancer Server, on page 6 and Configuring a SIP Trunk Security Profile for an Application Server, on page 7.
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 8.
3	Configure two SIP trunks for your load balancer servers.	See Configuring a SIP Trunk Security Profile for a Load Balancer Server, on page 6.
4	Configure three SIP trunks for your application servers.	See Configuring a SIP Trunk Security Profile for an Application Server, on page 7.
5	Configure one route group using the SIP trunk that you configured for your load balancer server in Task 3, above.	See Configuring a Route Group, on page 13.
6	Configure one route list using the route group that you configured in Task 5, above.	See Configuring a Route List, on page 13.
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 14.
8	Configure three SIP route patterns for your application servers.	See Configuring a SIP Route Pattern, on page 15.

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 balancer servers' IP addresses
- Four application servers' 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 balancer server and add a SIP trunk security profile for your application server. See Configuring a SIP Trunk Security Profile for a Load Balancer Server, on page 6 and Configuring a SIP Trunk Security Profile for an Application Server, on page 7.
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 8.
3	Configure two SIP trunks for your load balancer servers.	See Configuring a SIP Trunk Security Profile for a Load Balancer Server, on page 6.
4	Configure four SIP trunks for your application servers.	See Configuring a SIP Trunk Security Profile for an Application Server, on page 7.
5	Configure one route group using the SIP trunk that you configured for your load balancer server in Task 3, above.	See Configuring a Route Group, on page 13.
6	Configure one route list using the route group that you configured in Task 5, above.	See Configuring a Route List, on page 13.
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 14.
8	Configure four SIP route patterns for your application servers.	See Configuring a SIP Route Pattern, on page 15.