Configuring Cisco Unified Communications Manager (CUCM)

Configuring Cisco Unified Communications Manager

To enable teleconferencing on Cisco Webex Meetings Server you must configure one (or more) Cisco Unified Communications Manager (CUCM) system to manage call control. Optionally you can configure a second CUCM system for audio high availability.

CUCM in an MDC Environment

The CUCM configurations in a Multi-data Center (MDC) environment are the same as in a Single-data Center (SDC) environment. Configuration parameters modified on one data center are automatically matched on the other data center.

On CUCM, the basic configurations in a Multi-data Center (MDC) environment are the same as in a Single-data Center (SDC) environment. However, you must configure trunks to all data centers. Each data center can have a different route pattern. If you want to use more than one CUCM, each data center must have a SIP trunk to the CUCM in the other data centers for calls to transfer.

CUCM Secure Teleconferencing in an MDC Environment

It is not possible to import certificates from all data centers in a Multi-data Center (MDC) into a single Cisco Unified Call Manager (CUCM) as needed to secure teleconferencing when the common name of both certificates is the same.

By default, the common name for all data centers is the global site URL of the system. However, to make the common name unique, you can generate certificates. For more information, see Generating a Certificate Signing Request (CSR), on page 16. Select the local site URL instead of the global site URL to use in the common name.

Self-signed certificates generated during any system altering procedure (such as changing the site or administration URL, changing hostnames) results in a certificate that has the global site URL in the common name, so you must manually create certificates with the local site URL after this type of operation.

CUCM Configuration for Extended Systems

When you extend a large system, you must configure another SIP Trunk for each new media server that you add. A large system requires 3 SIP Trunks, so an extra large system requires 4–6, depending on the numbe of extension units.

Before You Begin

Obtain your Load Balancer Point and Application Point information from your Cisco Webex Meetings Server **Audio** page. 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. Sign into your Administration site and select **Settings** > **Audio** to see this information.

- 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

CUCM Configuration Checklist for Multi-data Center

The configuration checklist displays the number of each Cisco Unified Communication Manager (CUCM) configuration type that you must configure for your system with Multi-data Center (MDC).

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	4	1	1	N	2
800 users	2	1	4	1	1	N	2
2000 users with HA	2	1	6	1	1	N	4

CUCM Configuration Checklist with or without High Availability

The configuration checklist displays the number of each Cisco Unified Communication Manager (CUCM) configuration type that you must configure for your Single-data Center (SDC) system with or without High Availability (HA).

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

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 with HA	2	1	4	1	1	N	2
250 users	2	1	2	1	1	N	1
250 users with HA	2	1	4	1	1	N	2
800 users	2	1	2	1	1	N	1
800 users with HA	2	1	4	1	1	N	2
2000 users	2	1	5	1	1	N	3
2000 users with HA	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 in a CWMS Multi-data Center System

Typically, each site in a Multi-data Center (MDC) environment has a dedicated CUCM cluster associated with it. CUCM clusters are connected by using inter-cluster trunks (ICT). Each CUCM cluster has call-in/in-dial trunks to the local CWMS site. Session Manager Edition (SME) is supported. CWMS can be configured behind the local CUCM clusters. Each CUCM has SIP REFER trunks to all the media virtual machines in the MDC.

For redundancy, each CUCM cluster can have INVITE trunks to all the data centers. The call-in route pattern gives priority to the INVITE trunk associated with the local data center and uses the INVITE trunk to the remote data center only upon failure.

Note The Extended Capacity feature is not supported in an MDC deployment.

Table 1: CUCM SIP Trunks Configured on Each CUCM Cluster

Deployment	INVITE Trunks - Load Balancer (MACC)	REFER Trunks—Application Point (TAS)
Small	2	2
Medium	2	2
Large	4	6

Configuring CUCM on a 250- or 800-user Multi-data Center System

Configure Cisco Unified Communication Manager (CUCM) for 250- or 800-user Multi-data Center systems. Typically, each data center has a local CUCM cluster.

Before you begin

Collect the following information:

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

Procedure

Step 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 11 and Configuring a SIP Trunk Security Profile for an Application Point, on page 12.

Step 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 13.

Step 3 Configure two SIP trunks for your load balance points.

See Configuring a SIP Trunk on a Load Balance Point.

Step 4 Configure two SIP trunks for your application points.

See Configuring a SIP Trunk for an Application Point.

Step 5 Configure one route group by using the SIP trunk that you configured for your load balance point.

See Configuring a Route Group.

Step 6 Configure one route list by using the route group that you configured in the previous step.

See Configuring a Route List.

Step 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.

Step 8 Configure two SIP route patterns for your application points.

See Configuring a SIP Route Pattern.

Configuring CUCM on a 2000-user Multi-data Center System

Configure Cisco Unified Communication Manager (CUCM) for a 2000-user Multi-data Center (MDC) system. Typically, each data center has a local CUCM cluster.

Before you begin

Information required:

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

Procedure

Step 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 11 and Configuring a SIP Trunk Security Profile for an Application Point, on page 12.

Step 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 13.

Step 3 Configure two SIP trunks for your load balance points.

See Configuring a SIP Trunk on a Load Balance Point.

Step 4 Configure four SIP trunks for your application points.

See Configuring a SIP Trunk for an Application Point.

Step 5 Configure one route group by using the SIP trunk that you configured for your load balance point.

See Configuring a Route Group.

Step 6 Configure one route list by using the route group that you configured in the previous step.

See Configuring a Route List.

Step 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.

Step 8 Configure four SIP route patterns for your application points.

See Configuring a SIP Route Pattern.

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 without High Availability

Configure CUCM for 50-, 250-, and 800-user systems without High Availability.

Before you begin

Obtain the following information:

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

Procedure

Step 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 11 and Configuring a SIP Trunk Security Profile for an Application Point, on page 12.

Step 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 13.

Step 3 Configure one SIP trunk for your load balance point.

See Configuring a SIP Trunk on a Load Balance Point.

Step 4 Configure one SIP trunk for your application point.

See Configuring a SIP Trunk for an Application Point.

Step 5 Configure one route group by using the SIP trunk that you configured for your load balance point.

See Configuring a Route Group.

Step 6 Configure one route list by using the route group that you configured in the previous step.

See Configuring a Route List.

Step 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.

Step 8 Configure two SIP route patterns for your application points.

See Configuring a SIP Route Pattern.

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

This section describes the information required and detailed instructions on how to configure CUCM for 50-, 250-, or 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 11 and Configuring a SIP Trunk Security Profile for an Application Point, on page 12.
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 13.
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.

Task	Description	Detailed Information
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 a 2000-User System without High Availability

Configure Cisco Unified Communication Manager (CUCM) for a 2000-user system without High Availability.

Before you begin

Obtain the following information:

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

Procedure

Step 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 11 and Configuring a SIP Trunk Security Profile for an Application Point, on page 12.

Step 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 13.

Step 3 Configure two SIP trunks for your load balance point.

See Configuring a SIP Trunk on a Load Balance Point.

Step 4 Configure three SIP trunks for your application point.

See Configuring a SIP Trunk for an Application Point.

Step 5 Configure one route group by using the SIP trunk that you configured for your load balance point.

See Configuring a Route Group.

Step 6 Configure one route list by using the route group that you configured in the previous step.

See Configuring a Route List.

Step 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.

Step 8 Configure two SIP route patterns for your application points.

See Configuring a SIP Route Pattern.

What to do next

Configuring CUCM on a 2000-User System with High Availability

Configure Cisco Unified Communication Manager (CUCM) for a 2000-user system with High Availability.

Before you begin

Obtain the following information:

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

Procedure

Step 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 11 and Configuring a SIP Trunk Security Profile for an Application Point, on page 12.

Step 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 13.

Step 3 Configure two SIP trunks for your load balance points.

See Configuring a SIP Trunk on a Load Balance Point.

Step 4 Configure four SIP trunks for your application points.

See Configuring a SIP Trunk for an Application Point.

Step 5 Configure one route group by using the SIP trunk that you configured for your load balance point.

See Configuring a Route Group.

Step 6 Configure one route list by using the route group that you configured in the previous step.

See Configuring a Route List.

Step 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.

Step 8 Configure two SIP route patterns for your application points.

See Configuring a SIP Route Pattern.

What to do next

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 *Cisco Webex Meetings Server Administration Guide* at http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html.

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 by using UDP/TCP. Select **Encrypted** if you want CUCM to communicate with Cisco Webex Meetings Server by using TLS.
- X.509 Subject Name— Enter your certificate name if you want CUCM to communicate with Cisco Webex Meetings Server by using TLS.

Note If you want CUCM to communicate with Cisco Webex Meetings Server by 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 the 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 *Cisco Webex Meetings Server Administration Guide* at http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html.

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 **Non Secure** if you want CUCM to communicate with Cisco Webex Meetings Server by using UDP/TCP. Select **Encrypted** if you want CUCM to communicate with Cisco Webex Meetings Server by using TLS.
- X.509 Subject Name— Enter your certificate name if you want CUCM to communicate with Cisco Webex Meetings Server by using TLS.

  Note If you want CUCM to communicate with Cisco Webex Meetings Server by 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 by using UDP/TCP. Enter `5063` if you want CUCM to communicate with Cisco Webex Meetings Server by using TLS.

Note Do not configure any of the other fields on the page; leave the default settings.

Step 6 Select **Save**.

Configuring a SIP Profile

Configuring a Standard SIP Profile

The standard Session Initiation Protocol (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 Click **Cisco Unified CM Administration**.

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

Step 4 Click **Add New**.

Step 5 Configure the following fields:

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

Do not configure any of the other fields on the page; leave the fields with their default settings.

Step 6 Click **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 Click **Cisco Unified CM Administration**.

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

Step 4 Click **Add New**.

Step 5 Configure the following fields:

- Name—Enter a name for your SIP profile.

- Enable ENAT—Select the check box.

Do not configure any of the other fields on the page; leave the fields with their default settings.

Step 6 Click **Save**.

CUCM Certificate Management by Using TLS

If you want Cisco Unified Communications Manager (CUCM) to communicate with Cisco Webex Meetings Server (CWMS) by using TLS, you must perform the following actions:

- Obtain a CWMS certificate from the Application site and upload it to CUCM.

Note If CWMS uses third-party certificates, all certificates in the certificate chain must be uploaded to CUCM.

- Download your CUCM certificate, and then upload it to CWMS Administration site.

Note If CUCM uses third-party certificates, only the last certificate in the certificate chain (Root Certificate Authority (CA) certificate) must be uploaded to CWMS.

If you use TLS to connect all the data centers in a Multi-data Center (MDC) system to the same CUCM, CWMS cannot use the common site URL for the certificate common name. You must use each data center local site URL for each certificate common name, because the CUCM 10.5 and older versions treat multiple certificates with a common name as same certificate. If the names are not different, the second data center certificate replaces the first data center certificate after uploading the second data center certificate into CUCM.

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 Click **Cisco Unified OS Administration**.

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

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

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

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

Step 8 Click **Upload File**.

The system displays a "Success: Certificate Uploaded" message.

Step 9 Click **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.

The certificate authority sends you a certificate chain that can have the following:

- Certificate 1 (user) - issued to a 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, concatenate the three certificates into one file, with the user certificate first.

Procedure

Step 1 Import your third-party certificate file into your Cisco Webex Meetings Server as described in the *Cisco Webex Meetings Server Administration Guide* available from http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.

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 *Cisco Webex Meetings Server Administration Guide* at http://www.cisco.com/en/US/products/ps12732/prod_installation_guides_list.html.

Downloading CUCM Certificates

This procedure is required only if CUCM uses self-signed certificates. If CUCM uses third party certificates, upload only the last certificate (Root CA certificate) in the certificate chain to your Cisco Webex Meeting Server. Contact your Certificate Authority (CA) for information about how to obtain a Root CA certificate.

For more information about generating CUCM certificates, see the CUCM documentation.

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 Click **Cisco Unified OS Administration**.

Step 3 Click **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 Click **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.

Generating a Certificate Signing Request (CSR)

The hashing method used to generate Certificate Signing Request (CSR) and private key for SSL certificates uses SHA2 (SHA256).

Procedure

Step 1 Sign in to Webex Site Administration.

In a Multidata Center system, the DNS determines which data center Dashboard appears. Use this Dashboard to manage all the data centers in this system.

Step 2 Click **Settings** > **Security** > **Certificates** > **Certificates on CWMS System**.

On a Multi-data Center system, continue with **Certificates on CWMS System or Certificates on Datacenter *N***

Step 3 Click **Generate CSR** for the desired type of CSR.

On November 1, 2015, Certification Authorities (e.g. VeriSign, GoDaddy, and so forth) stopped issuing certificates for internal domain names (e.g. domain.local , domain.internal). Before CWMS version 2.0MR9, you could upload only a single SSL certificate with Subject Alternative Names for all components in the deployment, but this requires you to purchase expensive SAN SSL certificates for a complete solution. As of CWMS version 2.5MR5 you can purchase on Webex Site URL SSL a certificate from Certification Authority for use on IRP servers, and use Self-signed SSL certificates for the internal network virtual machines.

Step 4 Complete the fields on the **Generate CSR (Certificate Signing Request)** page.

Option	Description
Common Name	Click **Local Site URL** certificate, **Global Site URL** certificate, or **Wildcard** certificate.
Subject Alternative Names This option appears only if you select **Subject Alternative Name** for your Common Name type.	Your administration site and virtual machine names. No subject alternative names are required if you selected a wildcard common name.
Organization	Enter the organization name.
Department	Enter the department name.
City	Enter the city.
State/Province	Enter the state or province.
Country	Click the country.
Key Size	Click the key size.2048.
Hash Algorithm	Click the Hash Algorithm SHA256.

Step 5 Click **Generate CSR**.

The **Download CSR** dialog box appears.

Step 6 Click **Download**.

You receive a ZIP file that contains the CSR and the associated private key. The CSR file is called `csr.pem` and the private key file is called `csr_private_key.pem`.

Step 7 Back up your system by using VMware Data Recovery or VMware vSphere Data Protection.

Backing up your system preserves the private key if it becomes necessary to restore it.

Configuring a SIP Trunk

Note When deploying a 2000-user system with High Availability (HA) and multiple load balance and application points, each load balancer and application point in the CWMS solution requires a dedicated SIP trunk. Multiple destination IP addresses within the same SIP trunk are not supported.

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 Click **Cisco Unified CM Administration**.

Step 3 Click **Device** > **Trunk**.

Step 4 Click **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 parameters at their default settings.

Media Termination Point Required should be unchecked 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, select **Media Termination Point Required** when providing telephony services by using a third-party PBX infrastructure.

Step 6 Click **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, go to **System** > **Device Pool menu**. To verify which Cisco Unified Communications Managers are part of this group, go to **System** > **Cisco Unified CM Group**.

  Note Record the IP addresses of the primary and secondary server. These IP addresses are entered 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 for 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 a security profile for your load balance point, 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. Go to **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 and Out-Of-Dialog Refer Calling Search Space—Select a Calling Search Space and Out-Of-Dialog Refer Calling Search Space that contains the route partition that is configured for the SIP route pattern. See Configuring a SIP Route Pattern. If it is set to **< None >**, then the system only routes calls to route patterns with the route partition set to **< None >**, so the SIP route pattern must 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 the parameters at their default settings.

Step 8 Click **Save**.

Step 9 Click **Reset** and then select **Reset and Restart** in the popup window.

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 Click **Cisco Unified CM Administration**.

Step 3 Click **Device** > **Trunk**.

Step 4 Click **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 Click **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—Optionally enter the application server IPv6 address 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.

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 Click **Save**.

Step 9 Click **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 Click **Cisco Unified CM Administration**.

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

Step 4 Click **Add New**.

Step 5 Configure the following fields

- Route Group Name—Enter a name for your route group.
- Distribution Algorithm. Select **Circular** from the 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** from the **Available Devices** list. Then click **Add to Route Group**.

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

Step 6 Click **Save**.

What to do next

Create a route list for your route group. Proceed to Configuring a Route List, on page 21.

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 Click **Cisco Unified CM Administration**.

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

Step 4 Click **Add New**.

Step 5 Configure the following fields

- Name—Enter a name for your route list.

- Cisco Unified Communications Manager Group—Select **Default** from the drop-down menu.

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

Step 6 Click **Save**.

Step 7 Click **Add Route Group**.

The **Route List Detail Configuration** page appears.

Step 8 Select the previously configured route group from the **Route Group** drop-down menu, and the click **Save**.

The **Route List Configuration** page appears.

Step 9 Click **Save**.

What to do next

Configure a route pattern for your route list. Proceed to Configuring a Route Pattern, on page 22.

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 Click **Cisco Unified CM Administration**.

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

Step 4 Click **Add New**.

Step 5 Configure the following fields

- **Route Pattern**—Enter a name for your route pattern.

  Note Add a route pattern for each Blast Dial group. Record this name because you must enter it on the Administration **Settings** > **Audio** > **Blast Dial Group** page when you create a Blast Dial group.

- **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 these fields at their default settings.

Step 6 Click **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 Click **Cisco Unified CM Administration**.

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

Step 4 Click **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. See the SIP Configuration table on the Audio page in Webex Site Administration, to locate 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 these fields at their default settings.

Step 6 Click **Save**.

IP Addressing Mode Preferences

You can configure IP Addressing Mode Preferences globally, or make the preferences device specific by creating a Common Device Configuration.

To configure global settings, go to **System** > **Enterprise Parameters**. Configure your preferences on the **CUCM Enterprise Parameters** page.

To make the configuration device specific, go to **Device** > **Common Device Configuration**. Configure your preferences on the **CUCM Common Device Configuration** page.

Save the configuration, which you can later select when you create the trunks for CWMS.

Important CWMS supports either the IPv4 or IPv6 setting for **IP Addressing Mode Preference for Media**.

CWMS doesn't support the IPv6IP setting for **Addressing Mode Preference for Signaling**. CWMS supports only IPv4 for SIP Signaling. Setting **IP Addressing Mode Preference for Signaling** to use IPv6 disables the connection between CUCM and CWMS, and therefore disables teleconferencing.

CUCM Feature Compatibility and Support

CUCM Feature Compatibility

Cisco Webex Meetings Server (CWMS) supports Cisco Unified Call Manager (CUCM) 8.6 or 9.0 without TLS/SRTP, and CUCM 9.1, 10.0, 10.5, 11.0(1a), 11.5, 11.5(1)SU1 and later service updates (SU), and 12.0SU1 and later SUs.

For a list of CUCM releases tested with CWMS, see the *Release Notes for Cisco Webex Meetings Server* for your release.

Important TLS connections between CUCM and CWMS fail with releases of CUCM that do not support certificates that are signed with a signature algorithm SHA256 with RSA encryption.

Upgrade CUCM to a version that supports this signature algorithm or obtain a third-party certificate that is signed with SHA1 with RSA encryption. According to the latest National Institute of Standards and Technology (NIST) recommendation, SHA1 should no longer be used for digital signature generation as this has a security vulnerability.

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 CWMS does not support any unlisted CUCM versions or other third-party SIP proxy management applications.

Table 2: Feature Compatibility for the Supported Versions of CUCM

Feature	Pre-Conditions/Remarks
Call out (IPv6)	Configure CWMS with IPv6 addresses during the installation process.
Call in (IPv6)	Configure CWMS with IPv6 addresses during the installation process.
TLS/SRTP	Configure CWMS system security certificates.
RFC2833	Select this option during CUCM SIP trunk configuration.
KPML	Select this option during CUCM SIP trunk configuration.

Feature	Pre-Conditions/Remarks
Keepalive—CWMS sending	Performed by using the SIP OPTIONS message.
Keepalive—CWMS receiving	Performed by using the SIP OPTIONS message.
Quality of Service	Control packets.
TCP	Make sure that your default ports are: 5060 for conferencing load balance points; 5062 for conferencing application points.
TLS	Make sure that your default ports are: 5061 for conferencing load balance points; 5063 for conferencing application points.
UDP	Make sure that your default ports are: 5060 for conferencing load balance points; 5062 for conferencing application points.
Self-signed certificates	n/a
Third-party certificates	n/a

Supported Telephony Call Features

Note The CUCM 9.0 software that is part of the BE6K (Business Edition 6000) product is supported by CWMS.

- Call hold
- Call un-hold
- Caller ID display on EP
- Calling name display on EP
- Call transfer (IPv4 to IPv4)
- Call transfer (IPv6 to IPv4)
- Call transfer (IPv4 to IPv6)
- Call transfer (IPv6 to IPv6)

Telephony Media Features

CWMS supports participants with G.711, G.722, and G.729 codecs at the same time. Changing your codec configuration does not affect system performance. Packet sizes supported on CWMS:

- 10, 20, or 30ms for g.711 audio codecs
- 20ms for g.722 audio codec
- 10, 20, 30, 40, 50, or 60ms for g.729 audio codecs

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

Note All custom audio prompts, including Blast Dial prompts, are: 8KHz, 16-bit, 64kbps, momo, CCITT u-law (G.711).

Audio Endpoint Compatibility

You can use any standards-based audio endpoint that connects to Cisco Unified Communications Manager to join a Webex meeting. The supported audio endpoints include the Cisco IP Phones, Telepresence endpoints, and PSTN devices such as mobile phones and land line phones. Many audio endpoints support audio and video connectivity. However, only audio connectivity to the Cisco Webex Meetings Server is supported.

To permit users to join Webex meetings by using PSTN devices, you must deploy Analog-to-VoIP Gateways, such as Cisco Integrated Service Routers (ISR). The IP phones listed below have been tested with Cisco Webex Meetings Server:

- Cisco 7960
- Cisco 7970
- Cisco 7971
- Cisco 7940
- Cisco 9951
- Cisco 9971
- Cisco 7980 (Tandberg)
- Cisco 7975
- Cisco E20
- Cisco Telepresence (CTS 1100)
- Cisco IP Communicator
- Lifesize video phone
- Tandberg 1000
- Tandberg 1700
- Polycom

- Cisco Cius
- C20
- EX 60
- EX 90

Other Cisco UC-compatible endpoints should also operate normally. For a list of Cisco Unified IP Phones supported by Cisco Unified Communications Manager and the Device Packs available for each model, see Cisco Unified IP Phone Feature and Cisco Unified Communications Manager Device Pack Compatibility Matrix .