Secure Conference Resources Setup

This chapter provides information about secure conference resources setup.

Secure Conference

The Secure Conferencing feature provides authentication and encryption to secure a conference. A conference gets considered secure when all participating devices have encrypted signaling and media. The secure conference feature supports SRTP encryption over a secure TLS or IPSec connection.

The system provides a security icon for the overall security status of the conference, which is determined by the lowest security level of the participating devices. For example, a secure conference that includes two encrypted connections and one authenticated connection has a conference security status of authenticated.

To configure secure ad hoc and meet-me conferences, you configure a secure conference bridge.

- If a user initiates a conference call from a phone that is authenticated or encrypted, Unified Communications Manager allocates the secure conference bridge

- If a user initiates a call from a phone that is nonsecure, Unified Communications Manager allocates a nonsecure conference bridge.

When you configure conference bridge resources as nonsecure, the conference remains nonsecure, regardless of the security configuration for the phone.

Note Unified Communications Manager allocates a conference bridge from the Media Resource Group List (MRGL) for the phone that is initiating the conference. If a secure conference bridge is not available, Unified Communications Manager assigns a nonsecure conference bridge, and the conference is nonsecure. Likewise, if a nonsecure conference bridge is not available, Unified Communications Manager assigns a secure conference bridge, and the conference is nonsecure. If no conference bridge is available, the call will fail.

For meet-me conference calls, the phone that initiates the conference must also meet the minimum security requirement that is configured for the meet-me number. If no secure conference bridge is available or if the initiator security level does not meet the minimum, Unified Communications Manager rejects the conference attempt.

To secure conferences with barge, configure phones to use encrypted mode. After the Barge key is pressed and if the device is authenticated or encrypted, Unified Communications Manager establishes a secure connection between the barging party and the built-in bridge at the target device. The system provides a conference security status for all connected parties in the barge call.

Note Nonsecure or authenticated Cisco Unified IP Phones that are running release 8.3 or later can now barge encrypted calls.

Conference Bridge Requirements

A conference bridge can register as a secure media resource when you add a hardware conference bridge to your network and configure a secure conference bridge in Unified Communications Manager Administration.

Note Due to the performance impact to Unified Communications Manager processing, Cisco does not support secure conferencing on software conference bridge.

A Digital Signal Processor (DSP) farm, which provides conferencing on a H.323 or MGCP gateway, acts as the network resource for IP telephony conferencing. The conference bridge registers to Unified Communications Manager as a secure SCCP client.

- The conference bridge root certificate must exist in CallManager trust store, and the Cisco CallManager certificate must exist in the conference bridge trust store.
- The secure conference bridge security setting must match the security setting in Unified Communications Manager to register.

For more information about conferencing routers, refer to the IOS router documentation that is provided with your router.

Unified Communications Manager assigns conference resources to calls on a dynamic basis. The available conference resource and the enabled codec provide the maximum number of concurrent, secure conferences allowed per router. Because transmit and receive streams are individually keyed for each participating endpoint (so no rekeying is necessary when a participant leaves the conference), the total secure conference capacity for a DSP module equals one-half the nonsecure capacity that you can configure.

See *Feature Configuration Guide for Cisco Unified Communications Manager* for more information.

Secure Conference Icons

Cisco IP Phones display a conference security icon for the security level of the entire conference. These icons match the status icons for a secure two-party call, as described in the user documentation for your phone.

The audio and video portions of the call provide the basis for the conference security level. The call gets considered secure only if both the audio and video portions are secure.

For ad hoc and meet-me secure conferences, the security icon for the conference displays next to the conference softkey in the phone window for conference participants. The icon that displays depends on the security level of the conference bridge and all participants:

- A lock icon displays if the conference bridge is secure and all participants in the conference are encrypted.
- A shield icon displays if the conference bridge is secure and all participants in the conference are authenticated. Some phone models do not display the shield icon.
- When the conference bridge or any participant in the conference is nonsecure, the call state icon (active, hold, and so on) displays, or, on some older phone models, no icon displays.

Note The “Override BFCP Application Encryption Status When Designating Call Security Status” service parameter displays the lock icon when parameter value is True and audio is secure. This condition ignores the security statuses of all other media channels. The default parameter value is False.

When an encrypted phone connects to a secure conference bridge, the media streaming between the device and the conference bridge gets encrypted; however, the icon for the conference can be encrypted, authenticated, or nonsecure depending on the security levels of the other participants. A nonsecure status indicates that one of the parties is not secure or cannot be verified.

When a user presses Barge, the icon that displays next to the Barge softkey provides the security level for the barge conference. If the barging device and the barged device support encryption, the system encrypts the media between the two devices, but the barge conference status can be nonsecure, authenticated, or encrypted, depending on the security levels of the connected parties.

Secure Conference Status

Conference status can change as participants enter and leave the conference. An encrypted conference can revert to a security level of authenticated or nonsecure if an authenticated or nonsecure participant connects to the call. Likewise, the status can upgrade if an authenticated or nonsecure participant drops off the call. A nonsecure participant that connects to a conference call renders the conference nonsecure.

Conference status can also change when participants chain conferences together, when the security status for a chained conference changes, when a held conference call is resumed on another device, when a conference call gets barged, or when a transferred conference call completes to another device.

Note The Advanced Ad Hoc Conference Enabled service parameter determines whether ad hoc conferences can be linked together by using features such as conference, join, direct transfer, and transfer.

Unified Communications Manager provides these options to maintain a secure conference:

- Ad hoc conference lists
- Meet-Me conference with minimum security level

Ad Hoc Conference Lists

A conference list displays on participating phones when the ConfList softkey is pressed during a conference call. The conference list provides the conference status as well as the security status for each participant to identify participants that are not encrypted.

Conference list displays these security icons: nonsecure, authenticated, encrypted, held. The conference initiator can use the conference list to eject participants with a low security status.

Note The Advanced Ad Hoc Conference Enabled service parameter determines whether conference participants other than the conference initiator can eject conference participants.

As participants join the conference, they get added to the top of the conference list. To remove nonsecure participants from a secure conference with the ConfList and RmLstC softkeys, refer to the user documentation for your phone.

The following sections describe secure ad hoc conference interactions with other features.

Secure Ad Hoc Conference and Conference Chaining

When an ad hoc conference is chained to another ad hoc conference, the chained conference displays in the list as member “Conference” with its own security status. Unified Communications Manager includes the security level for the chained conference to determine the overall conference security status.

Secure Ad Hoc Conference and cBarge

When a user presses the cBarge softkey to join an active conference, Unified Communications Manager creates an ad hoc conference and allocates a conference bridge according to the security level and MRGL of the barged device. The cbarge member names display in the conference list.

Secure Ad Hoc Conference and Barge

If a participant in a secure ad hoc conference gets barged, the barge call security status shows in the conference list next to the barge target. The security icon for the barge target may show authenticated when, in fact, the media is encrypted between the barge target and the conference bridge, because the barge caller has an authenticated connection.

If the barge target is secure but in an unsecured ad hoc conference, if the ad hoc conference status later changes to secure, the barge caller icon will update as well.

Secure Ad Hoc Conference and Join

Authenticated or encrypted phone users can use the Join softkey at a Cisco Unified IP Phone (only phones that are running SCCP) to create or join a secure ad hoc conference. If a user presses Join to add a participant with an unknown security status to an existing conference, Unified Communications Manager downgrades the conference status to unknown. A participant who adds a new member with Join becomes the conference initiator and can eject the new member or any other participant from the conference list (if the Advanced Ad Hoc Conference Enabled setting is True).

Secure Ad Hoc Conference and Hold/Resume

When a conference initiator puts the conference call on hold to add a participant, the conference status remains unknown (nonsecure) until the added participant answers the call. After the new participant answers, conference status updates in the conference list.

If a caller on a shared line resumes a held conference call at another phone, the conference list updates when the caller presses Resume.

Meet-Me Conference with Minimum Security Level

As administrator, you can specify a minimum security level for a conference when you configure a meet-me pattern or number as nonsecure, authenticated, or encrypted. Participants must meet the minimum security requirement, or the system blocks the participant and drops the call. This action applies to meet-me conference call transfers, resumed meet-me conference calls on shared lines, and chained Meet-Me conferences.

The phone that initiates the meet-me conference must meet the minimum security level, or the system rejects the attempt. When the minimum security level specifies authenticated or encrypted and a secure conference bridge is not available, the call fails.

If you specify nonsecure as the minimum level for the conference bridge, the conference bridge accepts all calls, and the conference status is nonsecure.

The following sections describe secure meet-me conference interactions with other features.

Meet-Me Conference and Ad Hoc Conference

To add a meet-me conference to an ad hoc conference or add an ad hoc conference to a meet-me conference, the ad hoc conference must meet the minimum security level for the meet-me conference, or the call is dropped. The conference icon can change when the conference gets added.

Meet-Me Conference and Barge

Unless a barge caller meets the minimum security requirement when the caller barges a meet-me conference participant, the security level of the barged device downgrades, and both the barge caller and the barged call get dropped.

Meet-Me Conference and Hold/Resume

A phone on a shared line cannot resume a meet-me conference unless the phone meets the minimum security level. If a phone does not meet the minimum security level, all phones on the shared line get blocked when the user presses Resume.

Cisco Unified IP Phone Secure Conference and Icon Support

These Cisco Unified IP Phones support secure conference and secure conference icons:

- Cisco Unified IP Phones 7942 and 7962 (SCCP only, authenticated secure conference only)
- Cisco Unified IP Phones 6901, 6911, 6921, 6941, 6945, 6961, 7906G, 7911G, 7921G, , 7931G, 7942, 7941G, 7941G-GE, 7942G, 7945G, 7961G, 7961G-GE, 7962G, 7965G, 7970G, 7971G, 7971G-GE, 7975G, 8941, and 8945. (SCCP only)
- Cisco Unified IP Phones 6901, 6911, 6921, 6941, 6945, 6961, 7906G, 7911G, 7941G, 7941G-GE, 7942G, 7961G, 7961G-GE,7962G, 7965G, 7970G, 7971G, 7971G-GE, 7975G, 8941, 8945, 8961, 9971, and 9971.

  Cisco IP Phones 7811, 7821, 7841, 7861, Cisco IP Conference Phone7832, Cisco IP Phones 8811, 8841, 8845, 8851, 8851NR, 8861, 8865, 8865NR, Cisco Wireless IP Phone 8821, Cisco Unified IP Conference Phone 8831, Cisco IP Conference Phone 8832.

Warning To obtain the full benefit of secure conference features, Cisco recommends upgrading Cisco Unified IP Phones to release 8.3 or later, which supports the encryption features in this release. Encrypted phones that run earlier releases do not fully support these new features. These phones can only participate in secure conference as authenticated or nonsecure participants.

Cisco Unified IP Phones that are running release 8.3 with an previous release of Cisco Unified Communications Manager will display their connection security status, not the conference security status, during a conference call, and do not support secure conference features like conference list.

See topics related to Unified Communications Manager secure conference restrictions for more restrictions that apply to Cisco Unified IP Phones.

For additional information about secure conference calls and security icons, refer to the *Cisco IP Phone Administration Guide and Cisco IP Phone User Guide* for your phone.

Secure Conference CTI Support

Unified Communications Manager supports secure conference over licensed CTI devices. Refer to the *Unified Communications Manager JTAPI Developers Guide* and *Unified Communications Manager TAPI Developers Guide* for this release for more information.

Secure Conference Over Trunks and Gateways

Unified Communications Manager supports secure conference over intracluster trunks (ICTs), H.323 trunks/gateways, and MGCP gateways; however, encrypted phones that are running release 8.2 or earlier will revert to RTP for ICT and H.323 calls, and the media does not get encrypted.

If a conference involves a SIP trunk, the secure conference status is nonsecure. In addition, SIP trunk signaling does not support secure conference notifications to off-cluster participants.

CDR Data

CDR data provides the security status of each call leg from the phone endpoint to the conference bridge as well as the security status of the conference itself. The two values use two different fields inside the CDR database.

CDR data provides termination cause code 58 (Bearer capability not presently available) when a meet-me conference rejects a join attempt that does not meet the minimum security level requirement. See the *CDR Analysis and Reporting Administration Guide* for more information.

Interactions and Restrictions

This section contains information on the following topics:

- Cisco Unified Communications Manager Interactions with Secure Conference, on page 7
- Cisco Unified Communications Manager Restrictions with Secure Conference, on page 8

Cisco Unified Communications Manager Interactions with Secure Conference

This section describes Unified Communications Manager interactions with the secure conference feature.

- To keep a conference secure, if a participant in a secure ad hoc conference puts a call on hold or parks the call, the system does not play MOH, even if the Suppress MOH to Conference Bridge service parameter is set to False. The secure conference status does not change.
- In intercluster environments, if an off-cluster conference participant presses hold in a secure ad hoc conference, the media stream to the device stops, MOH plays, and the media status changes to unknown. If the off-cluster participant resumes a held call with MOH, the conference status may upgrade.
- A secure MeetMe call across an intercluster trunk (ICT) will clear if the remote user invokes a phone feature such a hold/resume, which changes the media status to unknown.
- Annunciator tones or announcements for Unified Communications Manager Multilevel Precedence and Preemption that play on a participant phone during a secure ad hoc conference change the conference status to nonsecure.
- If a caller barges a secure SCCP phone call, the system uses an internal tone-playing mechanism at the target device, and the conference status remains secure.
- If a caller barges a secure SIP phone call, the system provides tone-on-hold, and the conference status remains nonsecure during the tone.
- If a conference is secure and RSVP is enabled, the conference remains secure.
- For conference calls that involve the PSTN, the security conference icon shows the security status for only the IP domain portion of the call.
- The Maximum Call Duration Timer service parameter also controls the maximum conference duration.
- Conference bridge supports packet capture. During a packet capture session, the phone displays a nonsecure status for the conference, even if the media stream is encrypted.

- The media security policy that is configured for your system may alter secure conference behavior; for example, an endpoint will use media security according to the system media security policy, even when participating in a conference call with endpoints that do no support media security.

Cisco Unified Communications Manager Restrictions with Secure Conference

This section describes Unified Communications Manager restrictions with secure conferencing feature.

- Encrypted Cisco IP Phones that are running release 8.2 or earlier can only participate in a secure conference as authenticated or nonsecure participants.
- Cisco Unified IP Phones that are running release 8.3 with an previous release of Unified Communications Manager will display their connection security status, not the conference security status, during a conference call and do not support secure conference features like conference list.
- Cisco Unified IP Phones 7800 and 7911G do not support conference list.
- Due to bandwidth requirements, Cisco Unified IP Phones 7942 and 7962 do not support barge from an encrypted device on an active encrypted call. The barge attempt will fail.
- Cisco Unified IP Phone 7931G does not support conference chaining.
- Phones that are calling over SIP trunks get treated as nonsecure phones, regardless of their device security status.
- If a secure phone attempts to join a secure meet-me conference over a SIP trunk, the call gets dropped. Because SIP trunks do not support providing the “device not authorized” message to a phone that is running SIP, the phone does not update with this message. In addition, 7962 phones that are running SIP do not support the “device not authorized” message.
- In intercluster environments, the conference list does not display for off-cluster participants; however, the security status for the connection displays next to the Conference softkey as long as the connection between the clusters supports it. For example, for H.323 ICT connections, the authentication icon does not display (the system treats the authenticated connection as nonsecure), but the encryption icon displays for an encrypted connection.

  Off-cluster participants can create their own conference that connects to another cluster across the cluster boundary. The system treats the connected conferences as a basic, two-party call.

Securing Conference Resources Tips

Consider the following information before you configure secure conference bridge resources:

- Use localization if you want the phone to display custom text for secure conference messages. Refer to the Unified Communications Manager Locale Installer documentation for more information.
- The conference or built-in bridge must support encryption to secure conference calls.
- To enable secure conference bridge registration, set the cluster security mode to mixed mode.
- Ensure the phone that initiates a conference is authenticated or encrypted to procure a secure conference bridge.

- To maintain conference integrity on shared lines, do not configure devices that share a line with different security modes; for example, do not configure an encrypted phone to share a line with an authenticated or nonsecure phone.
- Do not use SIP trunks as ICTs when you want to share conference security status between clusters.
- If you set the cluster security mode to mixed mode, the security mode that is configured for the DSP farm (nonsecure or encrypted) must match the conference bridge security mode in Unified Communications Manager Administration, or the conference bridge cannot register. The conference bridge registers as encrypted when both security modes specify encrypted; the conference bridge registers as nonsecure when both security modes specify nonsecure.
- If you set the cluster security mode to mixed mode, if the security profile you applied to the conference bridge is encrypted, but the conference bridge security level is nonsecure, Unified Communications Manager rejects conference bridge registration.
- If you set the cluster security mode to nonsecure mode, configure the security mode at the DSP farm as nonsecure, so the conference bridge can register. The conference bridge registers as nonsecure even if the setting in Unified Communications Manager Administration specifies encrypted.
- During registration, the conference bridge must pass authentication. To pass authentication, the DSP farm system must contain one or more the Unified Communications Manager CallManager.pem certificates, and Unified Communications Manager must contain certificates for the DSP farm system and the DSP connection in the CallManager-trust store. The common Name specified in the X.509 Subject attribute must begin with the conference bridge name defined in Cisco Unified Communications Manager and on the DSP farm system using the associate **profile <profile-identifier> register <device-name>?** command. The Subject Alternate Name attribute is not supported. For example, if the certificate Subject Common Name is ?CN=example.cisco.com? then the Conference Bridge Name in Unified Communications Manager must be ?example? and the DSP farm system command must be **?associate profile <profile-identifier> register** example. If you have multiple secure conference bridges on the same DSP farm system, each requires a separate certificate.

Tip Make sure that the Conference Bridge Name is unique and that it can not be configured in any other place under the "Device" table. This applies to the Route list, SIP trunks, IP phones, and so on.

- If conference bridge certificates expire or change for any reason, use the certificate management feature in Cisco Unified Communications Operating System Administration to update the certificates in the trusted store. The TLS authentication fails when certificates do not match, and conference bridge does not work because it cannot register to Unified Communications Manager.
- The secure conference bridge registers to Unified Communications Manager through TLS connection at port 2443; a nonsecure conference bridge registers to Unified Communications Manager through TCP connection at port 2000.
- Changing the device security mode for the conference bridge requires a reset of Unified Communications Manager devices and a restart of the Cisco CallManager service.

Set Up Secure Conference Bridge

The following procedure provides the tasks used to add secure conferencing to your network.

Procedure

Step 1 Verify that you installed and configured the CiscoCTL Client for Mixed Mode.

Step 2 Verify that you configured the DSP farm security settings for Unified Communications Manager connection, including adding the Unified Communications Manager certificate to the trust store. Set the DSP farm security level to encrypted.

Refer to the documentation for your conference bridge.

Tip The DSP farm establishes the TLS port connection to Unified Communications Manager on port 2443.

Step 3 Verify the DSP farm certificate is in the CallManager trust store.

To add the certificate, use the certificate management function in the Cisco Unified Communications Operating System to copy the DSP certificate to the trusted store in Unified Communications Manager.

When you have finished copying the certificate, restart the CiscoCallManager service on the server.

For more information, see the *Administration Guide for Cisco Unified Communications Manager* and the *Cisco Unified Serviceability Administration Guide*.

Tip Be sure to copy the certificate to each server in the cluster and restart the CiscoCallManager service on each server in the cluster.

Step 4 In Unified Communications Manager Administration, configure Cisco IOS Enhanced Conference Bridge as the conference bridge type and select Encrypted Conference Bridge for device security mode.

Tip When you upgrade to this release, Unified Communications Manager automatically assigns a nonsecure conference bridge security profile to Cisco IOS Enhanced Conference Bridge configurations.

Step 5 Configure a minimum security level for Meet-Me Conferences.

Tip When you upgrade to this release, Unified Communications Manager automatically assigns a minimum security level of nonsecure to all Meet Me patterns.

Step 6 Configure packet capturing for the secure conference bridge.

See the *Troubleshooting Guide for Unified Communications Manager* for more information.

Tip Set packet capture mode to batch mode and capture tier to SRTP.

Set Up Secure Conference Bridge in Cisco Unified Communications Manager Administration

To configure a secure conference bridge in Unified Communications Manager Administration, perform the following procedure. After you configure encryption for the conference bridge, you must reset Unified Communications Manager devices and restart the CiscoCallManager service.

Ensure that you installed certificates in Unified Communications Manager and in the DSP farm to secure the connection between the devices.

Before you begin

Before You Begin

Procedure

Step 1 Choose **Media Resources** > **Conference Bridge**.

Step 2 In the **Find and List Conference Bridges** window, verify that a Cisco IOS Enhanced Conference Bridge is installed and go to Set Up Secure Conference Bridge, on page 10.

Step 3 If the device does not exist in the database, click **Add New**; go to Set Up Secure Conference Bridge in Cisco Unified Communications Manager Administration, on page 11.

Step 4 In the Conference Bridge Configuration window, select **Cisco IOS Enhanced Conference Bridge** in the **Conference Bridge Type** drop-down list box. Configure the Conference Bridge Name, Description, Device Pool, Common Device Configuration, and Location settings as described in the *Administration Guide for Cisco Unified Communications Manager* .

Step 5 In the Device Security Mode field, select **Encrypted Conference Bridge**.

Step 6 Click **Save**.

Step 7 Click **Reset**.

What to do next

To perform additional conference bridge configuration tasks, you can jump to the Meet-Me/Number Pattern Configuration window or the Service Parameter Configuration window by selecting the option from the Related Links drop-down list box and clicking **Go**.

Set Up Minimum Security Level for Meet-Me Conferences

To configure a minimum security level for Meet-Me conferences, perform the following procedure.

Procedure

Step 1 Choose **Call Routing** > **Meet-Me Number/Pattern**.

Step 2 In the Find and List Conference Bridges window, verify that the Meet-Me number/pattern is configured and go to Set Up Secure Conference Bridge, on page 10.

Step 3 If the Meet-Me number/pattern is not configured, click **Add New**; go to Set Up Minimum Security Level for Meet-Me Conferences, on page 11.

Step 4 In the **Meet-Me Number Configuration** window, enter a Meet-Me number or range in the Directory Number or Pattern field. Configure the Description and Partition settings as described in the *Feature Configuration Guide for Cisco Unified Communications Manager*.

Step 5 In the Minimum Security Level field, select **Non Secure**, **Authenticated**, or **Encrypted**.

Step 6 Click **Save**.

What to do next

If you have not yet installed a secure conference bridge, install and configure a secure conference bridge.

Set Up Packet Capturing for Secure Conference Bridge

To configure packet capturing for a secure conference bridge, enable packet capturing in the **Service Parameter Configuration** window; then, set the packet capture mode to batch mode and capture tier to SRTP for the phone, gateway, or trunk in the device configuration window. Refer to the *Troubleshooting Guide for Cisco Unified Communications Manager* for more information.

During a packet capture session, the phone displays a nonsecure status for the conference, even if the media stream is encrypted.