セキュアな会議リソースの設定

この章では、セキュアな会議リソースの設定について説明します。

セキュアな会議

セキュアな会議機能は、会議を保護するために認証と暗号化を提供します。会議に参加しているすべてのデバイスでシグナリングとメディアが暗号化されている場合に、会議は保護されている

とみなされます。セキュアな会議機能は、セキュアな TLS または IPSec 接続での SRTP 暗号化をサポートします。

システムでは、会議の全体的なセキュリティ ステータスを示すセキュリティ アイコンが表示されます。この全体的なステータスは、参加しているデバイスの最も低いセキュリティ レベルにより決定します。たとえば、2 つの暗号化接続と 1 つの認証済み接続を含むセキュアな会議のセキュリティ ステータスは認証済みです。

セキュアなアドホック会議とミートミー会議を設定するには、セキュアな会議ブリッジを設定します。

- ユーザが認証済みまたは暗号化済みの電話から電話会議を開始すると、Cisco Unified Communications Manager はセキュアな会議ブリッジを割り当てます。
- ユーザが非セキュアな電話からコールを開始すると、Cisco Unified Communications Manager は非セキュアな会議ブリッジを割り当てます。

会議ブリッジ リソースを非セキュアとして設定すると、電話のセキュリティ設定にかかわらず、会議は非セキュアになります。

（注） Cisco Unified Communications Manager は会議を開始している電話のメディア リソース グループ リスト（MRGL）から会議ブリッジを割り当てます。セキュアな会議ブリッジを使用できない場合は、Cisco Unified Communications Manager は非セキュアな会議ブリッジを割り当て、会議は非セキュアになります。同様に、非セキュアな会議ブリッジを使用できない場合、Cisco Unified Communications Manager はセキュアな会議ブリッジを割り当て、会議は非セキュアになります。会議ブリッジが利用不可の場合、コールは失敗します。

ミートミー会議コールでは、会議を開始する電話はミートミー番号に設定された最小セキュリティ要件を満たす必要があります。セキュアな会議ブリッジを使用できないか、発信者のセキュリティ レベルが最小要件を満たさない場合、Cisco Unified Communications Manager は会議の試行を拒否します。

割り込みを使用する会議を保護するには、暗号化モードを使用するよう電話を設定します。デバイスが認証済みまたは暗号化済みの場合に [Barge] キーを押すと、Cisco Unified Communications Manager は割り込み相手とターゲットデバイスでの組み込みブリッジの間でセキュアな接続を確立します。システムは、割り込みコールに接続されているすべての参加者に対して会議のセキュリティ ステータスを示します。

（注） リリース 8.3 以降を実行している非セキュアまたは認証済みの Cisco Unified IP Phone は暗号化済みコールに割り込めるようになりました。

関連トピック

最小セキュリティ レベルでのミートミー会議, （6 ページ）

会議ブリッジの要件

ハードウェアによる会議ブリッジをネットワークに追加し、[Cisco Unified Communications Manager Administration] でセキュアな会議ブリッジを設定する場合、会議ブリッジをセキュアなメディアリソースとして登録できます。

（注） Cisco Unified Communications Manager の処理のパフォーマンスに対する影響を考え、ソフトウェアによる会議ブリッジでのセキュアな会議はサポートしていません。

H.323 またはMGCP ゲートウェイでの会議を実現するデジタル シグナル プロセッサ（DSP）ファームが、IP テレフォニー会議のネットワーク リソースとして動作します。会議ブリッジは、Cisco Unified Communications Manager にセキュアな SCCP クライアントとして登録されます。

- 会議ブリッジのルート証明書が CallManager 信頼ストア内に存在し、Cisco CallManager 証明書が会議ブリッジの信頼ストアに存在する必要があります。
- セキュアな会議ブリッジのセキュリティ設定は、登録するCisco Unified Communications Manager のセキュリティ設定と一致している必要があります。

会議ルータの詳細については、IOS ルータに付属するドキュメンテーションを参照してください。

Cisco Unified Communications Manager は、コールに対して会議リソースを動的に割り当てます。使用可能な会議リソースと有効化されたコーデックによって、ルータに許容される最大同時実行数のセキュアな会議が実現されます。ストリームの送受信は、参加するエンドポイントそれぞれに対して個別にキー設定されるため（このため参加者が会議を退出しても再度のキー設定は不要）、DSP モジュールに対するトータルでのセキュアな会議のキャパシティは、設定可能な非セキュア キャパシティの半分に等しくなります。

詳細については、『*Feature Configuration Guide for Cisco Unified Communications Manager*』の「Understanding Conference Devices」“”を参照してください。

セキュアな会議のアイコン

Cisco Unified IP Phone は会議全体のセキュリティ レベルを示す会議セキュリティ アイコンを表示します。これらのアイコンは、ユーザ マニュアルに記載されているように、セキュアな 2 者間コールのステータス アイコンと一致します。

コールの音声とビデオ部分が会議のセキュリティ レベルのベースとなります。コールは、音声とビデオ部分がセキュアである場合に限り、安全とみなされます。

セキュアなアドホック会議とミートミー会議では、会議参加者の電話ウィンドウにある会議ソフトキーの横に会議のセキュリティ アイコンが表示されます。表示されるアイコンは、会議ブリッジおよびすべての参加者のセキュリティ レベルによって異なります。

- 会議ブリッジがセキュアで会議の全参加者が暗号化されている場合、ロック アイコンが表示されます。

- 会議ブリッジがセキュアで会議の全参加者が認証されている場合、シールドアイコンが表示されます。一部の電話モデルでは、シールド アイコンが表示されません。
- 会議ブリッジまたは会議のいずれかの参加者が非セキュアである場合に、コール状態アイコン（アクティブ、保留など）が表示されます。一部の古いモデルの電話では、アイコンは表示されません。

（注） 「Override BFCP Application Encryption Status When Designating Call Security Status」サービス パラメータは、パラメータ値が [True] で音声がセキュアであると、ロック アイコンを表示します。この状態は、他のすべてのメディア チャネルのセキュリティ ステータスを無視します。デフォルト パラメータ値は [False] です。

暗号化された電話がセキュアな会議ブリッジに接続すると、デバイスと会議ブリッジの間のメディア ストリーミングは暗号化されます。ただし、会議のアイコンは、他の参加者のセキュリティ レベルに応じて暗号化、認証済み、非セキュアのいずれかになります。非セキュア ステータスは、参加者のいずれかがセキュアでないか、または確認できないことを示します。

ユーザが [Barge] を押すと、[Barge] ソフトキーの横にあるアイコンが割り込み会議のセキュリティ レベルを示します。割り込むデバイスと割り込まれたデバイスが暗号化をサポートする場合、システムは 2 つのデバイス間のメディアを暗号化しますが、割り込み会議のステータスは、接続された参加者のセキュリティ レベルに応じて、非セキュア、認証済み、暗号化のいずれかになります。

セキュアな会議のステータス

会議のステータスは、参加者が会議に参加するときと退出するときに変わります。暗号化された会議は、認証済みまたは非セキュアな参加者がコールに接続すると、セキュリティ レベルが認証済みまたは非セキュアに戻ることがあります。同様に、認証済みまたは非セキュアな参加者がコールから退出すると、ステータスが上がることがあります。非セキュアな参加者が電話会議に接続すると、会議は非セキュアになります。

会議のステータスは、参加者が複数の会議を結合した場合、結合した会議のセキュリティ ステータスが変わった場合、保留にされた電話会議が別のデバイスで再開された場合、電話会議に割り込みがあった場合、または転送された電話会議が別のデバイスで完了した場合にも変化します。

（注） [Advanced Ad Hoc Conference Enabled] サービス パラメータは、会議、参加、直接転送、および転送などの機能を使用してアドホック会議をリンクできるかどうかを決定します。

Cisco Unified Communications Manager はセキュアな会議を維持するために以下のオプションを提供します。

- アドホック会議のリスト
- 最小セキュリティ レベルでのミートミー会議

関連トピック

アドホック会議のリスト，（5 ページ）
最小セキュリティ レベルでのミートミー会議，（6 ページ）

アドホック会議のリスト

会議リストは、電話会議中に [ConfList] ソフトキーが押された場合に、参加者の電話に表示されます。会議リストには、会議のステータス、および暗号化されていない参加者を識別するための参加者ごとのセキュリティ ステータスが一覧表示されます。

会議リストには、[nonsecure]、[authenticated]、[encrypted]、[held] の各セキュリティ アイコンが表示されます。会議の開催者は、会議リストを使用して、セキュリティ ステータスの低い参加者を退席させることができます。

（注） [Advanced Ad Hoc Conference Enabled] サービス パラメータによって、会議の開催者以外の会議参加者が他の会議参加者を退席させることができるかどうかが決定されます。

参加者は、会議に参加すると、会議リストの一番上に追加されます。非セキュアな参加者を [ConfList] ソフトキーと [RmLstC] ソフトキーでセキュアな会議から削除する方法については、ご使用の電話のユーザ マニュアルを参照してください。

次の各項では、セキュアなアドホック会議と他の機能とのインタラクションについて説明します。

セキュアなアドホック会議と会議チェーン

ある 1 つのアドホック会議が別のアドホック会議にチェーンされると、そのチェーンされた会議は、メンバー「Conference」としてそれ自体のセキュリティ ステータスとともにリストに表示されます。会議全体のセキュリティ ステータスを判別するために、Cisco Unified Communications Manager に、チェーンされた会議のセキュリティ レベルが組み込まれます。

セキュアなアドホック会議と C 割り込み

ユーザが [cBarge] ソフトキーを押してアクティブな会議に参加すると、Cisco Unified Communications Manager ではアドホック会議が作成され、割り込まれたデバイスのセキュリティ レベルと MRGL に従って会議ブリッジが割り当てられます。C 割り込みのメンバー名が会議リストに表示されます。

セキュアなアドホック会議と割り込み

セキュアなアドホック会議の参加者が割り込まれた場合、割り込みコールのセキュリティ ステータスが会議リストの割り込み先参加者の横に表示されます。メディアが割り込み先参加者と会議ブリッジの間で実際に暗号化済みの場合に、割り込み元発信者の接続が認証済みであるために、割り込み先参加者のセキュリティ アイコンが認証済みと表示されることがあります。

割り込み先参加者がセキュアだが非セキュアなアドホック会議に参加している場合に、アドホック会議のステータスがその後セキュアに変わると、割り込み元発信者のアイコンも更新されます。

セキュアなアドホック会議と参加

認証済みまたは暗号化済みの電話のユーザは、Cisco Unified IP Phone（SCCP が実行されている電話機のみ）の [Join] ソフトキーを使用して、セキュアなアドホック会議を作成またはそれに参加することができます。ユーザが [Join] を押してセキュリティ ステータスの不明な参加者を既存の会議に追加すると、Cisco Unified Communications Manager ではその会議のステータスを [unknown] にダウングレードします。[Join] を使用して新規メンバーを追加した参加者は会議の開催者になり、新規メンバーやその他の参加者を会議リストから退席させることができます（[Advanced Ad Hoc Conference Enabled] 設定が [True] になっている場合）。

セキュアなアドホック会議と保留/復帰

会議の開催者が参加者を追加するために電話会議を保留にすると、追加された参加者が電話に応答するまで、会議のステータスは不明（非セキュア）になります。その新規参加者が応答すると、会議リストで会議のステータスが更新されます。

共有回線上の発信者が保留中の電話会議を別の電話で復帰させる場合は、発信者が [Resume] を押したときに会議リストが更新されます。

最小セキュリティ レベルでのミートミー会議

管理者は、ミートミーのパターンまたは番号を非セキュア、認証済み、暗号化済みとして設定する場合、会議に最小セキュリティ レベルを指定できます。参加者は最小セキュリティ要件を満たしている必要があり、満たしていない場合はシステムが参加者をブロックし、コールをドロップします。このアクションはミートミー会議のコール転送、共有回線で再開されたミートミー会議コール、結合されたミートミー会議に適用されます。

ミートミー会議を開始する電話は、最小セキュリティ レベルを満たしている必要があります。満たしていない場合、システムによって試行が拒否されます。最小セキュリティ レベルとして認証済みまたは暗号化済みが指定されており、かつセキュアな会議ブリッジが使用できない場合、コールは失敗します。

会議ブリッジの最小レベルに非セキュアを指定すると、会議ブリッジはすべてのコールを受け入れ、会議のステータスは非セキュアになります。

ここでは、セキュアなミートミー会議とその他の機能のインタラクションについて説明します。

ミートミー会議とアドホック会議

ミートミー会議をアドホック会議に追加する場合、またはアドホック会議をミートミー会議に追加する場合、アドホック会議がミートミー会議の最小セキュリティ レベルを満たしている必要があります。満たしていない場合、コールはドロップされます。会議が追加されると、会議アイコンが変わる場合があります。

ミートミー会議と割り込み

割り込み発信者がミートミー会議参加者に割り込んだ場合、その発信者が最低セキュリティ要件を満たしていないと、割り込まれたデバイスのセキュリティ レベルは下がり、割り込み発信者と割り込まれたコールの両方がドロップされます。

ミートミー会議と保留/再開

共有回線の電話は、最小セキュリティ レベルを満たしていない限り、ミートミー会議を再開できません。電話が最小セキュリティ レベルを満たしていない場合、ユーザが [Resume] ボタンを押すと共有回線上のすべての電話がブロックされます。

関連トピック

ミートミー会議の最小セキュリティ レベルの設定, （14 ページ）

Cisco Unified IP Phone のセキュアな会議とアイコンのサポート

次の Cisco Unified IP Phone では、セキュア会議とセキュア会議アイコンがサポートされています。

- Cisco Unified IP Phone 7940G および 7960G（SCCP のみ、認証済みセキュア会議のみ）
- Cisco Unified IP Phone 6901、6911、6921、6941、6945、6961、7906G、7911G、7921G、7925G、7925G-EX、7926G、7931G、7940G、7941G、7941G-GE、7942G、7945G、7960G、7961G、7961G-GE、7962G、7965G、7970G、7971G、7971G-GE、7975G、8941、8945。（SCCP のみ）
- Cisco Unified IP Phone 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、9971。

警告 セキュア会議機能を十分に活用するため、Cisco Unified IP Phone をリリース 8.3 にアップグレードすることを推奨します。このリリースでは、暗号化機能がサポートされています。以前のリリースを実行している暗号化済みの電話は、これらの機能を完全にサポートしてはいません。そのような電話は、認証済みまたは非セキュアな参加者としてのみセキュア会議に参加できます。

リリース 8.3 の Cisco Unified IP Phone で、以前のリリースの Cisco Unified Communications Manager が使用されている場合、電話会議の間、会議のセキュリティ ステータスではなく接続のセキュリティ ステータスが表示され、会議リストなどのセキュア会議機能がサポートされません。

Cisco Unified IP Phone に適用されるその他の制限については、Cisco Unified Communications Manager のセキュア会議の制限関連項目を参照してください。

セキュア電話会議とセキュリティアイコンの詳細については、ご使用の電話のユーザガイド、およびこの Cisco Unified Communications Manager リリースに対応した『*Cisco Unified IP Phone Administration Guide* for Cisco Unified Communications Manager』を参照してください。

関連トピック

機能制限

セキュアな会議の CTI サポート

Cisco Unified Communications Manager はライセンス済み CTI デバイスでのセキュアな会議をサポートしています。詳細については、このリリースの『*Cisco Unified Communications Manager JTAPI Developers Guide*』および『*Cisco Unified Communications Manager TAPI Developers Guide*』を参照してください。

トランクおよびゲートウェイでのセキュアな会議

Cisco Unified Communications Manager はクラスタ間トランク（ICT）、H.323 トランク/ゲートウェイ、および MGCP ゲートウェイを介したセキュアな会議をサポートしています。ただし、リリース 8.2 以前を実行する暗号化された電話は ICT および H.323 コールの場合 RTP に戻り、メディアは暗号化されません。

会議に SIP トランクが使用される場合、セキュアな会議のステータスは非セキュアになります。さらに、SIP トランク シグナリングはクラスタ外の参加者へのセキュアな会議通知をサポートしていません。

CDR データ

CDR データは、電話エンドポイントから会議ブリッジへの各コール レッグのセキュリティ ステータス、および会議自体のセキュリティ ステータスを示します。2 つの値が CDR データベースの内の 2 つの異なるフィールドを使用します。

ミートミー会議において最も低いセキュリティ レベル要件を満たさない加入の試みが拒否される場合、CDR データは終了原因コード 58 を示します（現在ベアラー機能を使用できません）。詳細については、『*CDR Analysis and Reporting Administration Guide*』を参照してください。

連携動作と制限事項

ここでは、次のトピックについて説明します。

- Cisco Unified Communications Manager のセキュアな会議とのインタラクション, （8 ページ）
- Cisco Unified Communications Manager のセキュアな会議に関する制限事項, （9 ページ）

Cisco Unified Communications Manager のセキュアな会議とのインタラクション

このセクションでは、Cisco Unified Communications Manager とセキュア会議機能との間のインタラクションについて説明します。

- 会議をセキュアに保つため、セキュアなアドホック会議の参加者がコールを保留またはパークした場合は、[Suppress MOH to Conference Bridge] サービス パラメータが [False] に設定されている場合でも、システムは MOH を再生しません。セキュア会議のステータスは変わりません。
- クラスタ間環境では、セキュアなアドホック会議でクラスタ外の会議参加者が保留を押した場合に、そのデバイスへのメディア ストリームが停止し、MOH が再生され、メディア ステータスは不明に変わります。クラスタ外の参加者が MOH の保留コールを再開すると、会議のステータスがアップグレードされます。
- クラスタ間トランク（ICT）を介したセキュアなミートミー通話では、リモート ユーザが保留/再開のような電話の機能を作動させると、コールがクリアされ、メディア ステータスが不明に変わります。
- セキュアなアドホック会議の間に参加者の電話で再生される Cisco Unified Communications Manager のマルチレベル優先度およびプリエンプションの告知トーンや告知は、会議ステータスを非セキュアに変更します。
- 発信者がセキュアな SCCP 電話コールに割り込む場合、システムはターゲット デバイスで内部トーン再生メカニズムを使用し、会議ステータスはセキュアのままになります。
- 発信者がセキュアな SIP 電話コールに割り込む場合、システムは保留トーンを再生し、トーン再生中の会議ステータスは非セキュアのままになります。
- 会議がセキュアであり、RSVP が有効化されている場合、会議はセキュアなままになります。
- PSTN が関係する電話会議の場合、セキュリティ会議アイコンにはそのコールの IP ドメイン部分のみのセキュリティ ステータスが表示されます。
- 会議の長さの上限は、[Maximum Call Duration Timer] サービス パラメータでも制御できます。
- 会議ブリッジは、パケット キャプチャをサポートします。メディア ストリームが暗号化されている場合でも、パケット キャプチャ セッション中に、電話には会議について非セキュアのステータスが表示されます。
- システムに設定されたメディア セキュリティ ポリシーによって、セキュア会議の動作が変化する場合があります。たとえば、メディア セキュリティをサポートしていないエンドポイントとの電話会議に参加している場合でも、エンドポイントではシステムのメディア セキュリティ ポリシーに従ってメディア セキュリティが使用されます。

Cisco Unified Communications Manager のセキュアな会議に関する制限事項

このセクションでは、セキュア会議機能に関する Cisco Unified Communications Manager の制限事項について説明します。

- 暗号化された Cisco Unified IP Phone でリリース 8.2 以前が実行されている場合、セキュア会議には認証済みまたは非セキュア参加者としてのみ参加できます。

- リリース 8.3 の Cisco Unified IP Phone で、以前のリリースの Cisco Unified Communications Manager が使用されている場合、電話会議の間、会議のセキュリティ ステータスではなく接続のセキュリティ ステータスが表示され、会議リストなどのセキュア会議機能もサポートされません。
- Cisco Unified IP Phone 7905G および 7911G では、会議リストがサポートされません。
- 帯域幅の要件のため、Cisco Unified IP Phone 7940G と 7960G は、アクティブな暗号化されたコールでの暗号化されたデバイスからの割り込みをサポートしません。割り込みの試行は失敗します。
- Cisco Unified IP Phone 7931G では、会議チェーンがサポートされません。
- SIP トランクを介して発信している電話は、デバイスのセキュリティ ステータスにかかわらず、非セキュアな電話として扱われます。
- セキュアな電話が SIP トランクを介してセキュアなミートミー会議に参加しようとした場合、コールは切断されます。SIP トランクでは SIP を実行中の電話に対する「device not authorized」メッセージの提供がサポートされていないため、電話がこのメッセージで更新されることはありません。さらに、SIP を実行中の 7960G 電話では、「device not authorized」メッセージがサポートされません。
- クラスタ間環境では、クラスタ外の参加者に会議リストが表示されません。ただし、クラスタ間の接続でサポートされていれば、接続のセキュリティ ステータスが [Conference] ソフトキーの隣に表示されます。たとえば、H.323 ICT 接続では、認証アイコンは表示されませんが（システムは認証済み接続を非セキュアとして扱う）、暗号化されている接続の暗号化アイコンは表示されます。

  クラスタ外の参加者は、クラスタ境界を越えて別のクラスタに接続する独自の会議を作成できます。システムは、接続された会議を基本的な 2 者間コールとして処理します。

会議リソースの保護のヒント

セキュアな会議ブリッジ リソースを設定する前に、次の点を考慮してください。

- セキュアな会議メッセージのカスタムテキストを電話に表示するには、ローカリゼーションを使用します。詳細については、Cisco Unified Communications Manager のロケールインストーラのマニュアルを参照してください。
- 会議または組み込みブリッジでは、電話会議を保護するために暗号化がサポートされている必要があります。
- セキュアな会議ブリッジ登録を有効にするには、クラスタ セキュリティ モードを混合モードに設定します。
- セキュアな会議ブリッジを確立するために、会議を開始する電話が認証済みまたは暗号化済みであることを確認します。

- 共有回線での会議の整合性を維持するためには、回線を共有するデバイスをさまざまなセキュリティモードで設定しないでください。たとえば、暗号化済み電話が認証済みまたは非セキュアな電話と回線を共有するようには設定しないでください。
- クラスタ間で会議のセキュリティ ステータスを共有したい場合、ICT として SIP トランクを使用しないでください。
- クラスタ セキュリティ モードを混合モードに設定する場合、DSP ファームで設定されているセキュリティ モード（非セキュアまたは暗号化済み）は [Cisco Unified Communications Manager Administration] での会議ブリッジ セキュリティ モードに一致する必要があります。そうでないと、会議ブリッジは登録できません。両方のセキュリティモードが暗号化済みと指定されていれば、会議ブリッジは暗号化済みとして登録されます。両方のセキュリティモードが非セキュアと指定されていれば、会議ブリッジは非セキュアとして登録されます。
- クラスタ セキュリティ モードを混合モードに設定した場合で、会議ブリッジに適用したセキュリティ プロファイルが暗号化済み、会議ブリッジのセキュリティ レベルが非セキュアという場合は、Cisco Unified Communications Manager は会議ブリッジ登録を拒否します。
- クラスタ セキュリティ モードを非セキュア モードに設定する場合、DSP ファームのセキュリティ モードを非セキュアとして設定します。これにより会議ブリッジを登録できます。[Cisco Unified Communications Manager Administration] の設定で暗号化済みとして指定されていても、会議ブリッジは非セキュアとして登録されます。
- 登録時に、会議ブリッジは認証に合格する必要があります。認証に合格するには、DSP ファームに Cisco Unified Communications Manager 証明書が含まれ、Cisco Unified Communications Manager に DSP ファーム システムと DSP 接続の証明書が含まれている必要があります。確実に会議ブリッジが認証に合格するには、X509 証明書名に会議ブリッジ名を含める必要があります。
- 会議ブリッジの証明書が何らかの理由で期限切れまたは変更された場合は、Cisco Unified Communications Operating System Administration の証明書の管理機能を使用して信頼ストアの証明書を更新します。証明書が一致しないと TLS 認証が失敗し、また会議ブリッジが動作しません。これは、会議ブリッジが Cisco Unified Communications Manager に登録できないためです。
- セキュアな会議ブリッジは、ポート 2443 で TLS 接続を介して Cisco Unified Communications Manager に登録されます。非セキュアな会議ブリッジは、ポート 2000 で TCP 接続を介して Cisco Unified Communications Manager に登録されます。
- 会議ブリッジのデバイス セキュリティ モードを変更するには、Cisco Unified Communications Manager デバイスのリセットと Cisco CallManager サービスの再起動が必要です。

セキュアな会議ブリッジのセットアップ

次の手順は、セキュアな会議をご使用のネットワークに追加するための手順を示します。

手順

ステップ 1 Cisco CTL クライアントをインストールし、混合モードに設定したことを確認します。

ステップ 2 信頼ストアへの Cisco Unified Communications Manager 証明書の追加も含め、Cisco Unified Communications Manager 接続用の DSP ファーム セキュリティを設定したことを確認します。DSP ファームのセキュリティ レベルを暗号化済みに設定します。
ご使用の会議ブリッジのマニュアルを参照してください。

ヒント DSP ファームは、ポート 2443 で Cisco Unified Communications Manager への TLS ポート接続を確立します。

ステップ 3 DSP ファーム証明書が CallManager 信頼ストア内にあることを確認してください。
証明書を追加するには、Cisco Unified Communications オペレーティング システムの証明書管理機能を使用して DSP 証明書を Cisco Unified Communications Manager 内の信頼ストアにコピーします。

証明書のコピーが終わったら、サーバで Cisco CallManager サービスを再起動します。

詳細については、『*Administration Guide for Cisco Unified Communications Manager*』および『*Cisco Unified Serviceability Administration Guide*』を参照してください。

ヒント 証明書はクラスタ内の各サーバに必ずコピーし、クラスタ内の各サーバで Cisco CallManager サービスを再起動する必要があります。

ステップ 4 [Cisco Unified Communications Manager Administration] で、[Cisco IOS Enhanced Conference Bridge] を会議ブリッジ タイプとして設定し、[Encrypted Conference Bridge] をデバイスのセキュリティ モードとして選択します。

ヒント 今回のリリースにアップグレードすると、Cisco Unified Communications Manager は自動的に非セキュアな会議ブリッジセキュリティプロファイルを Cisco IOS Enhanced Conference Bridge 設定に割り当てます。

ステップ 5 ミートミー会議の最小セキュリティ レベルを設定します。

ヒント 今回のリリースにアップグレードすると、Cisco Unified Communications Manager は最小セキュリティ レベルとして非セキュアをすべてのミートミー パターンに自動的に割り当てます。

ステップ 6 セキュアな会議ブリッジのパケット キャプチャを設定します。
詳細については、『*Troubleshooting Guide for Cisco Unified Communications Manager*』を参照してください。

ヒント パケット キャプチャ モードをバッチ モードに設定し、キャプチャ層を SRTP に設定します。

関連トピック

会議リソースの保護のヒント, （10 ページ）
ミートミー会議の最小セキュリティ レベルの設定, （14 ページ）
セキュアな会議ブリッジのパケット キャプチャの設定, （14 ページ）

Cisco Unified Communications Manager Administration でのセキュアな会議ブリッジの設定, （13 ページ）

Cisco Unified Communications Manager Administration でのセキュアな会議ブリッジの設定

[Cisco Unified Communications Manager Administration] でセキュアな会議ブリッジを設定するには、次の手順を実行します。会議ブリッジに暗号化を設定した後、Cisco Unified Communications Manager の各デバイスをリセットして、Cisco CallManager サービスを再起動する必要があります。

デバイス間の接続をセキュリティで保護するために、Cisco Unified Communications Manager と DSP ファームにそれぞれ証明書をインストールしたことを確認してください。

はじめる前に

はじめる前に

手順

ステップ 1 [Media Resources] > [Conference Bridge] を選択します。

ステップ 2 [Find and List Conference Bridges] ウィンドウで、Cisco IOS Enhanced Conference Bridge がインストールされていることを確認してから、セキュアな会議ブリッジのセットアップ, （11 ページ）に進みます。

ステップ 3 デバイスがデータベース内に存在しない場合は、[Add New] をクリックして、に進みます。

ステップ 4 [Conference Bridge Configuration] ウィンドウで、[Conference Bridge Type] ドロップダウン リスト ボックスから [Cisco IOS Enhanced Conference Bridge] を選択します。『*Administration Guide for Cisco Unified Communications Manager*』の説明に従って、[Conference Bridge Name]、[Description]、[Device Pool]、[Common Device Configuration]、および [Location] の設定を行います。

ステップ 5 [Device Security Mode] フィールドで、[Encrypted Conference Bridge] を選択します。

ステップ 6 [Save] をクリックします。

ステップ 7 [Reset] をクリックします。

次の作業

その他の会議ブリッジ設定タスクを実行するために、[Related Links] ドロップダウンリスト ボックスからオプションを選択して [Go] をクリックし、[Meet-Me Number/Pattern Configuration] ウィンドウまたは [Service Parameter Configuration] ウィンドウに移動できます。

関連トピック

セキュアな会議リソースに関する詳細情報の入手先, （15 ページ）

ミートミー会議の最小セキュリティ レベルの設定

ミートミー会議の最小セキュリティ レベルを設定するには、次の手順を実行します。

手順

ステップ 1 [Call Routing] > [Meet-Me Number/Pattern] を選択します。

ステップ 2 [Find and List Conference Bridges] ウィンドウで、ミートミー番号/パターンが設定されていることを確認してから、セキュアな会議ブリッジのセットアップ, （11 ページ）に進みます。

ステップ 3 ミートミー番号/パターンが設定されていない場合は、[Add New] をクリックして、に進みます。

ステップ 4 [Meet-Me Number Configuration] ウィンドウで、[Directory Number or Pattern] フィールドにミートミー番号または範囲を入力します。『*Feature Configuration Guide for Cisco Unified Communications Manager*』の説明に従って、[Description] と [Partition] の設定を行います。

ステップ 5 [Minimum Security Level] フィールドで、[Non Secure]、[Authenticated] または [Encrypted] を選択します。

ステップ 6 [Save] をクリックします。

次の作業

セキュアな会議ブリッジをまだインストールしていない場合は、セキュアな会議ブリッジをインストールして設定します。

関連トピック

Cisco Unified Communications Manager Administration でのセキュアな会議ブリッジの設定, （13 ページ）
セキュアな会議リソースに関する詳細情報の入手先, （15 ページ）

セキュアな会議ブリッジのパケット キャプチャの設定

セキュアな会議ブリッジにパケット キャプチャを設定するには、[Service Parameter Configuration] ウィンドウでパケット キャプチャを有効にしてから、デバイス設定ウィンドウで、電話、ゲートウェイ、またはトランクに対してパケット キャプチャ モードをバッチ モードに設定し、キャプチャ層を SRTP に設定します。詳細については、『*Troubleshooting Guide for Cisco Unified Communications Manager*』を参照してください。

メディア ストリームが暗号化されている場合でも、パケット キャプチャ セッション中に、電話には会議について非セキュアのステータスが表示されます。

セキュアな会議リソースに関する詳細情報の入手先

関連トピック

システム要件
連携動作と制限事項
証明書
認証と暗号化のセットアップ
セキュアな会議, （1 ページ）
会議ブリッジの要件, （3 ページ）
セキュアな会議のアイコン, （3 ページ）
セキュアな会議のステータス, （4 ページ）
Cisco Unified IP Phone のセキュアな会議とアイコンのサポート, （7 ページ）
セキュアな会議の CTI サポート, （8 ページ）
トランクおよびゲートウェイでのセキュアな会議, （8 ページ）
連携動作と制限事項, （8 ページ）
会議リソースの保護のヒント, （10 ページ）
セキュアな会議ブリッジのセットアップ, （11 ページ）
セキュアな会議ブリッジのパケット キャプチャの設定, （14 ページ）