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。会議は、すべての参加デバイスが暗号化されたシグナリングとメディアを持っている場合、セキュアと見なされます。セキュアな会議機能は、セキュアな TLS または IPSec 接続を介した SRTP 暗号化をサポートします。

システムには、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。これは、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って決定されます。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には、認証済みの会議セキュリティステータスがあります。

セキュアなアドホック会議と会議室の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、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、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） 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、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、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。会議ブリッジが使用できない場合、コールは失敗します。

会議コールの場合、会議を開始する電話機は、会議番号に設定されている最小のセキュリティ要件を満たしている必要があります。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、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、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、割り込みコールで接続されているすべての通話者に対して会議のセキュリティ ステータスを提供します。

（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 電話 は暗号化済みコールに割り込めるようになりました。

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、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） 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、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。

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なコーデックは、ルータごとに許可される同時のセキュアな会議の最大数を提供します。送信ストリームと受信ストリームは、参加している各エンドポイントに個別にキーが割り当てられるため (参加者が会議を退室したときにキー再生成は必要ありません)、DSPモジュールの合計セキュア会議容量は、非セキュアな容量の1分に相当します。を設定できます。

『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

セキュアな会議アイコン

Cisco IP 電話 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、電話機のユーザマニュアルで説明されているように、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。

コールの音声およびビデオ部分によって、会議のセキュリティレベルの基準が提供されます。音声とビデオの両方の部分がセキュアである場合にのみ、コールはセキュアと見なされます。

アドホックおよび会議のセキュアな会議では、会議の参加者の電話ウィンドウの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、会議ブリッジと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、会議のすべての参加者が暗号化されている場合は、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、会議のすべての参加者が認証されている場合は、シールドアイコンが表示されます。一部の電話機モデルでは、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、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。または、一部の古い電話機モデルでは、アイコンが表示されません。

（注） 「コールセキュリティステータスを指定した場合の BFCP アプリケーション暗号化ステータスのオーバーライド」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場合に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。

暗号化された電話機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が暗号化されます。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、または非セキュアにすることができます。非セキュアステータスは、いずれかの当事者がセキュアでないか、または検証できないことを示します。

ユーザが [割り込み (割り込み)] を押すと、[割り込み (割り込み)] ソフトキーの横に表示されるアイコンによって割り込み会議のセキュリティレベルが提供されます。割り込みデバイスと割り込まれたデバイスが暗号化をサポートしている場合、システムは2つのデバイス間でメディアを暗号化しますが、接続されている通話者のセキュリティレベルに応じて、割り込み会議のステータスは非セキュア、認証済み、または暗号化済み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、参加者が会議に出入りしたときに変更できます。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、認証済みまたは非セキュアのセキュリティレベルに戻ることができます。同様に、認証済みまたは非セキュアな参加者がコールを切断した場合、ステータスはアップグレードされます。非セキュアな参加者が電話会議に接続すると、その会議は非セキュアとしてレンダリングされます。

会議の状態は、参加者が会議をチェーンするとき、チェーン会議のセキュリティステータスが変更されたとき、別のデバイスで保留中の会議コールが再開されたとき、会議コールが割り込まれたしたとき、または転送されたときに変更することもできます。会議コールは別のデバイスに対して完了します。

（注） Advanced Ad Hoc 会議が有効になっているサービスパラメータは、会議、参加、直接転送、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。

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の会議の開催

アドホック会議のリスト

会議コール中にConfListソフトキーを押すと、参加している電話機に会議リストが表示されます。会議のリストには、会議のステータスと各参加者のセキュリティステータスが表示され、暗号化されていない参加者を識別します。

会議リストには、非セキュア、認証済み、暗号化済み、保留中のセキュリティアイコンが表示されます。会議の開始者は、会議リストを使用して、セキュリティステータスが低い参加者を退出させることができます。

（注） 高度なアドホック会議の有効化サービスパラメータは、会議の開催者以外の会議参加者が会議参加者を追放できるかどうかを決定します。

参加者が会議に参加すると、会議リストの先頭に追加されます。ConfList および RmLstC ソフトキーを使用してセキュアな会議から非セキュアな参加者を削除するには、お使いの電話機のユーザマニュアルを参照してください。

ここでは、他の機能とのセキュアなアドホック会議の相互作用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、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、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した場合は、割り込みターゲットの横にある会議リストに割り込みコールのセキュリティステータスが表示されます。割り込みの発信者には認証済みの接続があるため、割り込みターゲットと会議ブリッジの間でメディアが暗号化されている場合、割り込みターゲット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。

割り込みターゲットがセキュアだが非セキュアなアドホック会議では、アドホック会議のステータスが [セキュア (secure)] に変わると、[割り込み発信者 (割り込み caller)] 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ユーザは、 Cisco Unified IP 電話 (sccp を実行している電話機のみ) で [参加 (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参加できます。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、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。参加している新しいメンバーを追加した参加者は会議の開催者になり、会議リストから新しいメンバーまたは他の参加者を取り出します (高度なアドホック会議が有効になっている設定が True の場合)。

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会議コールを保留にすると、追加された参加者がコールに応答するまで、会議のステータスは [不明 (unknown)] (非セキュア) のままになります。新しい参加者が応答すると、会議リストの会議ステータスが更新されます。

共有回線の発信者が別の電話で開催中の会議コールを再開すると、発信者が [再開 (Resume)] を押すと会議リストが更新されます。

最小セキュリティレベルの会議の開催

管理者は、ミーティングのパターンまたは番号を非セキュア、認証済み、または暗号化済みとして設定するときに、会議の最小セキュリティレベルを指定できます。参加者は最小のセキュリティ要件を満たしている必要があります。または、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、会議コールの転送、共有回線での会議コールの再開、およびチェーン会議に適用されます。

会議室の会議を開始する電話機が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。一致しない場合、システムはその試行を拒否します。最小セキュリティレベルで認証済みまたは暗号化済みが指定されていて、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として非セキュアを指定した場合、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、他の機能とのセキュアな会議の連携動作について説明します。

会議とアドホック会議

会議をアドホック会議に追加したり、会議にアドホック会議を追加したりするには、アドホック会議が会議の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。または、コールがドロップされます。会議アイコンは、会議が追加されたときに変更されることがあります。

ミートミー会議と割り込み

発信者が会議参加者を割り込むときに、割り込みの発信者が最小のセキュリティ要件を満たしていない限り、割り込まれたデバイスのセキュリティレベルがダウングレードし、割り込みの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。

会議の開催と保留/再開

電話機が最小セキュリティレベルを満たしていない限り、共有回線上の電話機が会議の開催を再開することはできません。電話機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 [再開 (Resume)] 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。

Cisco Unified IP 電話 セキュアな会議とアイコンのサポート

これらのCisco Unified IP 電話はセキュアな会議とセキュアな会議のアイコンをサポートしています。

- Cisco Unified IP 電話 7942 および 7962（SCCP のみ、認証済みセキュア会議のみ）
- Cisco Unified IP 電話 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、8945。（SCCP のみ）
- Cisco Unified IP 電話 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。

  Cisco IP 電話 7811、7821、7841、7861、Cisco IP電話 7832、Cisco IP 電話 8811、8841、8845、8851、8851NR、8861、8865、8865nr、Cisco ワイヤレス IP 電話 8821、統一 IP 会議電話機 8831、Cisco IP 会議電話 8832。

警告 セキュア会議機能を十分に活用するため、Cisco Unified IP 電話 をリリース 8.3 以降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された電話は、これらの新機能を完全にはサポートしていません。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 電話 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 電話 に適用されるその他の制限については、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*Cisco IP* 電話 の管理ガイド および *Cisco IP* 電話 ユーザ ガイドを参照してください。

セキュアな会議の CTI サポート

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『*Unified Communications Manager JTAPI Developers Guide*』および『*Unified Communications Manager TAPI Developers Guide*』を参照してください。

トランクとゲートウェイを介したセキュアな会議

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 トランクが含まれている場合、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、オフクラスタ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、電話機の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 ステータスを提供します。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

この項では、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）
• セキュアな会議による Cisco Unified Communications Manager の制約事項 （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、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。

- 会議を安全に保つために、セキュアなアドホック会議の参加者がコールを保留にするか、コールをパークする場合、[MOH を会議ブリッジに抑制 (hold MOH to call 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。セキュアな会議のステータスは変更されません。
- 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、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が

unknown に変わります。クラスタ外の参加者が MOH を使用して保留中の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ることがあります。

- クラスタ間トランク (ICT) を介したセキュアな MeetMe コールは、リモートユーザが保留/再開などの電話機能を起動し、メディアステータスが unknown に変更されたかどうかをクリアします。
- 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 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、RSVP が有効になっている場合、会議はセキュアなままになります。
- PSTN を含む電話会議の場合、セキュリティ会議アイコンには、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。
- Maximum Call Duration Timer サービスパラメータは、会議の最大継続時間も制御します。
- 会議ブリッジはパケットキャプチャをサポートしています。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、電話機には会議の非セキュアステータスが表示されます。
- システムに設定されているメディアセキュリティポリシーによって、セキュアな会議の動作が変更されることがあります。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、エンドポイントはシステム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を使用します。

セキュアな会議による Cisco Unified Communications Manager の制約事項

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

- 暗号化された Cisco IP 電話 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 電話 で、以前のリリースの 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 電話 7800 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 電話 7942 と 7962 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 電話の 79 31g は、会議のチェーンをサポートしていません。
- SIP トランクを介してコールしている電話は、デバイスのセキュリティステータスに関係なく、非セキュアな電話機として扱われます。
- セキュアな電話機が SIP トランクを介してセキュアな会議に参加しようとすると、コールはドロップされます。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 7962G 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の会議リストは表示されません。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会議ソフトキーの横に表示されます。たとえば、h.323 ICT 接続の場合、認証アイコンは表示されません (システムは認証された接続を非セキュアとして扱う) が、暗号化された接続の暗号化アイコンが表示されます。

  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者間コールとして扱います。

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、次の情報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機で表示する場合は、ローカリゼーションを使用します。詳細については、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は、会議コールを保護するために暗号化をサポートする必要があります。
- セキュアな会議ブリッジの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調達するために、会議を開始する電話機が認証または暗号化されていることを確認します。
- 共有回線で会議の整合性を維持するには、異なるセキュリティモードで回線を共有するデバイスを設定しないでください。たとえば、認証済みまたは非セキュアな電話機を使用して回線を共有するように暗号化された電話機を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する場合は、SIP トランクを ICTs として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 [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、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。Unified Communications Manager Administration の設定が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します。
- 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 システムに 1 つ以上の Unified Communications Manager の CallManager.pem 証明書が含まれ、Unified Communications Manager の CallManager の信頼性ストアに 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。X.509 Subject 属性で指定された共通名は、Cisco Unified Communications Manager で定義された会議ブリッジ名から開始し、関連付け**プロファイル < プロファイル識別子 > register < device Name >?**コマンドを使用して DSP ファームシステムで指定する必要があります。サブジェクト代替名属性はサポートされていません。たとえば、証明書サブジェクトの共通名が ?CN=example.cisco.com? の場合、Unified Communications Manager の会議ブリッジ名は ?example? で、DSP ファーム システム コマンドは **?associate profile <profile-identifier> register** example である必要があります。同じ DSP ファームシステム上に複数のセキュアな会議ブリッジがある場合、それぞれに個別の証明書が必要です。

ヒント 会議ブリッジ名が一意であること、および「デバイス」テーブルの下の他の場所で構成できないことを確認してください。これは、ルートリスト、SIP トランク、IP 電話などに適用されます。

- 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 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 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 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、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

次の手順では、ネットワークにセキュアな会議を追加するために使用するタスクについて説明します。

手順

Step 1 CiscoCTL クライアントが混合モードにインストールされ、設定されていることを確認します。

Step 2 信頼ストアへの Unified Communications Manager 証明書の追加も含め、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に設定します。

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 Unified Communications Manager への TLS ポート接続を確立します。

Step 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 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 CiscoCallManager 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 CiscoCallManager サービスを再起動する必要があります。

Step 4 Unified Communications Manager の管理ページで、Cisco IOS Enhanced Conference Bridge を会議ブリッジタイプとして設定し、暗号化済み会議ブリッジ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、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。

Step 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、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。

Step 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 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、階層を SRTP にキャプチャします。

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

[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、Unified Communications Manager の各デバイスをリセットして、CiscoCallManager 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、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。

始める前に

はじめる前に

手順

Step 1　**[Media Resources]** > **[Conference Bridge]** を選択します。

Step 2　[**会議ブリッジの検索と一覧表示**] ウィンドウで、Cisco IOS Enhanced 会議ブリッジがインストールされてセキュアな会議ブリッジのセットアップ（12 ページ）いることを確認し、に進みます。

Step 3　デバイスがデータベースに存在しない場合は、[**新規追加 (Add New)**] をクリックします。に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）進みます。

Step 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、会議ブリッジの名前、説明、デバイスプール、共通デバイス設定、およびロケーション設定を構成します。

Step 5　[Device Security Mode] フィールドで、[**Encrypted 会議ブリッジ**] を選択します。

Step 6　[保存（Save）] をクリックします。

Step 7　[リセット（Reset）] をクリックします。

次のタスク

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。

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

Step 1 **[Call Routing]** > **[Meet-Me Number/Pattern]** を選択します。

Step 2 [会議ブリッジの検索/一覧表示 (Find and List bridge bridge)] ウィンドウで、会議番号/パターンが設定されていることを確認し、セキュアな会議ブリッジのセットアップ（12ページ）に進みます。

Step 3 Meet a の番号/パターンが設定されていない場合は、[**新規追加 (Add New)**] をクリックします。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） に進みます。

Step 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、説明とパーティションの設定を行います。

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

Step 6 [保存（Save）] をクリックします。

次のタスク

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。

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のパケットキャプチャを設定するには、[**サービスパラメータ設定 (Service Parameter Configuration**)] ウィンドウでパケットキャプチャを有効にします。次に、[デバイス設定 (device configuration)] ウィンドウで、パケットキャプチャモードをバッチモードに設定し、電話、ゲートウェイ、またはトランクの SRTP に階層をキャプチャします。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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。