AS-SIP の設定

Assured Services SIP（AS-SIP）エンドポイントは、MLPP、DSCP、TLS/SRTP、および IPv6 の要件に準拠した SIP エンドポイントです。 AS-SIP は、Unified Communications Manager 上で複数のエンドポイント インターフェイスを実現します。 サードパーティ製 AS-SIP エンドポイント デバイス タイプを使用すれば、サードパーティ製 AS-SIP 準拠の汎用エンドポイントを設定して Unified CM で使用できるようになります。

シスコ純正の RoundTable（RT）8961、9951、および 9971 SIP 電話機と対応する Unified CM インターフェイスが AS-SIP 機能を提供するように拡張されています。 RT MLPP の動作では、SCCP MLPP 実装との機能の同等性が維持されます。 Unified CM と RT 電話機間の SIP シグナリング インターフェイスと、Unified CM とサードパーティ製 AS-SIP エンドポイント間のインターフェイスは異なります。 Unified CM は、拡張マークアップ言語（XML）設定ファイルの一部として RT エンドポイントに新しい設定パラメータを送信します。 これらのパラメータは、AS-SIP 機能を有効または無効にしたり、この機能が使用されているときの RT エンドポイントの動作を制御したりします。 また、RT エンドポイントは、特定のコールのリソース プライオリティを示す新しいヘッダーを解釈、処理、および送信します。 RoundTable 機能拡張では、RT エンドポイントと Unified CM 間の TFTP 設定および SIP コール処理の交換に焦点が当てられています。

- AS-SIP の機能，2 ページ
- AS-SIP 回線エンドポイントの設定，2 ページ
- AS-SIP を実行している電話機の設定の違い，4 ページ
- AS-SIP 会議，5 ページ
- Unified Communications Manager によるサードパーティ製電話機の識別，5 ページ
- AS-SIP を実行しているサードパーティ製電話機，6 ページ
- エンド ユーザの設定，6 ページ
- SIP プロファイルの設定項目，7 ページ
- DTMF 受信が必要，8 ページ
- 電話セキュリティ プロファイル設定値の設定，8 ページ
- TLS の設定，8 ページ

• サードパーティ製電話機の追加と設定，8 ページ

AS-SIP の機能

LSC と AS-SIP 回線の要件に従って、サードパーティ製 AS-SIP エンドポイント インターフェイスに対して以下の機能が実装または使用可能になっています。

- MLPP
- TLS
- SRTP
- 優先レベルの DSCP
- エラー応答
- V.150.1 MER
- 会議ファクトリ フローのサポート
- MLPP 認証および許可
- AS-SIP 回線早期オファー

（注） AS-SIP 回線早期オファーを除く上記の機能は、LSC と SIP EI の要件に従って、RT 8961、9951、および 9971 電話機および対応する Unified CM インターフェイスに対しても、実装されているか、使用可能になっているか、またはすでに存在しています。

AS-SIP 回線エンドポイントの設定

Unified CM は、SIP を備えた Cisco Unified IP Phone だけでなく、SIP を実行している RFC3261 準拠のサードパーティ製電話機もサポートしています。この手順は、SIP を実行しているサードパーティ製電話機を手動で設定するためのタスクを示しています。Cisco Unified Communications Manager の管理ページを使用して、サードパーティ製電話機を設定します。

手順

ステップ 1 電話機に関する次の情報を収集します。

- 電話機に関連付ける Unified Communications Manager ユーザの物理ロケーション
- パーティション、コーリング サーチ スペース、およびロケーションの情報（使用する場合）
- 電話機に割り当てる回線および関連 DN の数

ステップ 2 十分なデバイス ライセンス ユニットが使用可能かどうかを調べます。

Unified CM と Unity Connection に関するすべてのライセンスが、Enterprise License Manager 上に保存され、一括管理されます。 詳細については、『*Enterprise License Manager User Guide*』を参照してください。

ステップ 3 ダイジェスト ユーザにするエンド ユーザを設定します。
フィールドの説明については、エンド ユーザの設定値に関するトピックを参照してください。

（注） MLPP 認証（オプション）では、電話機から MLPP ユーザ名とパスワードを送信する必要があります。 エンド ユーザは、許可された最高の MLPP 優先レベルを指定します。 MLPP クレデンシャルはユーザに関連付けられますが、それを使用する必要性はデバイスに関連付けられます（デバイスで使用される SIP プロファイル内の [MLPP認証(Mutilevel Precedence and Preemption Authorization)] チェックボックスによる）。

ステップ 4 SIP プロファイルを設定します。または、デフォルト プロファイルを使用します。 SIP プロファイルは、[電話の設定(Phone Configuration)] ウィンドウを使用して、SIP を実行している電話機に追加されます。
サードパーティ製 AS-SIP 電話機は、電話機固有のパラメータ セクションに含まれる以下のフィールドと一緒に、[SIP設定(SIP Configuration)] ウィンドウの [SIPプロファイル情報(SIP Profile Information)] セクションを使用します。

- [リソースプライオリティネームスペース(Resource Priority Namespace)]
- [MLPPユーザ認証(MLPP User Authorization)]

（注） 電話機固有のパラメータはサードパーティ製 AS-SIP 電話機にダウンロードされません。これらは Unified CM でのみ使用されます。 サードパーティ製電話機では同じ設定値をローカルに設定する必要があります。

詳細については、SIP プロファイルの設定値と Cisco Unified IP Phone の設定に関するトピックを参照してください。

ステップ 5 電話セキュリティ プロファイルを設定します。
ダイジェスト認証を使用するには、新しい電話セキュリティ プロファイルを設定する必要があります。 自動登録用に提供されている標準の非セキュア SIP プロファイルの 1 つを使用する場合は、ダイジェスト認証を使用可能にできません。 詳細については、電話セキュリティ プロファイル設定に関連するトピックと『*Cisco Unified Communications Manager* セキュリティ ガイド』を参照してください。

電話セキュリティ プロファイルは TLS 用に設定する必要があります。 詳細については、「TLS」の項を参照してください。

ステップ 6 [新しい電話機設定の追加(Add a New Phone Configuration)] ウィンドウで [サードパーティAS-SIPエンドポイント(Third-party AS-SIP Endpoint)] を選択して、SIP を実行しているサードパーティ製電話機を追加および設定します。
詳細については、Cisco Unified IP Phone の設定に関するトピックを参照してください。

ステップ 7 電話機に対して回線（DN）を追加し、設定します。
詳細については、電話番号設定に関するトピックを参照してください。

ステップ 8 [エンドユーザの設定(End User Configuration)] ウィンドウで、[デバイスの割り当て(Device Associations)] を使用して、SIP を実行している電話機を選択し、SIP を実行しているサードパーティ製の電話機をユーザに関連付けます。
詳細については、エンドユーザへのデバイスの関連付けに関するトピックを参照してください。

ステップ 9 [電話の設定(Phone Configuration)] ウィンドウの [ダイジェストユーザ(Digest User)] フィールドで、手順 3 で作成したエンドユーザを選択します。

ステップ 10 SIP を実行しているサードパーティ製の電話機を設置して電源をオンにし、ネットワーク接続を確認して、ネットワーク設定を行います。
SIP を実行している電話機に付属のアドミニストレーション ガイドを参照してください。

ステップ 11 AS-SIP を実行しているサードパーティ製の電話機でコールを発信します。
SIP を実行しているサードパーティ製の電話機に付属のユーザ ガイドを参照してください。

AS-SIP を実行している電話機の設定の違い

下の表は、Cisco Unified IP Phone と AS-SIP を実行しているサードパーティ製電話機の設定上の違いを比較したものです。

AS-SIP を実行している電話機	中央集中型 TFTP との統合	MAC アドレスの送信	ソフトキーファイルのダウンロード	ダイヤル プラン ファイルのダウンロード	Unified Communications Manager のフェールオーバーとフォールバックのサポート	リセットと再起動のサポート
Cisco Unified IP Phone 8961、9951、9971	する	する	する	する	する	する
サードパーティ製 AS-SIP デバイス	しない	しない	しない	しない	しない	しない

Unified CM の管理ページを使用して、SIP を実行しているサードパーティ製電話機を設定します（「SIPプロファイルの設定値」の項を参照）。また、管理者は、SIPを実行しているサードパーティ製の電話機上で設定手順を実行する必要もあります。次の例を参照してください。

- 電話機のプロキシ アドレスを Unified Communications Manager の IP アドレスまたは完全修飾ドメイン名（FQDN）にする。

- 電話機の電話番号を、Unified CM の管理ページでデバイスに設定した電話番号と一致させる。
- 電話機のダイジェスト ユーザ ID（認可 ID とも呼ばれる）を、Unified CM の管理ページで設定したダイジェスト ユーザ ID と一致させる。

詳細については、SIP を実行しているサードパーティ製の電話機に付属のマニュアルを参照してください。

AS-SIP 会議

機能の呼び出し元（保留元、転送元、または会議開催者）でシスコ独自の機能シグナリングがサポートされている場合は、MOH がそのターゲット（保留先、転送直前の転送先、または参加直前の会議出席者）に適用されます。 機能の呼び出し元でシスコ独自の機能シグナリングがサポートされていない場合は、MOH がそのターゲットに適用されません。 また、エンドポイントが会議ミキサーであることを明示的に伝達する場合は、MOH がそのターゲットで再生されません。
AS-SIP 会議には次の 2 つの形態があります。

- ローカル混合
- 会議ファクトリ

ローカル混合

Unified CM からは、会議開催者が他の会議参加者のそれぞれに対してアクティブ コールを同時に確立したようにしか見えません。 会議は開催者によってローカルにホストされ、そこで音声が混合されます。 会議開催者からのコールには MOH ソースへの接続を拒否する特殊なシグナリングが含まれています。

会議ファクトリ

会議開催者は SIP トランクの外側に設置された会議ファクトリ サーバを呼び出します。 そして、IVR シグナリングを通して、会議ブリッジを予約するように会議ファクトリに指示します。 会議ファクトリから会議開催者に数値アドレス（ルーティング可能な DN）が返され、会議開催者はブリッジとの登録を確立して、参加者を追跡するための会議リスト情報を受け取ります。 会議ファクトリにより、MOH ソースへの接続を拒否する特殊なシグナリングが送信されます。

Unified Communications Manager によるサードパーティ製電話機の識別

SIP を実行しているサードパーティ製の電話機は MAC アドレスを送信しないため、ユーザ名を使用して自分自身の身元を証明する必要があります。

REGISTER メッセージには次のヘッダーが含まれています。

Authorization: Digest
username=”swhite”,realm=”ccmsipline”,nonce=”GBauADss2qoWr6k9y3hGGVDAqnLfoLk5”,uri
=”sip:172.18.197.224”,algorithm=MD5,response=”126c0643a4923359ab59d4f53494552e”

ユーザ名 swhite は、Unified CM の管理ページの [エンドユーザの設定(End User Configuration)] ウィンドウで設定されたエンド ユーザと一致する必要があります（「エンド ユーザの設定値」を参照）。 管理者は、[電話の設定(Phone Configuration)] ウィンドウの [ダイジェストユーザ(Digest User)] フィールド内のユーザ（swhite など）を使用してサードパーティ製 SIP 電話機を設定します（「Cisco Unified IP Phone の設定」を参照）。

（注） 各エンド ユーザ ID は、（[電話の設定(Phone Configuration)] ウィンドウの [ダイジェストユーザ(Digest User)] フィールドで）1 つのサードパーティ製電話機だけに割り当てることができます。 同じエンド ユーザ ID がダイジェスト ユーザとして複数の電話機に割り当てられている場合、そのエンド ユーザ ID が割り当てられているサードパーティ製電話機は正しく登録されません。

AS-SIP を実行しているサードパーティ製電話機

AS-SIP を実行しているサードパーティ製電話機は、Unified Communications Manager TFTP サーバを使用して設定されません。 お客様が、ネイティブ電話機設定メカニズム（通常は、Web ページまたは tftp ファイル）を使用して、電話機を設定します。 お客様は、Unified Communications Manager データベース内のデバイスおよび回線の設定と、ネイティブ電話機設定の同期を保つ必要があります（たとえば、電話機の内線番号 1002 と Unified Communications Manager の 1002）。 さらに、回線の電話番号が変更された場合、Unified CM の管理ページとネイティブ電話機設定メカニズムの両方でその電話番号が変更されていることを確認してください。

エンド ユーザの設定

Unified CM の管理ページの [エンドユーザの設定(End User Configuration)] ウィンドウを使用すれば、管理者は、Unified Communications Manager のエンド ユーザに関する情報を追加、検索、表示、および保守することができます。 [エンドユーザの設定(End User Configuration)] ウィンドウで電話機を関連付けた後は、エンド ユーザが電話機を制御できます。 MLPP 認証が AS-SIP に対して有効になっている場合は、MLPP 認証をエンド ユーザ管理ページで設定する必要もあります。 この MLPP 認証には、ユーザ識別番号とパスワードが必要です。 MLPP ユーザ識別番号は 6 ～ 20 桁の数字で構成し、MLPP パスワードは 4 ～ 20 桁の数字で構成する必要があります。 優先認証レベルは、[標準(Routine)] から [エクゼクティブオーバーライド(Executive Override)] までの、任意の標準優先レベルに設定できます。

（注） エクステンション モビリティはサードパーティ製 AS-SIP デバイスに対してサポートされていません。

（注） サードパーティ製 AS-SIP デバイスは CAPF をサポートしていません。

SIP プロファイルの設定項目

SIP プロファイルの設定値には、[Assured SIPサービスは有効か(Is Assured SIP Service Enabled)] チェックボックスが含まれます。 このチェックボックスは、サードパーティ製 AS-SIP エンドポイントだけでなく、AS-SIP トランクに対してもオンにする必要があります。 この設定により、特定の Assured Service の動作が会議ファクトリや SRTP などのサービスに影響します。

SIP を実行しているサードパーティ製電話機に対するダイジェスト認証の有効化

SIP を実行しているサードパーティ製の電話機のダイジェスト認証を使用可能にするには、管理者が電話セキュリティプロファイルを作成する必要があります（一般的な説明については、「電話機のセキュリティ プロファイルの設定」の項を参照してください。詳細については、『Unified Communications Manager セキュリティ ガイド』を参照してください）。[電話セキュリティプロファイルの設定(Phone Security Profile Configuration)] ウィンドウで、[ダイジェスト認証を有効化(Enable Digest Authentication)] チェックボックスをオンにします。 セキュリティ プロファイルの設定後、管理者は、[電話の設定(Phone Configuration)] ウィンドウを使用して、そのセキュリティ プロファイルを SIP を実行している電話機に割り当てる必要があります。 このチェックボックスがオフになっている場合は、Unified CM では、エンドユーザ ID で電話機を識別するためにダイジェスト認証を使用し、ダイジェスト パスワードは確認しません。 このチェックボックスがオンになっている場合は、Unified CM ではパスワードを確認します。

DTMF 受信

デュアル トーン多重周波数（DTMF）受信を要求するには、Unified CM の管理ページの [電話の設定(Phone Configuration)] ウィンドウに表示される [DTMF受信が必要(Require DTMF Reception)] チェックボックスをオンにします。

電話機のセキュリティ プロファイルの設定

Unified CM の管理ページで、[システム(System)] > [セキュリティ(Security)] > [電話セキュリティプロファイル(Phone Security Profile)] メニュー パスを使用して、電話セキュリティ プロファイルを設定します。

[電話セキュリティプロファイル(Phone Security Profile)] ウィンドウに含まれているセキュリティ関連の設定値には、デバイス セキュリティ モード、Certificate Authority Proxy Function （CAPF）の設定値、ダイジェスト認証の設定値（SIP を実行している電話機のみ）、暗号化された設定ファイルの設定値などがあります。 セキュリティ プロファイルは、Unified CM の管理ページで設定したすべての電話機に適用する必要があります。

DTMF 受信が必要

電話セキュリティ プロファイル設定値の設定

TLS の設定

サードパーティ製 AS-SIP デバイスの TLS については、『Unified Communications Operating System Administration Guide』の「Security」の章に記載された手順を使用して、コール マネージャを正しく設定してください。

証明書の作成に関するローカル手順にも従う必要があります。

電話セキュリティ プロファイルの設定と適用に関する詳細については、『Unified Communications Manager セキュリティ ガイド』を参照してください。

サードパーティ製電話機の追加と設定

AS-SIP デバイスの追加と設定は、既存のサードパーティ製デバイス タイプの場合とほぼ同一です。 ただし、若干の違いがあります。 AS-SIP デバイス タイプには次のような特徴があります。

- MLPP 用に設定できます。
- セキュリティ プロファイル内にオプションのデバイス セキュリティ モードが含まれています。
- サードパーティ製 AS-SIP デバイスの場合は、Unified CM 上のプリエンプション設定を使用できません。 この設定はサードパーティ製電話機によって完全に制御されます。
- 音声コールとビデオ コールに対する早期オファーをサポートしています。

（注） 音声コールとビデオ コールに対する早期オファー サポートから着信側に初期 INVITE 内の SDP オファーが送信されます。

早期オファーがデバイスに対して有効になっており、Unified CM が遅延オファー コールを想定している場合は、MTP の挿入を避けるためにメディア リソース グループ リストを設定する必要があります。

以下の手順を使用して、メディア リソース グループ リストを設定します。

手順

ステップ 1 CUCM の管理ページで、[メディアリソース(Media Resources)]>[メディアリソースグループ(Media Resource Group)] を選択します。

ステップ 2 [新規追加(Add New)] ボタンをクリックして、新しいメディア リソース グループ リストを追加します。

ステップ 3 [メディアリソースグループリスト(Media Resource Group List)] で、Unified CM ベースのソフトウェア MTP だけをメディア リソース グループ（MRG）に追加します。 通常、Unified CM ソフトウェア リソースには MTP_# という名前が付けられます。ここで、# は番号です（「MTP_2」など）。

ステップ 4 Unified CM のすべてのソフトウェア MTP リソースが含まれているこのメディア リソース グループは、メディア リソース グループ リスト（MRGL）に適用しないでください。 MTP リソースを MRG 内に配置して、MRGL 内に配置しないことにより、これらの MTP リソースがシステム上のどのデバイスからも使用できなくなるため、この方法が推奨されています。

（注） システム上でハードウェア MTP リソースが（デフォルト以外で）設定されている場合も、同じ手順を使用してこれらのリソースを使用できないようにする必要があります。

サードパーティ製電話機の追加と設定に関する詳細については、『CUCM アドミニストレーション ガイド』の「Cisco Unified IP Phone の設定」を参照してください。