プロトコル

ここでは、SIP および H.323 プロトコルをサポートするように Expressway を設定する方法について説明します。

（注） SIP および H.323 プロトコルは、X8.9.2 以降の新しいバージョンのインストールではデフォルトで無効になっています。**[設定（Configuration）]** > > **[プロトコル（Protocols）]** のページを使用して、それらを有効にします。

H.323 について

Expressway は H.323 プロトコルをサポートします。これは H.323 ゲートキーパーです。

Expressway は、H.323 と SIP 間のSIP および H.323 のインターワーキングの設定も可能にします。これら 2 つのプロトコル間で変換を行って、これらのプロトコルのいずれかしかサポートしないエンドポイントが互いにコールできるようにします。H.323 をサポートするには、**H.323 モード**を有効にする必要があります。

H.323 ゲートキーパーとしての Expressway の使用

H.323 ゲートキーパーとして、Expressway は H.323 からの登録を受け入れ、アドレス変換やアドミッション制御などのコール制御機能を提供します。

H.323 ゲートキーパーとして Expressway を有効にするには、**[H.323 モード（H.323 mode）]** を *[オン（On）]* に必ず設定してください（**[設定（Configuration）]**>**[プロトコル（Protocols）]**> **[H.323]**）。

H.323 エンドポイントの登録

ネットワーク内の H.323 エンドポイントが Expressway をゲートキーパーとして使用するには、エンドポイントを Expressway に登録する必要があります。

登録先の Expressway を H.323 エンドポイントが見つけるには、2 つの方法があります。

- 手動
- 自動

このオプションは、[ゲートキーパーの検出（Gatekeeper Discovery）] の設定で、エンドポイント自体に設定します（この設定へのアクセス方法については、エンドポイントのマニュアルを参照してください）。

- モードが自動に設定されている場合は、検出できる Expressway にエンドポイントが登録しようとします。これは、Gatekeeper Discovery Request（ゲートウェイ検出要求）を送信し、適格な Expressway がそれに応答することによって行われます。
- モードが手動に設定されている場合は、エンドポイントを登録する Expressway の IP アドレスを指定する必要があり、エンドポイントはその Expressway のみに登録しようとします。

自動 H.323 登録の回避

Expressway への H.323 エンドポイントの自動登録を回避することができます。これには、Expressway で **[自動検出（Auto Discovery）]** を無効にします（**[設定（Configuration）]** > **[プロトコル（Protocols）]** > **[H.323]**）。

登録の更新

H.323 の [存続時間（Time to live）] 設定で、H.323 エンドポイント登録の更新頻度を制御します。更新頻度は、存続時間が減少すると高くなります。H.323 エンドポイントが多数ある場合は、TTL ツールを低く設定しすぎないように注意してください。大量の登録要求によって Expressway のパフォーマンスに不要な影響を与えます。

H.323 の設定

[設定（Configuration）] > **[プロトコル（Protocols）]** > **[H.323]**を選択し、Expressway の H.323 について 設定を指定します。

設定可能なオプションは次のとおりです。

フィールド	説明	使用方法のヒント
H.323 モード（H.323 Mode）	Expressway で H.323 を有効または無効にします。デフォルトでは、H.323 サポートは *[オフ（Off）]* になっています。	導入する際に H.323 エンドポイントがなくても、Expressway をクラスタリングする場合は H.323 モードを有効にする必要があります。
登録 UDP ポート（Registration UDP port）	H.323 UDP 登録用のリスニング ポート。	デフォルトの Expressway 設定では標準的なポート番号を使用します。そのため、最初に設定を行うことなく、そのままで H.323 サービスを使用できます。
登録競合モード（Registration conflict mode）	エンドポイントが別の IP アドレスから現在登録されているエイリアスの登録を試行した場合のシステムの動作を決定します。 *[拒否（Reject）]*：新しい登録を拒否します。これはデフォルトです。 *[上書き（Overwrite）]*：元の登録を削除して、新しい登録に置き換えます。	H.323 エンドポイントは、別の IP アドレスから Expressway にすでに登録されているエイリアスを使用して Expressway に登録しようとする可能性があります。次のようなことがこの理由として考えられます。 • 異なる IP アドレスのエンドポイントが同じエイリアスを使用して登録しようとしている。 • 以前に、単一のエンドポイントが特定のエイリアスを使用して登録されていた。エンドポイントに割り当ててから変更する IP アドレスとエンドポイントが同じエイリアスを使用して再登録しようとしている。 *[拒否（Reject）]* は、プライオリティによって 2 人のユーザが同じエイリアスを使用して登録することを防ぐ場合に役立ちます。*[上書き（Overwrite）]* は、不要な登録拒否を回避するためにエンドポイントに新しい IP アドレスが頻繁に割り当てられるネットワークの場合に役立ちます。 （注） クラスタでは、登録競合は、同じピアで登録要求を受信した場合にのみ検出されます。
コール シグナリング TCP ポート（Call signaling TCP port）	H.323 コール シグナリング用のリスニング ポート	

フィールド	説明	使用方法のヒント
コール シグナリング ポートの範囲の開始（Call signaling port range start）と終了（end）	H.323 コールの確立後に使用するポート範囲を指定します。	コール シグナリング ポートの範囲は、必要なすべての同時発生コールをサポートするのに十分なものである必要があります。
存続可能時間（Time to live）	H.323 エンドポイントが現在も機能していることを確認するために Expressway に再登録する必要がある間隔（秒単位）。 デフォルトは 1800 です。	古いエンドポイントの中には、システムへの定期的な再登録機能をサポートしないものもあります。この場合や指定した期間内にエンドポイントからの確認をシステムが受けなかった場合は、IRQ をエンドポイントに送信して現在も機能していることを確認します。 （注） 登録の存続時間を短縮しすぎると、登録要求が Expressway へ大量に送り付けられるリスクがあり、パフォーマンスに重大な影響を及ぼします。この影響はエンドポイントの数に比例します。したがって、パフォーマンスを良好に保つ必要性に対して、不定期に発生するフェールオーバーの必要性とのバランスをとることが必要です。
コール存続時間（Call time to live）	Expressway がコール中のエンドポイントをポーリングし、まだコール中であることを確認するための間隔（秒単位） デフォルトは 120 です。	エンドポイントが応答しない場合、そのコールは切断されます。 コール タイプがトラバーサルか非トラバーサルかに関係なく、コール中のエンドポイントがポーリングされます。
自動検出（Auto discover）	エンドポイントが送信した H.323 についてに応答するかどうかを決定します。 デフォルトは [On] です。	H.323 エンドポイントが Expressway に自動的に登録されることを回避するには、**[自動検出（Auto discover）]** を *[オフ（Off）]* に設定します。つまり、**[ゲートキーパーの検出（Gatekeeper Discovery）]** の設定値が *[手動（Manual）]* になっており、エンドポイントが Expressway の IP アドレスで設定されている場合は、それらのエンドポイントのみを Expressway に登録できます。

フィールド	説明	使用方法のヒント
発信者 ID（Caller ID）	ISDN ゲートウェイのプレフィックスを宛先のエンドポイントに提供される発信者の E.164 番号に挿入するかどうかを指定します。	プレフィックスを含めると、受信者はコールを直接返せます。

SIP について

Expressway は SIP プロトコルをサポートします。SIP レジストラ、SIP プロキシ、および SIP Presence Server として機能します。Expressway は SIP と H.323 の間にインターワーキングを実現し、これら 2 つのプロトコル間で変換を行って、これらのプロトコルのいずれかしかサポートしないエンドポイントが相互にコールできるようにします。

SIP をサポートするには、次の手順を実行します。

- SIP の設定を有効にする必要があります。
- 少なくても、1 つ以上の SIP トランスポート プロトコル（UDP、TCP、または TLS）がアクティブである必要があります。

（注） SIP メッセージのサイズは単一の UDP パケットよりも大きい場合が多いため、ビデオでの UDP の使用は推奨しません。

INVITE や SUBSCRIBE など、ルート セットを含むダイアログを形成する要求は拒否されます。ルートセットを含んでいない要求は、既存のコール処理ルールに従って、通常どおりにプロキシ経由で送信されます。

SIP レジストラとしての Expressway

エイリアスを介して接続可能な SIP エンドポイントについては、レコードのアドレス（AOR）とその場所を SIP レジストラに登録する必要があります。SIP レジストラはエンドポイントの AOR に対するエンドポイントの詳細を保持します。AOR はエンドポイントへの接続が可能なエイリアスです。これは SIP URI であり、常に **username@domain** の形式をとります。

その AOR 宛のコールを受信すると、SIP レジストラはレコードを参照して対応するエンドポイントを検索します

（注） 複数の SIP エンドポイントが同じ AOR を同時に使用できます。ただし、すべてのエンドポイントが検出されるようにするには、それらのエンドポイントすべてを同じ Expressway または Expressway クラスタに登録する必要があります。

SIP レジストラは、それ自体が権限を持つドメインでの登録のみを受け入れます。Expressway は最大 200 のドメインの SIP レジストラとして機能します。Expressway を SIP レジストラとして機能させるには、その Expressway が権限を持つことになる ドメインの設定でその Expressway を設定する必要があります。これにより、そのドメインに対して登録しようとするすべてのエンドポイントに対する登録要求が VCS によって処理されます。

（注） また、Expressway は AOR のドメインの部分が FQDN でも Expressway の IP アドレスでも登録要求を受け入れます。Expressway が登録要求を受け入れるかどうかは、登録制御の設定によって異なります。

ユニファイドコミュニケーション導入環境では、SIP デバイスのエンドポイント登録は Unified CM により行われることがあります。このシナリオでは、Expressway が Unified CM 登録にセキュアなファイアウォールトラバーサルと回線側サポートを提供します。ドメイン設定時は、ドメインに登録とプロビジョニングのサービス提供元を Cisco Unified Communications Manager と Expressway から選択できます。

SIP エンドポイント登録

登録する レジストラ を SIP エンドポイントが見つけるには、手動と自動の 2 つの方法があります。このオプションは、SIP の **[サーバ検出（Server Discovery）]** オプションでエンドポイント自体に設定されます（この設定へのアクセス方法については、エンドポイントのマニュアルを参照してください。**プロキシ検出**と呼ばれる場合もあります）。

- **[サーバ検出（Server Discovery）]** モードが自動に設定されている場合、エンドポイントはエンドポイントが登録を試行するドメインに対する権限を持つ SIP サーバに REGISTER メッセージを送信します。たとえば、エンドポイントを **john.smith@example.com** という URI で登録しようとしている場合、その要求は **example.com** ドメインに対する権限があるレジストラに送信されます。エンドポイントは、ビデオ通信ネットワークの実装方法に応じて、DHCP や DNS、またはプロビジョニングなどのさまざまな方法で適切なサーバを検出できます。
- **[サーバ検出（Server Discovery）]** モードが手動に設定されている場合は、登録するレジストラ（Expressway または Expressway クラスタ）の IP アドレスまたは FQDN を指定する必要があります。これにより、エンドポイントはそのレジストラのみに登録を試行します。

Expressway は SIP サーバであり、かつ、SIP レジストラです。

- エンドポイントを Expressway に登録すると、Expressway はそのエンドポイントにインバウンド コールを転送できるようになります。

- Expressway が SIP ドメインを使用して設定されていない場合、その Expressway は SIP サーバとして機能します。**[SIP 登録プロキシモード（SIP registration proxy mode）]** の設定に応じて、Expressway はプロキシとして登録要求を別のレジストラに送信する場合があります。

登録更新間隔

システム上での通常レベルのアクティブな登録数に応じて、**[標準的な登録更新戦略（Standard registration refresh strategy）]** を *[変動（Variable）]* に設定し、次のように更新間隔を設定することができます。

アクティブな登録数	最小更新間隔	最小更新間隔
1 ～ 100	45	60
101 ～ 500	150	200
501 ～ 1,000	300	400
1,000 ～ 1,500	450	800
1500+	750	1000

（注） H.323 エンドポイントと SIP エンドポイントが混在している場合、Expressway が H.323 登録要求と SIP 登録要求の両方を受信する数が多すぎると、それらによって Expressway のパフォーマンスが低下する可能性があります。H.323 の設定を参照してください。

登録の復元力を確保する場合は、SIP アウトバウンド登録を次で説明するように使用します。

SIP 登録の復元力

Expressway は RFC 5626 に概説されているように、複数のクライアント発信接続（「「SIP アウトバウンド」」とも呼ばれる）をサポートします。

これにより、*RFC 5626* をサポートする SIP エンドポイントが複数の Expressway クラスタ ピアに同時に登録できます。その結果、復元力が向上します。エンドポイントがあるクラスタ ピアとの接続を損失した場合でも、別の登録接続の 1 つを介してコールを受信できます。

SIP プロキシ サーバとしての Expressway

[SIP モード（SIP mode）] が有効になっている場合、Expressway は SIP プロキシ サーバとして機能します。プロキシ サーバの役割は、エンドポイントまたは他のプロキシ サーバから要求（REGISTER や INVITE など）をプロキシ サーバや宛先のエンドポイントにさらに転送することです。

SIP プロキシサーバとしての Expressway の動作は、以下により決定されます。

- SIP 登録プロキシモードの設定
- 要求ヘッダー内のルート セット（Route Set）情報の存在
- 要求を送信したプロキシ サーバが Expressway のネイバーかどうか

ルートセット（Route Set）は、エンドポイントとレジストラ間で要求をプロキシ経由で送信するときに使用するパスを指定します。たとえば、REGISTER 要求がプロキシとして Expressway から送信されると、Expressway はパス ヘッダー コンポーネントをこの要求に追加します。これにより、そのエンドポイントへのコールは Expressway を通過するルーティングが必要であることが示されます。通常、これはファイアウォールが存在しており、シグナリングが指定されたパスを移動してファイアウォールを正常に通過しなければならない場合に必要です。パス ヘッダーの詳細については、RFC 3327 を参照してください。

ルート セット（Route Set）の情報が含まれている要求を Expressway がプロキシとして送信する場合は、パスに指定された URI に直接転送します。Expressway に設定されたすべてのコール処理ルールはバイパスされます。これは、ルートセットの情報が信用できない場合はセキュリティ上のリスクがある可能性があります。そのため、ルート セットを含んでいる要求を Expressway がプロキシとして送信する方法を **[SIP 登録プロキシ モード（SIP registration proxy mode）]** で次のように設定できます。

- *[オフ（Off）]*：ルートセットを含む要求を拒否します。この設定は、最も高いレベルのセキュリティを提供します。
- *[既知のみにプロキシ経由で送信（Proxy to known only）]*：既知のゾーンから要求を受信した場合にのみ、ルート セットを含んだ要求をプロキシ経由で送信します。
- *[任意の場所にプロキシ経由で送信（Proxy to any）]*：ルートセットを含んだ要求を常にプロキシ経由で送信します。

いずれの場合も、ルートセットを含んでいない要求は、既存のコール処理ルールに従って、通常どおりにプロキシ経由で送信されます。この設定は、INVITE や SUBSCRIBE など、ダイアログを形成する要求にのみ適用されます。NOTIFY などの他の要求は、この設定に関係なく、常にプロキシ経由で送信されます。

登録要求のプロキシ経由での送信

レジストラとして機能していない（Expressway に SIP ドメインが設定されていない）ドメイン宛の登録要求を Expressway が受信した場合は、Expressway はプロキシとしてその登録要求をさらに先に送信する場合があります。これは、[SIP 登録プロキシ モード（SIP registration proxy mode）] の設定により次のように異なります。

- *[オフ（Off）]*：Expressway は登録要求をプロキシ経由で送信しません。「「403 Forbidden」」メッセージで拒否されます。
- *[既知のみにプロキシ経由で送信（Proxy to known only）]*：Expressway はプロキシとして既存のコール処理ルールに従って要求を送信しますが、送信先は既知のネイバー、トラバーサル クライアント、およびトラバーサル サーバ ゾーンのみです。

- *[任意の場所にプロキシ経由で送信（Proxy to any）]*：これは、[既知の場所にプロキシ経由で送信（Proxy to known only）] と同じですが、すべてのゾーンタイプ、つまり *ENUM* ゾーンや *DNS* ゾーンにも送信します。

プロキシ経由の登録の許可

Expressway がプロキシ経由で送信された登録要求を受け取った場合、Expressway の標準的な登録制御の他に、要求を受け取ったゾーンに応じて Expressway が登録を受け入れるかどうかも制御できます。これを行うには、**[プロキシ経由の登録を許可（Accept proxied registrations）]** をゾーンの設定時に設定します。

プロキシ経由で送信された登録は、プロキシ経由で最後に送信されたゾーンに属するものとして分類されます。これは、Expressway 内のサブゾーンに割り当てられるプロキシ経由で送信されていない登録要求とは異なります。

SIP プレゼンス サーバとしての Expressway

Expressway は、SIP ベースの SIMPLE プロトコルをサポートします。このような VCS は権限を持つ SIP ドメインのプレゼンス サーバおよびプレゼンス ユーザ エージェントとして機能することができます。Expressway を SIP プレゼンス サーバとして有効にして使用する方法について詳しくは、プレゼンスの項を参照してください。

SIP の設定

[SIP] ページ（[設定（Configuration）] > [プロトコル（Protocols）] > [SIP]） を使用して、次を含めて、Expressway 上で SIP の設定値を設定します。

- SIP 機能と SIP 固有のトランスポート モードおよびポート
- TLS 接続の証明書失効確認モード
- 標準的な登録およびアウトバンド登録の登録制御

SIP 機能と SIP 固有のトランスポート モードおよびポート

ここでは、SIP 機能を有効にし、SIP 固有のさまざまなトランスポート モードとポートを設定するための基本的な設定について説明します。設定可能なオプションは次のとおりです。

フィールド	説明	使用方法のヒント
SIP モード（SIP mode）	Expressway で SIP 機能（SIP レジストラおよび SIP プロキシ サービス）を有効または無効にします。 デフォルトは [オフ（Off）] です。	プレゼンス サーバまたはプレゼンス ユーザ エージェントのいずれかを使用するには、このモードを有効にする必要があります。

フィールド	説明	使用方法のヒント
SIP プロトコルとポート（SIP protocols and ports）	Expressway は **UDP**、**TCP**、および **TLS** 転送プロトコルを使用した SIP をサポートします。**[モード（Mode）]** 設定と **[ポート（Port）]** 設定を使用して、前述のプロトコルを使用した着信接続と発信接続をサポートするかどうかを設定します。サポートする場合は、Expressway がこれらの接続をリッスンするポートです。 デフォルトのモードは次のとおりです。 • UDP モード：オフ • TCP モード：オフ • TLS モード：オン • 相互 TLS モード：オフ	SIP機能を有効にするには、トランスポート プロトコルの 1 つ以上を *[オン（On）]* にする必要があります。 TLS と MTLS の両方を使用する場合は、別々のポートで有効にすることをお勧めします。MTLS にポート 5061 を使用する場合は、**[メディア暗号化モード（Media encryption mode）]** を *[自動（Auto）]* に切り替えてB2BUA を関与を防ぐ必要があります。
TCP アウトバウンド ポートの開始/終了（TCP outbound port start/end）	TCP 接続と TLS 接続が確立されたときに Expressway が使用するポートの範囲。	必要な同時発生接続すべてをサポートするのに十分な範囲である必要があります。
セッション更新間隔（Session refresh interval）	SIP コールのセッション更新要求間に許容される最大時間。デフォルトは 1800 秒です。	詳細については、*RFC 4028* の *Session-Expires* の定義を参照してください。
最小セッション更新間隔（Minimum session refresh interva）	SIP コールのセッション更新間隔を Expressway がネゴシエートする最小値。デフォルトは 500 秒です。	詳細については、*RFC 4028* の *Min-SE header* の定義を参照してください。
TLS ハンドシェイクのタイムアウト（TLS handshake timeout）	TLS ソケットのハンドシェイクのタイムアウト時間。デフォルトは 5 秒です。	TLS サーバ証明書の検証が遅く（OCSP サーバがタイムリーに応答を返さないなど）、そのために接続試行がタイムアウトになる場合は、この値を引き上げることができます。

証明書失効確認モード

ここでは、SIP TLS 接続の証明書失効確認モードについて説明します。設定可能なオプションは次のとおりです。

フィールド	説明	使用方法のヒント
Certificate revocation checking mode	失効確認が SIP TLS 接続の確立時に交換された証明書に対し実行されるかどうかを制御します。	失効確認をイネーブルにすることを推奨します。
Use OCSP	Online Certificate Status Protocol（OCSP）を証明書失効確認を実行するために使用するかどうかを制御します。	OCSP を使用するには、以下の条件が必要です。 • チェック対象の X.509 証明書に OCSP レスポンダの URI が含まれている必要があります。 • OCSP レスポンダーは、SHA-256 ハッシュアルゴリズムをサポートしている必要があります。サポートされていない場合、OCSP 失効チェックと証明書検証は失敗します。
Use CRLs	証明書失効リスト（CRL）を証明書失効確認を実行するために使用するかどうかを制御します。	CRL は、証明書が OCSP をサポートしていない場合に使用できます。 CRL は手動で Expressway にロードしたり、事前に設定された URI から自動的にダウンロードしたりできます（「証明書失効リスト（CRL）の管理」を参照）あるいは、X.509 証明書に含まれている CRL 配布ポイント（CDP）URI からも自動的にダウンロードすることもできます。
Allow CRL downloads from CDPs	X.509 証明書に含まれる CDP URI からの CRL のダウンロードを許可するかどうかを制御します。	

フィールド	説明	使用方法のヒント
Fallback behavior	たとえば、失効の送信元に連絡を取れないなど、失効ステータスを確立できない場合に、失効確認の動作を制御します。 *[*失効として処理（*Treat as revoked*）*]*：証明書を失効したとして処理します（そのため、TLS 接続を許可しません）。 *[*失効していないものとして処理（*Treat as not revoked*）*]*：失効していないものとして証明書を処理します。 デフォルト：*[*失効していないものとして処理（*Treat as not revoked*）*]*。	*[*失効していないものとして処理（*Treat as not revoked*）*]*では、失効の送信元に連絡をとれない場合、システムは通常の方法で稼働し続けますが、失効した証明書が承認される可能性があることを意味します。

登録制御

ここでは、標準的な SIP 登録とアウトバウンド SIP 登録の登録制御について説明します。設定可能なオプションは次のとおりです。

フィールド	説明	使用方法のヒント
標準的な登録更新戦略（Standard registration refresh strategy）	標準的な登録に SIP 登録の有効期限（SIP エンドポイントを再登録してその登録の期限切れを回避する期間）の生成に使用する方法。 *Maximum*：設定した**最大**更新値と登録で要求された値のうちの小さいほうを使用します。 *Variable*：設定した**最小**更新値と、設定した**最大**更新値と登録で要求された値のいずれか小さいほうの値の間でランダム値を生成します。 デフォルトは [最大（Maximum）] です。	*[*最大（*Maximum*）*]* の設定では、指定した最大と最小の範囲内であれば、要求された値を使用します。 *[*変動（*Variable*）*]* 設定では、負荷を継続的に分散するように、各登録（および再登録）要求にランダムの更新期間を計算します。Expressway は要求された値よりも大きい値を返すことはありません。 これは、Expressway に登録されたエンドポイントのみに適用されます。Expressway を経由して送信された登録のエンドポイントには適用されません。

フィールド	説明	使用方法のヒント
標準的な登録更新の最小値（Standard registration refresh minimum）	標準的な登録についての SIP 登録更新期間の最小許容値。これよりも小さな値の要求は、「423 Interval Too Brief」応答で登録が拒否されます。デフォルトは 45 秒です。	登録更新間隔を参照してください。
標準的な登録更新の最大値（Standard registration refresh maximum）	標準的な登録についての SIP 登録更新期間の最大許容値。これよりも大きな値の要求では、小さな値が返されることになります（[標準的な登録更新戦略（Standard registration refresh strategy）] に従って計算されます）。デフォルトは 60 秒です。	
アウトバウンド登録更新戦略（Outbound registration refresh strategy）	アウトバウンド登録についての SIP 登録有効期限の生成に使用する方法。 *Maximum*：設定した**最大**更新値と登録で要求された値のうちの小さいほうを使用します。 *Variable*：設定した**最小**更新値と、設定した**最大**更新値と登録で要求された値のいずれか小さいほうの値の間でランダム値を生成します。 デフォルトは [変動（Variable）] です。	これらのオプションは、[標準的な登録更新戦略（Standard registration refresh strategy）] と同様に動作します。 ただし、アウトバウンド登録では、標準的な登録よりもかなり大きな最大値を使用できます。これは、標準的な登録が再登録メカニズムを使用してサーバとの接続を有効に保つためです。アウトバウンド登録では、キープアライブプロセスはリソースの消費が少ない別のプロセスで処理され、再登録（リソースの消費が多い）の頻度を低くできます。
アウトバウンド登録更新の最小値（Outbound registration refresh minimum）	アウトバウンド登録についての SIP 登録更新期間の最小許容値。これよりも小さな値の要求は、「423 Interval Too Brief」応答で登録が拒否されます。デフォルトは 300 秒です。	

フィールド	説明	使用方法のヒント
アウトバウンド登録更新の最大値（Outbound registration refresh maximum）	アウトバウンド登録についての SIP 登録更新期間の最大許容値。これよりも大きな値の要求では、小さな値が返されることになります（[アウトバウンド登録更新戦略（Outbound registration refresh strategy）] に従って計算されます）。デフォルトは 3600 秒です。	
SIP 登録プロキシモード	Expressway がレジストラとして機能していないドメイン宛の登録要求を受信したときに、プロキシ経由の登録とルートセットを含んだ要求をどのように処理するかを指定します。 *[オフ（Off）]*：登録要求はプロキシ経由で送信されません（ただし、Expressway がそのドメインのレジストラとしての権限がある場合は、ローカルで許可されます）。既存のルートセットを含む要求は拒否されます。 *[既知のみにプロキシ経由で送信（Proxy to known only）]*：既存のコール処理ルールに従ってプロキシ経由で登録を送信しますが、送信先は既知のネイバー、トラバーサルクライアント、およびトラバーサルサーバゾーンのみです。既知のゾーンから要求を受信した場合にのみ、ルートセットを含んだ要求をプロキシ経由で送信します。 *[任意の場所にプロキシ経由で送信（Proxy to any）]*：既存のコール処理ルールに従って、登録要求を既知のすべてのゾーンに送信します。ルートセットを含んだ要求は常にプロキシ経由で送信します。 デフォルトはオフです。	詳細については、登録要求のプロキシ経由での送信を参照してください。

認証制御

ここでは、委任クレデンシャル チェックを有効にする場合のデバイス認証について説明します。設定可能なオプションは次のとおりです。

フィールド	説明	使用方法のヒント
委任クレデンシャル チェック（**Delegated credential checking**）	SIP メッセージのクレデンシャル チェックをトラバーサル ゾーンを介して別の Expressway に委任するかどうかを制御します。 *[オフ（Off）]*：認証チャレンジを実行する Expressway で関連クレデンシャル チェックのメカニズム（ローカルデータベース、Active Directory サービスまたは LDAP を介して H.350 ディレクトリ）を使用します。 *[オン（On）]*：クレデンシャルチェックをトラバーサルクライアントに委任します。 デフォルトはオフです。	（注） 委任されたクレデンシャルチェックは、トラバーサル サーバとトラバーサルクライアントの両方で有効にする必要があります。 詳細については、「委任クレデンシャル チェック」を参照してください。

SIP 詳細設定

フィールド	説明	使用方法のヒント
SIP の最大サイズ（SIP max size）	サーバが処理できる SIP メッセージの最大サイズ（バイト単位）を指定します。 デフォルトは 32,768 バイトです。	Expressway と MeetingServer を使用して Microsoft をデュアルホーム会議と相互運用していて、AVMCU が Microsoft 側で呼び出される場合は、32768 以上の値を指定することを推奨します。
SIP TCP 接続のタイムアウト（SIP TCP connect timeout）	発信 SIP TCP 接続が確立されるまで待機する最大秒数を指定します。 デフォルトは 10 秒です。	この値を引き下げると、切断ルート（SIP プロキシ ピアへ送信できないなど）の試行から良好なルートへフェールオーバーするまでの時間を短縮できます。 高遅延ネットワークの場合は、接続を確立するための時間を十分に残しておくよう注意してください。

破損した/不正な SIP メッセージ（CLI）に対する接続の維持

X8.11 以降、（Web ユーザ インターフェイスではなく）CLI コマンドを使用して、不正な、または破損した SIP メッセージを受信したとしても接続を開いたままにするようにオプションで Expressway を設定できます。これは、必須ではないヘッダーのみに指定することも、必須ヘッダーにも指定することもできます。Zones Zone [1..1000] Neighbor RetainConnectionOnParseErrorMode: <mode> を参照してください。

ドメインの設定

「ドメイン（Domains）」ページ（**[設定（Configuration）]>[ドメイン（Domains）]**）にこの Expressway が管理する SIP ドメインのリストが表示されます。

ドメイン名は複数のレベルで構成できます。各レベルの名前に使用できるのは文字、数字、ハイフンのみで、各レベルはピリオド（ドット）で区切ります。レベル名はハイフンで開始または終了できません。また、最後のレベル名は文字で開始する必要があります。有効なドメインの例としては、**100.example-name.com** などがあります。

（注） **Index** カラムに示されている値は **%localdomain1%, %localdomain2%、. . %localdomain200%** パターン マッチング変数の数値要素に対応します。

最大 200 のドメインを設定できます。

（注） Expressway-E ではドメインを設定できません。

ユニファイド コミュニケーションのサポート対象のサービスの設定（Expressway-C のみ）

Expressway-C をユニファイド コミュニケーションのモバイルおよびリモート アクセス用に設定する場合は、各ドメインがサポートするサービスを選択する必要があります。次のオプションがあります。

- **Expressway での SIP 登録とプロビジョニング**：Expressway が、この SIP ドメインに対する権限を持ちます。Expressway はこのドメインの SIP レジストラとして（および VCS システムの場合はプレゼンス サーバとしても）機能し、このドメインを含むエイリアスの登録を試みるすべての SIP エンドポイントの登録要求を受け入れます。デフォルトは [On] です。
- **Unified CM での SIP 登録およびプロビジョニング**：この SIP ドメインのエンドポイントの登録、コール制御およびプロビジョニングのサービスが Unified CM によって提供されます。Expressway はユニファイド コミュニケーション ゲートウェイとして機能し、Unified

CM登録にセキュアなファイアウォール トラバーサルおよび回線側のサポートを提供します。デフォルトはオフです。

- **IM and Presence Service**：この SIP ドメインのインスタントメッセージングおよびプレゼンス サービスは、Unified CM IM and Presence サービスによって提供されます。デフォルトはオフです。
- **XMPP フェデレーション**：このドメインとパートナードメイン間でXMPPフェデレーションを有効化します。デフォルトはオフです。
- **展開**：複数の展開がある場合は、ドメインと、選択された展開を関連付けます。1 つの展開のみが存在する場合（常に少なくとも 1 つの展開が存在する）、この設定はありません。

1 つ以上の既存ドメインが *Unified CM* 上の *IM and Presence* サービスまたは *XMPP* フェデレーションに設定されていると、ドメイン設定の変更によって Expressway-C と Expressway-E の両方の XCP ルータが自動的に再起動します。

エンドユーザへの影響としてはフェデレーションが一時的に失われ、Mobile and Remote Access を使用している Jabber クライアントは一時的に切断されます。クライアントは短時間で自動的に再接続されます。

委任クレデンシャル チェックの設定（Expressway-E のみ）

[委任クレデンシャル チェック（delegated credential checking）]（**[設定（Configuration）] > [プロトコル（Protocols）] > [SIP]**）を有効にしている場合、このドメインの SIP メッセージのクレデンシャルチェックを委任するときに使用するトラバーサルゾーンを指定する必要があります。これは、Expressway がサービス プロバイダーおよび SIP レジストラとして機能している SIP ドメインにのみ適用されます。

必要に応じて、SIP ドメインごとに異なるゾーンを指定できます。

この Expressway-E を使用してクレデンシャル チェックを継続する場合は、*[委任しない（Do not delegate）]* を選択します。

クレデンシャル チェック サービスのテスト

クレデンシャル チェックを委任されている Expressway がメッセージを受信して、関連の認証チェックを実行できるかどうか確認するには、以下の手順を実行します。

手順

ステップ 1 **[設定（Configuration）] > [ドメイン（Domains）]** に移動します。

ステップ 2 関連するドメインを選択します。

ステップ 3 [クレデンシャル チェック サービスのテスト（Test credential checking service）] をクリックします。

[結果（Results）] セクションが表示され、受信側の Expressway にトラバーサル ゾーン経由で到達できるかどうか、また、NTLM と SIP の両方のダイジェスト タイプのチャレンジのクレデンシャル チェックを実行できるかどうかが示されます。

ビデオ ネットワークで NTLM 認証を使用していない場合、受信側の Expressway には Active Directory サービスへの接続が設定されていないため、NTLM のチェックは失敗します。

SIP および H.323 のインターワーキングの設定

「インターワーキング（Interworking）」 ページ（**[設定（Configuration）] > [プロトコル（Protocols）] > [インターワーキング（Interworking）]**）では、Expressway が SIP コールと H.323 コール間のゲートウェイとして機能するかどうかを設定できます。あるプロトコルから別のプロトコルへのコールの変換を「インターワーキング」と呼びます。

デフォルトでは、Expressway は SIP から H.323 へと、H.323 から SIP へのゲートウェイとして機能しますが、コールに関与しているエンドポイントの少なくとも 1 つがローカルに登録されている場合に限ります。この設定を、関与するエンドポイントがローカルに登録されているかどうかに関係なく、Expressway が SIP から H.323 へのゲートウェイとして機能するように変更できます。また、インターワーキングを完全に無効にするオプションもあります。

この **H.323 <-> SIP インターワーキング モード**のオプションは、次のとおりです。

- *[オフ（Off）]*：Expressway は SIP から H.323 へのゲートウェイとして機能しません。
- *[登録済みのみ（Registered only）]*：Expressway は SIP から H.323 へのゲートウェイとして機能しますが、これは、エンドポイントの 1 つがローカルに登録されている場合に限ります。
- *[オン（On）]*：Expressway は、エンドポイントがローカルに登録されているかどうかに関係なく、SIP から H.323 へのゲートウェイとして機能します。

（注） この設定を [登録済みのみ（Registered only）] のままにしておくことをお勧めします。ネットワークが正しく設定されていない場合は、*[オン（On）]* に設定すると（すべてのコールがインターワーキングされる）、H.323 エンドポイント間のコールが SIP で行われる、またはその逆などの不要なインターワーキングが発生することになる可能性があります。

Expressway が H.323 ゲートウェイへの SIP として機能するコールは、両方のエンドポイントがシスコインフラストラクチャに登録されている場合を除き、RMS コールです。Expressway は常に、SIP 側と H.323 側でペイロード タイプを個別にネゴシエートできるように SIP ～ H.323 のインターワーキング コールを取得し、これらをメディア パスとして書き直します。

また、SIP SDP ネゴシエーションでは、複数のコーデック機能を承認でき（複数のビデオ コーデックを受け入れることができ）、SIP デバイスはいつでも自由に使用するコーデックをコール内で変更できます。Expressway はメディア パスに存在するため、これが行われると、メディ

アが変更されるたびに（必要に応じて）H.323 デバイスへの論理チャンネルを開閉し、そのメディアを正しく通過させます。

DH キー長の設定

X12.6では、Expressway のセキュリティ強化の一環として、H.323 コール暗号化用 2048 ビット Diffie-Hellman キーのサポートを導入しました。そのため、Expressway はデフォルトの動作として、1024 ビットと 2048 ビットの暗号キーの長さを提供します。

これにより、展開されたファイアウォールの ALG 機能またはエンドポイントが Diffie-Hellman キー交換の 1024 ビットと 2048 ビットの両方を処理できない場合、予期しない H.323 コールエラーが発生する可能性があります。この場合、X12.6.4 の管理者は、CLI コマンド *xConfiguration Interworking Encryption KeySize2048: <On/Off>* を使用して、オプションで 1024 ビットの暗号化に戻すことができます。

インターワーキング暗号キーサイズの変更を有効にするために、再起動する必要ありません。クラスタ内のプライマリノードに対する変更は、その補助ノードに自動的にレプリケートされます。

プロトコルによる検索

ゾーンを検索する場合、Expressway は最初に着信コールのプロトコルを使用して検索を実行します。検索に失敗すると、Expressway は、送信元と [インターワーキング モード（Interworking mode）] に応じて、代替プロトコルを使用して、ゾーンを再度検索します。

（注） また、ゾーンは有効になっている関連プロトコルで設定されている必要があります（デフォルトでは、SIP と H.323 はゾーンで有効になっています）。

- 要求をネイバー システムから受け取っており、**[インターワーキングモード（Interworking mode）]**が *[登録済みのみ（Registered only）]* に設定されている場合、Expressway は両方のプロトコルを使用してローカルゾーンを検索します。また、その他のゾーンにはネイティブのプロトコルのみを使用して検索します（エンドポイントの一方がローカルに登録されている場合にのみコールをインターワーキングするため）。
- **[インターワーキング モード（Interworking mode）]** が *[オン（On）]* に設定されているか、または要求がローカルに登録されているエンドポイントから発信されたものである場合、Expressway は両方のプロトコルを使用して、ローカル ゾーンとすべての外部ゾーンを検索します。

H.323 番号をダイヤルするための SIP エンドポイントの有効化

SIP エンドポイントは、**name@domain** などの形式の URI でのみ、コールすることができます。発信者がコールの実行時にドメインを指定しない場合、SIP エンドポイントは自動的に自身のドメインをダイヤルされた番号に追加します。

つまり、SIP エンドポイントから **123** をダイヤルすると、**123@domain** が検索されます。ダイヤルする H.323 エンドポイントが **123** として登録されている場合、Expressway はエイリアスの

123@domain を見つけることができずにコールは失敗します。これを解決するには、次のいずれかを実行します。

- H.323 と SIP の両方で、すべてのエンドポイントが **name@domain** の形式のエイリアスで登録するようにします。
- 事前検索トランスフォーメーションを **number@domain** の形式の URI のエイリアスの **@domain** 部分を取り除いて Expressway 上に作成します。

  事前検索トランスフォーメーションの設定方法については、事前検索トランスフォーメーションの項を、H.323 番号からドメイン名を取り除く方法については H.323 番号にダイヤルする @domain の除去の項を参照してください。

DTMF 信号のインターワーキング

SIP コールの場合、Expressway は RTP ペイロードに DTMF シグナリング用の RFC 2833 を実装しています。

H.323 コールの場合、Expressway は DTMF シグナリング用の H.245 UserInputIndication を実装しています。**dtmf** がサポートされる唯一の **UserInputCapability** です。Expressway は他の H.245 ユーザ入力機能（**basicString** や **generalString** など）をサポートしません。

Expressway が SIP と H.323 間でコールをインターワーキングしている場合、DTMF シグナリングもインターワーキングしますが、これは RFC 2833 DTMF と H.245 ユーザ入力インジケータ「dtmf」と「basicString」間に限ります。